	plen=1024 qlen=160	plen=2048 qlen=224	plen=2048 qlen=256
Hash algorithm	SHA-1	SHA-224	SHA-256
Hash length	160	224	256
KDF		Concatenation KDF	
Derived Key Material length	320	448	512
MacKey length	80	112	128
MacTag length	80	112	128
ID_U		"ALICE"	
ID_V		"BOBBY"	
Message Strings (Unilateral)		KC_1_U KC_1_V	
Message Strings (Bilateral)		KC_2_U KC_2_V	
OtherInfo for KDF			
AlgorithmID	123456789ABCDEF0		
PartyUInfo	414C494345313233		
PartyVInfo	424F424259343536		
SupPubInfo	not used		

OtherInfo for KDF (dhStatic) requires the PartyUInfo to contain a nonce therefore the value is:
PartyUInfo = 414C494345313233 || nonceU_byte_len || nonceU

```
##############################################################

Key Establishment Schemes for Finite Field Cryptography
plen: 1024
qlen: 160
Hash algorithm used: SHA-1
KDF: Contatenation KDF
DKM len: 320
MacKey length: 80
MacTag len: 80
ID_U: "ALICE"
ID_V: "BOBBY"

P is
                                                B10B8F96 A080E01D
        DE92DE5E AE5D54EC 52C99FBC FB06A3C6 9A6A9DCA 52D23B61
        6073E286 75A23D18 9838EF1E 2EE652C0 13ECB4AE A9061123
        24975C3C D49B83BF ACCBDD7D 90C4BD70 98488E9C 219A7372
        4EFFD6FA E5644738 FAA31A4F F55BCCC0 A151AF5F 0DC8B4BD
        45BF37DF 365C1A65 E68CFDA7 6D4DA708 DF1FB2BC 2E4A4371


Q is
                F518AA87 81A8DF27 8ABA4E7D 64B7CB9D 49462353


G is
                                                A4D1CBD5 C3FD3412
        6765A442 EFB99905 F8104DD2 58AC507F D6406CFF 14266D31
        266FEA1E 5C41564B 777E690F 5504F213 160217B4 B01B886A
        5E91547F 9E2749F4 D7FBD7D3 B9A92EE1 909D0D22 63F80A76
        A6A24C08 7A091F53 1DBF0A01 69B6A28A D662A4D1 8E73AFA3
        2D779D59 18D08BC8 858F4DCE F97C2A24 855E6EEB 22B3B2E5



##############################################################


dhHybrid1(160)
--------------------------------------------------------------
xU is
                488C4A74 D904BD8C F522B072 A4C1D4CC ADFD0A8A


yU is
```

                                                92FF6A92 3A2611A8
        251C65D3 07DE34BA DD701E71 377850AC 659CDF20 370DA2C8
        B72AA24A 5BCBEA61 4C0BFDEE 19B68D1B 66996C82 49A2F0BC
        E128B3E8 EF548E62 9B7098E4 9657BC74 96D1658A CAD918B3
        AE7D966B 7D4099A2 88AEE7FB 2FA8AB2A 3CB4D35E 948F014E
        5FBFB1CA 495D3F12 EEA9387B 4438F700 FFA2DC14 9F75A2F4

xV is
                875A5065 584974BF DE5D833A 01556EA8 27E04F21

yV is
                                                693AB770 0B57AE80
        4EA5FAD7 14BE42B4 78089136 2922FA1E ECF92B86 0C5E86FD
        8423EFC1 9B31C728 6BBB1B75 89C81B3D 0F19C28C F30647AC
        A2BD2A39 A5AE2074 386A2739 BA9319C6 256867DA AE120E47
        94C88970 3FA5B6C3 AF209EEA B24AC5C9 6BF25EE9 3E6700EC
        43F180EE A7B4E8C0 E5F2A83B F7A1EC0E 767C454C A77C1CAC

rU is
                0C69270C E103732F 8CFE8A06 862CBC08 47F037D4

tU is
                                                781AAECD 57093E51
        EAC44696 5707BC43 5FE28745 52EB2E31 28795514 A4E2CDE1
        2CBEFB1B 81219B52 AEE9573D FD9DC0CD 0C5A4B96 BD6E0BCA
        11B92759 20813EE6 E83250A6 D254C8D7 40B12F11 EAF0210C
        C99892D7 BFB7482A 510A673A C92509BC F7E33DC1 B5C0758F
        2447971A 1946AC33 E9E5C0C6 3B837957 7FD1329F C684A4A6

rV is
                1AF13D1E BB11F5D8 05517F8A 64CF934A C0098ED5

tV is
                                                6D0FE39B A4DCA9A7
        78E01C67 81616EB5 B7A3408C 77CBC576 5A77E7D2 57CEE6E9
        C3303973 63A819F6 CB125BE4 B7D4A274 DA238202 DB018A8F
        406CD1A0 3789F74F 7F6D8179 A290D43F 5872AA42 3C4F7620
        2FBBB5FB 2ABBB8E6 C7097945 6BEA46B9 578D8D2C 6877B3AE
        DDCC5DF1 6209F390 D7B0F520 F7AE02EC E058E992 56B5BABB

```
-----------------------------------------------------------
no Key Confirmation
Zs is
                                                AD371125 57E0E634
        B581327A 4AD32C7C 764BE8F8 080D372C 632093A7 67F155BD
        22EC003C A61C8B43 320F3ABE B5DDC4A3 B18982FD D6510F88
        3C8DC1E0 B157FFB9 CFC0A59C E2D4055F FC73E715 2A6A9543
        B919E794 E9496133 BE2A2318 D9056EFD 74482DC6 3C0DB58F
        E6426B0F E7354542 C2197AB6 BD35F1A9 2DCE90B1 C46D32C1


Ze is
                                                715DC0EA 246B4656
        63A89CDE 0412C192 E19E58D5 B0B6366D A789ADBF 449A38AA
        4669FE36 30A20F7F A3149C9B 4B0AB5CD 3E14182B 7504D5D2
        752BF658 7AABC9F4 CB8FE529 236AB815 36ADD2BD 25D6BF9D
        5F1DF576 165AA55C 249961D8 F87500ED 8DBFC5D2 50534C07
        D99AC917 F9846046 AC5CB8A2 98742622 D3C98618 069246E8


Z is
                        715DC0EA 246B4656 63A89CDE 0412C192
        E19E58D5 B0B6366D A789ADBF 449A38AA 4669FE36 30A20F7F
        A3149C9B 4B0AB5CD 3E14182B 7504D5D2 752BF658 7AABC9F4
        CB8FE529 236AB815 36ADD2BD 25D6BF9D 5F1DF576 165AA55C
        249961D8 F87500ED 8DBFC5D2 50534C07 D99AC917 F9846046
        AC5CB8A2 98742622 D3C98618 069246E8 AD371125 57E0E634
        B581327A 4AD32C7C 764BE8F8 080D372C 632093A7 67F155BD
        22EC003C A61C8B43 320F3ABE B5DDC4A3 B18982FD D6510F88
        3C8DC1E0 B157FFB9 CFC0A59C E2D4055F FC73E715 2A6A9543
        B919E794 E9496133 BE2A2318 D9056EFD 74482DC6 3C0DB58F
        E6426B0F E7354542 C2197AB6 BD35F1A9 2DCE90B1 C46D32C1


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


KeyData is
                        1B5FCC8D 81A5D9A9 3694E647 7788D803
        1584C3F5 2E9F117A E8184DBA 56479D87 667692F1 2D7BD38B
```

```
-----------------------------------------------------------
Scheme Initiator, Key Confirmation Provider: U to V
Zs is
                                              AD371125 57E0E634
        B581327A 4AD32C7C 764BE8F8 080D372C 632093A7 67F155BD
        22EC003C A61C8B43 320F3ABE B5DDC4A3 B18982FD D6510F88
        3C8DC1E0 B157FFB9 CFC0A59C E2D4055F FC73E715 2A6A9543
        B919E794 E9496133 BE2A2318 D9056EFD 74482DC6 3C0DB58F
        E6426B0F E7354542 C2197AB6 BD35F1A9 2DCE90B1 C46D32C1


Ze is
                                              715DC0EA 246B4656
        63A89CDE 0412C192 E19E58D5 B0B6366D A789ADBF 449A38AA
        4669FE36 30A20F7F A3149C9B 4B0AB5CD 3E14182B 7504D5D2
        752BF658 7AABC9F4 CB8FE529 236AB815 36ADD2BD 25D6BF9D
        5F1DF576 165AA55C 249961D8 F87500ED 8DBFC5D2 50534C07
        D99AC917 F9846046 AC5CB8A2 98742622 D3C98618 069246E8


Z is
                         715DC0EA 246B4656 63A89CDE 0412C192
        E19E58D5 B0B6366D A789ADBF 449A38AA 4669FE36 30A20F7F
        A3149C9B 4B0AB5CD 3E14182B 7504D5D2 752BF658 7AABC9F4
        CB8FE529 236AB815 36ADD2BD 25D6BF9D 5F1DF576 165AA55C
        249961D8 F87500ED 8DBFC5D2 50534C07 D99AC917 F9846046
        AC5CB8A2 98742622 D3C98618 069246E8 AD371125 57E0E634
        B581327A 4AD32C7C 764BE8F8 080D372C 632093A7 67F155BD
        22EC003C A61C8B43 320F3ABE B5DDC4A3 B18982FD D6510F88
        3C8DC1E0 B157FFB9 CFC0A59C E2D4055F FC73E715 2A6A9543
        B919E794 E9496133 BE2A2318 D9056EFD 74482DC6 3C0DB58F
        E6426B0F E7354542 C2197AB6 BD35F1A9 2DCE90B1 C46D32C1


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


MacData is
                                              4B435F31 5F55414C
        49434542 4F424259 781AAECD 57093E51 EAC44696 5707BC43
        5FE28745 52EB2E31 28795514 A4E2CDE1 2CBEFB1B 81219B52
        AEE9573D FD9DC0CD 0C5A4B96 BD6E0BCA 11B92759 20813EE6
        E83250A6 D254C8D7 40B12F11 EAF0210C C99892D7 BFB7482A
```

510A673A C92509BC F7E33DC1 B5C0758F 2447971A 1946AC33
E9E5C0C6 3B837957 7FD1329F C684A4A6 6D0FE39B A4DCA9A7
78E01C67 81616EB5 B7A3408C 77CBC576 5A77E7D2 57CEE6E9
C3303973 63A819F6 CB125BE4 B7D4A274 DA238202 DB018A8F
406CD1A0 3789F74F 7F6D8179 A290D43F 5872AA42 3C4F7620
2FBBB5FB 2ABBB8E6 C7097945 6BEA46B9 578D8D2C 6877B3AE
DDCC5DF1 6209F390 D7B0F520 F7AE02EC E058E992 56B5BABB

MacKey is
1B5F CC8D81A5 D9A93694

Mtag is
AA95 E68877F3 EC24A8A1

KeyData is
E6477788 D8031584 C3F52E9F 117AE818
4DBA5647 9D876676 92F12D7B D38B1B09 FF01EDFA 24910C47

Scheme Responder, Key Confirmation Provider: V to U
Zs is
AD371125 57E0E634
B581327A 4AD32C7C 764BE8F8 080D372C 632093A7 67F155BD
22EC003C A61C8B43 320F3ABE B5DDC4A3 B18982FD D6510F88
3C8DC1E0 B157FFB9 CFC0A59C E2D4055F FC73E715 2A6A9543
B919E794 E9496133 BE2A2318 D9056EFD 74482DC6 3C0DB58F
E6426B0F E7354542 C2197AB6 BD35F1A9 2DCE90B1 C46D32C1

Ze is
715DC0EA 246B4656
63A89CDE 0412C192 E19E58D5 B0B6366D A789ADBF 449A38AA
4669FE36 30A20F7F A3149C9B 4B0AB5CD 3E14182B 7504D5D2
752BF658 7AABC9F4 CB8FE529 236AB815 36ADD2BD 25D6BF9D
5F1DF576 165AA55C 249961D8 F87500ED 8DBFC5D2 50534C07
D99AC917 F9846046 AC5CB8A2 98742622 D3C98618 069246E8

Z is
715DC0EA 246B4656 63A89CDE 0412C192

E19E58D5 B0B6366D A789ADBF 449A38AA 4669FE36 30A20F7F
A3149C9B 4B0AB5CD 3E14182B 7504D5D2 752BF658 7AABC9F4
CB8FE529 236AB815 36ADD2BD 25D6BF9D 5F1DF576 165AA55C
249961D8 F87500ED 8DBFC5D2 50534C07 D99AC917 F9846046
AC5CB8A2 98742622 D3C98618 069246E8 AD371125 57E0E634
B581327A 4AD32C7C 764BE8F8 080D372C 632093A7 67F155BD
22EC003C A61C8B43 320F3ABE B5DDC4A3 B18982FD D6510F88
3C8DC1E0 B157FFB9 CFC0A59C E2D4055F FC73E715 2A6A9543
B919E794 E9496133 BE2A2318 D9056EFD 74482DC6 3C0DB58F
E6426B0F E7354542 C2197AB6 BD35F1A9 2DCE90B1 C46D32C1

OtherInfo is
12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536

MacData is
4B435F31 5F56424F
42425941 4C494345 6D0FE39B A4DCA9A7 78E01C67 81616EB5
B7A3408C 77CBC576 5A77E7D2 57CEE6E9 C3303973 63A819F6
CB125BE4 B7D4A274 DA238202 DB018A8F 406CD1A0 3789F74F
7F6D8179 A290D43F 5872AA42 3C4F7620 2FBBB5FB 2ABBB8E6
C7097945 6BEA46B9 578D8D2C 6877B3AE DDCC5DF1 6209F390
D7B0F520 F7AE02EC E058E992 56B5BABB 781AAECD 57093E51
EAC44696 5707BC43 5FE28745 52EB2E31 28795514 A4E2CDE1
2CBEFB1B 81219B52 AEE9573D FD9DC0CD 0C5A4B96 BD6E0BCA
11B92759 20813EE6 E83250A6 D254C8D7 40B12F11 EAF0210C
C99892D7 BFB7482A 510A673A C92509BC F7E33DC1 B5C0758F
2447971A 1946AC33 E9E5C0C6 3B837957 7FD1329F C684A4A6

MacKey is
1B5F CC8D81A5 D9A93694

Mtag is
66D7 1897183B E5FDAA90

KeyData is
E6477788 D8031584 C3F52E9F 117AE818
4DBA5647 9D876676 92F12D7B D38B1B09 FF01EDFA 24910C47

```
------------------------------------------------------------
Scheme Initiator, Key Confirmation Bilateral
Zs is
                                                AD371125 57E0E634
        B581327A 4AD32C7C 764BE8F8 080D372C 632093A7 67F155BD
        22EC003C A61C8B43 320F3ABE B5DDC4A3 B18982FD D6510F88
        3C8DC1E0 B157FFB9 CFC0A59C E2D4055F FC73E715 2A6A9543
        B919E794 E9496133 BE2A2318 D9056EFD 74482DC6 3C0DB58F
        E6426B0F E7354542 C2197AB6 BD35F1A9 2DCE90B1 C46D32C1


Ze is
                                                715DC0EA 246B4656
        63A89CDE 0412C192 E19E58D5 B0B6366D A789ADBF 449A38AA
        4669FE36 30A20F7F A3149C9B 4B0AB5CD 3E14182B 7504D5D2
        752BF658 7AABC9F4 CB8FE529 236AB815 36ADD2BD 25D6BF9D
        5F1DF576 165AA55C 249961D8 F87500ED 8DBFC5D2 50534C07
        D99AC917 F9846046 AC5CB8A2 98742622 D3C98618 069246E8


Z is
                        715DC0EA 246B4656 63A89CDE 0412C192
        E19E58D5 B0B6366D A789ADBF 449A38AA 4669FE36 30A20F7F
        A3149C9B 4B0AB5CD 3E14182B 7504D5D2 752BF658 7AABC9F4
        CB8FE529 236AB815 36ADD2BD 25D6BF9D 5F1DF576 165AA55C
        249961D8 F87500ED 8DBFC5D2 50534C07 D99AC917 F9846046
        AC5CB8A2 98742622 D3C98618 069246E8 AD371125 57E0E634
        B581327A 4AD32C7C 764BE8F8 080D372C 632093A7 67F155BD
        22EC003C A61C8B43 320F3ABE B5DDC4A3 B18982FD D6510F88
        3C8DC1E0 B157FFB9 CFC0A59C E2D4055F FC73E715 2A6A9543
        B919E794 E9496133 BE2A2318 D9056EFD 74482DC6 3C0DB58F
        E6426B0F E7354542 C2197AB6 BD35F1A9 2DCE90B1 C46D32C1


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


U2V
----------------
MacData is
                                                4B435F32 5F55414C
        49434542 4F424259 781AAECD 57093E51 EAC44696 5707BC43
        5FE28745 52EB2E31 28795514 A4E2CDE1 2CBEFB1B 81219B52
        AEE9573D FD9DC0CD 0C5A4B96 BD6E0BCA 11B92759 20813EE6
        E83250A6 D254C8D7 40B12F11 EAF0210C C99892D7 BFB7482A
```

510A673A C92509BC F7E33DC1 B5C0758F 2447971A 1946AC33
E9E5C0C6 3B837957 7FD1329F C684A4A6 6D0FE39B A4DCA9A7
78E01C67 81616EB5 B7A3408C 77CBC576 5A77E7D2 57CEE6E9
C3303973 63A819F6 CB125BE4 B7D4A274 DA238202 DB018A8F
406CD1A0 3789F74F 7F6D8179 A290D43F 5872AA42 3C4F7620
2FBBB5FB 2ABBB8E6 C7097945 6BEA46B9 578D8D2C 6877B3AE
DDCC5DF1 6209F390 D7B0F520 F7AE02EC E058E992 56B5BABB

MacKey is
1B5F CC8D81A5 D9A93694

Mtag is
AA91 03ECB9EB FE36110A

V2U

MacData is
4B435F32 5F56424F
42425941 4C494345 6D0FE39B A4DCA9A7 78E01C67 81616EB5
B7A3408C 77CBC576 5A77E7D2 57CEE6E9 C3303973 63A819F6
CB125BE4 B7D4A274 DA238202 DB018A8F 406CD1A0 3789F74F
7F6D8179 A290D43F 5872AA42 3C4F7620 2FBBB5FB 2ABBB8E6
C7097945 6BEA46B9 578D8D2C 6877B3AE DDCC5DF1 6209F390
D7B0F520 F7AE02EC E058E992 56B5BABB 781AAECD 57093E51
EAC44696 5707BC43 5FE28745 52EB2E31 28795514 A4E2CDE1
2CBEFB1B 81219B52 AEE9573D FD9DC0CD 0C5A4B96 BD6E0BCA
11B92759 20813EE6 E83250A6 D254C8D7 40B12F11 EAF0210C
C99892D7 BFB7482A 510A673A C92509BC F7E33DC1 B5C0758F
2447971A 1946AC33 E9E5C0C6 3B837957 7FD1329F C684A4A6

MacKey is
1B5F CC8D81A5 D9A93694

Mtag is
21DE 38FCCA61 9BF5D318

KeyData is
E6477788 D8031584 C3F52E9F 117AE818
4DBA5647 9D876676 92F12D7B D38B1B09 FF01EDFA 24910C47

==========

MQV2(160)
---
xU is
6BE93BE8 7EF5232C 3E88EE62 9AB304C5 886AB1E3

yU is
19E112B4 19FD1AAA
7E966C3D 20E31EDD 69F9C87F 7283C0B4 8344143A 252A5A91
31B6652B 8F850C45 6F783081 D71DE58A 6333A34E AACA2C6D
D1B20B86 E32CDFA0 AF29F080 EC55250B 09B1B26B A9F0F6EF
DB81050B AECEC067 34A6EB4F B2A26588 C63B347F 45A9ABB6
167FB065 2B044D2D 449C81D8 97A0B6E1 EDA3D24B 9CC8D457

xV is
82DB8539 09F6E35B 2BDAF7DC 8B502538 B4FC4CDC

yV is
8BCD5CDE 2FD600C0
883786FD 5C7BFEF6 A89A192D 11F1145B 0C8ECE8A D6116ABA
E012801E 89212337 30CE3534 505D542D 3AEFD15F 1788BA94
82B8DFE0 BDA94069 897E25C3 BF0A90CD 8DD3BC28 6E4614E6
61785EBC 9DE25E20 0D32467B 3373F505 7EA0E7FE 128DDB92
8F340E90 1C9AB1D2 78B8E6B3 454984BF D48E3D24 6DD4A089

rU is
E9DDA9BC E4CB6291 B25F5BA2 D6B8F0E3 355B9A82

tU is
A26C3019 19AA7849
76A8B641 8421C067 325DE9A5 E6719561 89790920 45331E68
5A8A2458 421D425D D6994EF5 218544D0 E6FDCD9E A92F1179
74F12BCE 08BF90C8 F9BB24A4 49963D48 06BDA131 0DED6921
E8A12335 428C5D4B 775722E5 A85CE15F D33F707D A006EF6E
A2A7A801 FF95AF75 2EF809E9 979141AF EF898796 95CD3D33

rV is

0BEDE2A5 6AF823DA 6A166E38 3F4ABA14 18E4085C

tV is
77B43832 A934072C
DDA230E0 38C58304 98990002 5BF9057B F1F1434E 5A93F130
FEEF64A3 BAB73A57 989CAA46 E7209528 8227C072 A3F92617
27562354 04B5A415 F39FC562 C2F1A675 C1AFC55E 0F4618BF
C2A87A14 0036D638 4BBAEA6C 31F1172B 017BD7A9 020D182A
FA21105D EC22B201 2A938F27 55F0E2DA 02994990 91C897D4

---

no Key Confirmation
Z is
33E050BD 209F2DF2
771978FC D1D4C82E 49D01D65 BB620320 D30BFEA8 7AA869E1
07A517A4 C85B6928 4521CA54 B77F59E9 4A856DAA 30A385A5
25D8A3F7 E15EE5E9 AA128D45 EF63F90C 10E08FC5 26361377
81547A58 9F9787F9 D7DD6143 419A2616 80168240 AAB2013D
8020DBE8 4B7E2BED CE671B94 03BD1F91 71A25790 CE667DED

OtherInfo is
12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536

KDFval is
35108585 FC5562B5 F18F207B A83563E4
4928456A 5E53637E AE6BB5FC 3388AE02 91790A1D C8314E28

KeyData is
35108585 FC5562B5 F18F207B A83563E4
4928456A 5E53637E AE6BB5FC 3388AE02 91790A1D C8314E28

Scheme Initiator, Key Confirmation Provider: U to V
Z is
33E050BD 209F2DF2
771978FC D1D4C82E 49D01D65 BB620320 D30BFEA8 7AA869E1

```
        07A517A4 C85B6928 4521CA54 B77F59E9 4A856DAA 30A385A5
        25D8A3F7 E15EE5E9 AA128D45 EF63F90C 10E08FC5 26361377
        81547A58 9F9787F9 D7DD6143 419A2616 80168240 AAB2013D
        8020DBE8 4B7E2BED CE671B94 03BD1F91 71A25790 CE667DED


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


KDFval is
                                                            3510
        8585FC55 62B5F18F 207BA835 63E44928 456A5E53 637EAE6B
        B5FC3388 AE029179 0A1DC831 4E287F32 136B1B88 3ADEA2B9


MacData is
                                            4B435F31 5F55414C
        49434542 4F424259 A26C3019 19AA7849 76A8B641 8421C067
        325DE9A5 E6719561 89790920 45331E68 5A8A2458 421D425D
        D6994EF5 218544D0 E6FDCD9E A92F1179 74F12BCE 08BF90C8
        F9BB24A4 49963D48 06BDA131 0DED6921 E8A12335 428C5D4B
        775722E5 A85CE15F D33F707D A006EF6E A2A7A801 FF95AF75
        2EF809E9 979141AF EF898796 95CD3D33 77B43832 A934072C
        DDA230E0 38C58304 98990002 5BF9057B F1F1434E 5A93F130
        FEEF64A3 BAB73A57 989CAA46 E7209528 8227C072 A3F92617
        27562354 04B5A415 F39FC562 C2F1A675 C1AFC55E 0F4618BF
        C2A87A14 0036D638 4BBAEA6C 31F1172B 017BD7A9 020D182A
        FA21105D EC22B201 2A938F27 55F0E2DA 02994990 91C897D4


MacKey is
                                        3510 8585FC55 62B5F18F


Mtag is
                                        D1FA 58CD2CB8 D5D254D4


KeyData is
                            207BA835 63E44928 456A5E53 637EAE6B
        B5FC3388 AE029179 0A1DC831 4E287F32 136B1B88 3ADEA2B9
```

```
-----------------------------------------------------------
Scheme Responder, Key Confirmation Provider: V to U
Z is
                                                33E050BD 209F2DF2
        771978FC D1D4C82E 49D01D65 BB620320 D30BFEA8 7AA869E1
        07A517A4 C85B6928 4521CA54 B77F59E9 4A856DAA 30A385A5
        25D8A3F7 E15EE5E9 AA128D45 EF63F90C 10E08FC5 26361377
        81547A58 9F9787F9 D7DD6143 419A2616 80168240 AAB2013D
        8020DBE8 4B7E2BED CE671B94 03BD1F91 71A25790 CE667DED


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


KDFval is
                                                            3510
        8585FC55 62B5F18F 207BA835 63E44928 456A5E53 637EAE6B
        B5FC3388 AE029179 0A1DC831 4E287F32 136B1B88 3ADEA2B9


MacData is
                                                4B435F31 5F56424F
        42425941 4C494345 77B43832 A934072C DDA230E0 38C58304
        98990002 5BF9057B F1F1434E 5A93F130 FEEF64A3 BAB73A57
        989CAA46 E7209528 8227C072 A3F92617 27562354 04B5A415
        F39FC562 C2F1A675 C1AFC55E 0F4618BF C2A87A14 0036D638
        4BBAEA6C 31F1172B 017BD7A9 020D182A FA21105D EC22B201
        2A938F27 55F0E2DA 02994990 91C897D4 A26C3019 19AA7849
        76A8B641 8421C067 325DE9A5 E6719561 89790920 45331E68
        5A8A2458 421D425D D6994EF5 218544D0 E6FDCD9E A92F1179
        74F12BCE 08BF90C8 F9BB24A4 49963D48 06BDA131 0DED6921
        E8A12335 428C5D4B 775722E5 A85CE15F D33F707D A006EF6E
        A2A7A801 FF95AF75 2EF809E9 979141AF EF898796 95CD3D33


MacKey is
                                        3510 8585FC55 62B5F18F


Mtag is
                                        CF81 78981B97 A5B51AE1


KeyData is
                            207BA835 63E44928 456A5E53 637EAE6B
```

```
        B5FC3388 AE029179 0A1DC831 4E287F32 136B1B88 3ADEA2B9



-------------------------------------------------------------
Scheme Initiator, Key Confirmation Bilateral
Z is
                                                33E050BD 209F2DF2
        771978FC D1D4C82E 49D01D65 BB620320 D30BFEA8 7AA869E1
        07A517A4 C85B6928 4521CA54 B77F59E9 4A856DAA 30A385A5
        25D8A3F7 E15EE5E9 AA128D45 EF63F90C 10E08FC5 26361377
        81547A58 9F9787F9 D7DD6143 419A2616 80168240 AAB2013D
        8020DBE8 4B7E2BED CE671B94 03BD1F91 71A25790 CE667DED


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


KDFval is
                                                          3510
        8585FC55 62B5F18F 207BA835 63E44928 456A5E53 637EAE6B
        B5FC3388 AE029179 0A1DC831 4E287F32 136B1B88 3ADEA2B9


U2V
----------------
MacData is
                                                4B435F32 5F55414C
        49434542 4F424259 A26C3019 19AA7849 76A8B641 8421C067
        325DE9A5 E6719561 89790920 45331E68 5A8A2458 421D425D
        D6994EF5 218544D0 E6FDCD9E A92F1179 74F12BCE 08BF90C8
        F9BB24A4 49963D48 06BDA131 0DED6921 E8A12335 428C5D4B
        775722E5 A85CE15F D33F707D A006EF6E A2A7A801 FF95AF75
        2EF809E9 979141AF EF898796 95CD3D33 77B43832 A934072C
        DDA230E0 38C58304 98990002 5BF9057B F1F1434E 5A93F130
        FEEF64A3 BAB73A57 989CAA46 E7209528 8227C072 A3F92617
        27562354 04B5A415 F39FC562 C2F1A675 C1AFC55E 0F4618BF
        C2A87A14 0036D638 4BBAEA6C 31F1172B 017BD7A9 020D182A
        FA21105D EC22B201 2A938F27 55F0E2DA 02994990 91C897D4


MacKey is
                                          3510 8585FC55 62B5F18F
```

```
Mtag is
                                        8C73 A3B0E33F E401EC5D


V2U
----------------
MacData is
                                                4B435F32 5F56424F
        42425941 4C494345 77B43832 A934072C DDA230E0 38C58304
        98990002 5BF9057B F1F1434E 5A93F130 FEEF64A3 BAB73A57
        989CAA46 E7209528 8227C072 A3F92617 27562354 04B5A415
        F39FC562 C2F1A675 C1AFC55E 0F4618BF C2A87A14 0036D638
        4BBAEA6C 31F1172B 017BD7A9 020D182A FA21105D EC22B201
        2A938F27 55F0E2DA 02994990 91C897D4 A26C3019 19AA7849
        76A8B641 8421C067 325DE9A5 E6719561 89790920 45331E68
        5A8A2458 421D425D D6994EF5 218544D0 E6FDCD9E A92F1179
        74F12BCE 08BF90C8 F9BB24A4 49963D48 06BDA131 0DED6921
        E8A12335 428C5D4B 775722E5 A85CE15F D33F707D A006EF6E
        A2A7A801 FF95AF75 2EF809E9 979141AF EF898796 95CD3D33


MacKey is
                                        3510 8585FC55 62B5F18F


Mtag is
                                        A8C9 D408674A D952C2DC


KeyData is
                           207BA835 63E44928 456A5E53 637EAE6B
        B5FC3388 AE029179 0A1DC831 4E287F32 136B1B88 3ADEA2B9


============================================================


dhEphem(160)
------------------------------------------------------------
rU is
                 B9A3B3AE 8FEFC1A2 93049650 7086F845 5D48943E


tU is
                                                2A853B3D 92197501
```

```
        B9015B2D EB3ED84F 5E021DCC 3E52F109 D3273D2B 7521281C
        BABE0E76 FF5727FA 8ACCE269 56BA9A1F CA26F202 28D8693F
        EB10841D 84A73600 54ECE5A7 F5B7A61A D3DFB3C6 0D2E4310
        6D8727DA 37DF9CCE 95B47875 5D06BCEA 8F9D4596 5F75A5F3
        D1DF3701 165FC9E5 0C4279CE B07F9895 40AE96D5 D88ED776


rV is
                9392C9F9 EB6A7A6A 9022F7D8 3E7223C6 835BBDDA


tV is
                                           717A6CB0 53371FF4
        A3B93294 1C1E5663 F861A1D6 AD34AE66 576DFB98 F6C6CBF9
        DDD5A56C 7833F6BC FDFF0955 82AD868E 440E8D09 FD769E3C
        ECCDC3D3 B1E4CFA0 57776CAA F9739B6A 9FEE8E74 11F8D6DA
        C09D6A4E DB46CC2B 5D520309 0EAE6126 311E53FD 2C14B574
        E6A3109A 3DA1BE41 BDCEAA18 6F5CE067 16A2B6A0 7B3C33FE




------------------------------------------------------------
no Key Confirmation
Z is
                                           5C804F45 4D30D9C4
        DF85271F 93528C91 DF6B48AB 5F80B3B5 9CAAC1B2 8F8ACBA9
        CD3E39F3 CB614525 D9521D2E 644C53B8 07B810F3 40062F25
        7D7D6FBF E8D5E8F0 72E9B6E9 AFDA9413 EAFB2E8B 0699B1FB
        5A0CACED DEAEAD7E 9CFBB36A E2B42083 5BD83A19 FB0B5E96
        BF8FA4D0 9E345525 167ECD91 55416F46 F408ED31 B63C6E6D


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


KDFval is
                         FAA022CE 7FA9BA95 EBA39F3F 44F3EE14
        960A0B23 9D014B57 70E471D7 5A99EA87 10E38F0C EF0FFC67


KeyData is
                         FAA022CE 7FA9BA95 EBA39F3F 44F3EE14
        960A0B23 9D014B57 70E471D7 5A99EA87 10E38F0C EF0FFC67
```

```
============================================================


dhHybridOneFlow(160)
------------------------------------------------------------
xU is
                77D616A1 041B9CDF FE6F2E5A 7A69E920 EF0F6CE6


yU is
                                            70635A65 FCE1A89C
        CA93EDA4 E8487D70 64164A43 1FF8872F B3F20213 955E3F34
        04B5D605 45B0F481 0421109C 9A0FE5B9 06E8A817 D07C2708
        79DDC2C1 AAE6E45E A0F4FEE5 50DEF963 636E62C4 3B686CDB
        22D6B31C B0F94FF9 0991E39F F743C0EA 0704F21A CD13B42E
        3207B991 39894740 5423F9C3 B8FE5EFA AF67EAC6 BA89770B


xV is
                0A510EFA 62479D7A 9E51590C EB9DC847 038B313B


yV is
                                            19AADA41 FB6C16B6
        FF1BC2F0 5DFFA956 AEA8DAF3 E617EC08 99B5D156 8DA40FC3
        31BB48CF B8EB3B17 8C79413A 7866C306 63EA251C 78A739CE
        6128542E F3C907B4 0404CDE2 BC518B75 C3103A95 F5E047E3
        5AE6B690 758C470F 3FE9D2AA 6A8D3E4E EBF950A1 ED03D901
        D805C6F6 55342245 B9C20D29 02E97B47 3AF89F6F B6BA11A4


rU is
                A495C5AD BAFB98AC 42226A6F 524D24CF 4B16B0C8


tU is
                                            934C1B90 64E384DD
        F3DB7BCA 92EF41C1 7DB545FB AEB43977 094F49FD 09F570DF
        D8DF7BCA E8CBC893 FBA990B5 437750AF 390EAC68 2F358FEC
        39A98504 0011E12F F3B6BA29 5A8A3245 7777E57A 3E9C897D
        F022338F FF2969F0 67724BF4 AEA72B6B 6C0C3FCA 6D2AB282
        8F97D522 4C522EDB 2EA66475 5E772467 04696E88 64931FFC
```

```
------------------------------------------------------------
no Key Confirmation
Zs is
                                                4963B3B5 F596751F
        D360FFCA DD1178E3 15BC8C92 225361D6 920CD5C8 F1B01417
        D86D43D2 CF2D1376 E32CB0DE 3D888912 0315BAE4 CB902D88
        C8E4B634 70B4BD83 9D704E17 D9805DEE 10D3C927 EA605637
        39F30B6C FD06AEAB 0AFED5D2 64ABFC1A 04530BCC 71C47958
        FA2191C3 682C55AA E0B30B5A 44DBB431 FBC262D3 4B12DC9A


Ze is
                                                43C96FD0 1E78BEBF
        7A3394CA 9C61CDEC 27896216 55FDA3DF ADAFBDA7 B37CB00D
        E434D917 93C00ABA 7D93CF7E 2E47E9A4 9BCE9704 4FDAF332
        AD4EEBA3 B047F557 F4074C33 52582BB7 C234E03A 8EAC7298
        5FBA57EC A38F96CF 18854EF3 B5BA8B81 CA969D41 1F894C93
        4A034826 79827027 DF2D4932 168804F8 2FA3AE12 641D850B


Z is
                        43C96FD0 1E78BEBF 7A3394CA 9C61CDEC
        27896216 55FDA3DF ADAFBDA7 B37CB00D E434D917 93C00ABA
        7D93CF7E 2E47E9A4 9BCE9704 4FDAF332 AD4EEBA3 B047F557
        F4074C33 52582BB7 C234E03A 8EAC7298 5FBA57EC A38F96CF
        18854EF3 B5BA8B81 CA969D41 1F894C93 4A034826 79827027
        DF2D4932 168804F8 2FA3AE12 641D850B 4963B3B5 F596751F
        D360FFCA DD1178E3 15BC8C92 225361D6 920CD5C8 F1B01417
        D86D43D2 CF2D1376 E32CB0DE 3D888912 0315BAE4 CB902D88
        C8E4B634 70B4BD83 9D704E17 D9805DEE 10D3C927 EA605637
        39F30B6C FD06AEAB 0AFED5D2 64ABFC1A 04530BCC 71C47958
        FA2191C3 682C55AA E0B30B5A 44DBB431 FBC262D3 4B12DC9A


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


KDFval is
                        5E121366 2D4EE074 234B060F A7A363F0
        6A1FA9AE 7A1F438B 15F9BAB0 55D0F549 59C596C5 88C56FA6


KeyData is
                        5E121366 2D4EE074 234B060F A7A363F0
```

6A1FA9AE 7A1F438B 15F9BAB0 55D0F549 59C596C5 88C56FA6

Scheme Initiator, Key Confirmation Provider: U to V
NonceV is
022317D7 3E524030 88978832 60503412 339FBB62

Zs is
4963B3B5 F596751F
D360FFCA DD1178E3 15BC8C92 225361D6 920CD5C8 F1B01417
D86D43D2 CF2D1376 E32CB0DE 3D888912 0315BAE4 CB902D88
C8E4B634 70B4BD83 9D704E17 D9805DEE 10D3C927 EA605637
39F30B6C FD06AEAB 0AFED5D2 64ABFC1A 04530BCC 71C47958
FA2191C3 682C55AA E0B30B5A 44DBB431 FBC262D3 4B12DC9A

Ze is
43C96FD0 1E78BEBF
7A3394CA 9C61CDEC 27896216 55FDA3DF ADAFBDA7 B37CB00D
E434D917 93C00ABA 7D93CF7E 2E47E9A4 9BCE9704 4FDAF332
AD4EEBA3 B047F557 F4074C33 52582BB7 C234E03A 8EAC7298
5FBA57EC A38F96CF 18854EF3 B5BA8B81 CA969D41 1F894C93
4A034826 79827027 DF2D4932 168804F8 2FA3AE12 641D850B

Z is
43C96FD0 1E78BEBF 7A3394CA 9C61CDEC
27896216 55FDA3DF ADAFBDA7 B37CB00D E434D917 93C00ABA
7D93CF7E 2E47E9A4 9BCE9704 4FDAF332 AD4EEBA3 B047F557
F4074C33 52582BB7 C234E03A 8EAC7298 5FBA57EC A38F96CF
18854EF3 B5BA8B81 CA969D41 1F894C93 4A034826 79827027
DF2D4932 168804F8 2FA3AE12 641D850B 4963B3B5 F596751F
D360FFCA DD1178E3 15BC8C92 225361D6 920CD5C8 F1B01417
D86D43D2 CF2D1376 E32CB0DE 3D888912 0315BAE4 CB902D88
C8E4B634 70B4BD83 9D704E17 D9805DEE 10D3C927 EA605637
39F30B6C FD06AEAB 0AFED5D2 64ABFC1A 04530BCC 71C47958
FA2191C3 682C55AA E0B30B5A 44DBB431 FBC262D3 4B12DC9A

OtherInfo is
12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536

```
KDFval is
                                                              5E12
        13662D4E E074234B 060FA7A3 63F06A1F A9AE7A1F 438B15F9
        BAB055D0 F54959C5 96C588C5 6FA6F4ED 6EB23FA7 97E65D6D


MacData is
                 4B435F31 5F55414C 49434542 4F424259 934C1B90
        64E384DD F3DB7BCA 92EF41C1 7DB545FB AEB43977 094F49FD
        09F570DF D8DF7BCA E8CBC893 FBA990B5 437750AF 390EAC68
        2F358FEC 39A98504 0011E12F F3B6BA29 5A8A3245 7777E57A
        3E9C897D F022338F FF2969F0 67724BF4 AEA72B6B 6C0C3FCA
        6D2AB282 8F97D522 4C522EDB 2EA66475 5E772467 04696E88
        64931FFC 022317D7 3E524030 88978832 60503412 339FBB62


MacKey is
                                       5E12 13662D4E E074234B


Mtag is
                                       9058 3086CA3C 38B979C0


KeyData is
                           060FA7A3 63F06A1F A9AE7A1F 438B15F9
        BAB055D0 F54959C5 96C588C5 6FA6F4ED 6EB23FA7 97E65D6D




------------------------------------------------------------
Scheme Responder, Key Confirmation Provider: V to U
NonceU is
                 022317D7 3E524030 88978832 60503412 339FBB62


Zs is
                                              4963B3B5 F596751F
        D360FFCA DD1178E3 15BC8C92 225361D6 920CD5C8 F1B01417
        D86D43D2 CF2D1376 E32CB0DE 3D888912 0315BAE4 CB902D88
        C8E4B634 70B4BD83 9D704E17 D9805DEE 10D3C927 EA605637
        39F30B6C FD06AEAB 0AFED5D2 64ABFC1A 04530BCC 71C47958
        FA2191C3 682C55AA E0B30B5A 44DBB431 FBC262D3 4B12DC9A
```

Ze is
                                                43C96FD0 1E78BEBF
        7A3394CA 9C61CDEC 27896216 55FDA3DF ADAFBDA7 B37CB00D
        E434D917 93C00ABA 7D93CF7E 2E47E9A4 9BCE9704 4FDAF332
        AD4EEBA3 B047F557 F4074C33 52582BB7 C234E03A 8EAC7298
        5FBA57EC A38F96CF 18854EF3 B5BA8B81 CA969D41 1F894C93
        4A034826 79827027 DF2D4932 168804F8 2FA3AE12 641D850B

Z is
                            43C96FD0 1E78BEBF 7A3394CA 9C61CDEC
        27896216 55FDA3DF ADAFBDA7 B37CB00D E434D917 93C00ABA
        7D93CF7E 2E47E9A4 9BCE9704 4FDAF332 AD4EEBA3 B047F557
        F4074C33 52582BB7 C234E03A 8EAC7298 5FBA57EC A38F96CF
        18854EF3 B5BA8B81 CA969D41 1F894C93 4A034826 79827027
        DF2D4932 168804F8 2FA3AE12 641D850B 4963B3B5 F596751F
        D360FFCA DD1178E3 15BC8C92 225361D6 920CD5C8 F1B01417
        D86D43D2 CF2D1376 E32CB0DE 3D888912 0315BAE4 CB902D88
        C8E4B634 70B4BD83 9D704E17 D9805DEE 10D3C927 EA605637
        39F30B6C FD06AEAB 0AFED5D2 64ABFC1A 04530BCC 71C47958
        FA2191C3 682C55AA E0B30B5A 44DBB431 FBC262D3 4B12DC9A

OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536

KDFval is
                                                            5E12
        13662D4E E074234B 060FA7A3 63F06A1F A9AE7A1F 438B15F9
        BAB055D0 F54959C5 96C588C5 6FA6F4ED 6EB23FA7 97E65D6D

MacData is
        4B435F31 5F56424F 42425941 4C494345 934C1B90 64E384DD
        F3DB7BCA 92EF41C1 7DB545FB AEB43977 094F49FD 09F570DF
        D8DF7BCA E8CBC893 FBA990B5 437750AF 390EAC68 2F358FEC
        39A98504 0011E12F F3B6BA29 5A8A3245 7777E57A 3E9C897D
        F022338F FF2969F0 67724BF4 AEA72B6B 6C0C3FCA 6D2AB282
        8F97D522 4C522EDB 2EA66475 5E772467 04696E88 64931FFC

MacKey is
                                          5E12 13662D4E E074234B

Mtag is
                                    5558 21FF24B3 326523B4

KeyData is
                        060FA7A3 63F06A1F A9AE7A1F 438B15F9
        BAB055D0 F54959C5 96C588C5 6FA6F4ED 6EB23FA7 97E65D6D

Scheme Initiator, Key Confirmation Bilateral
NonceV is
                022317D7 3E524030 88978832 60503412 339FBB62

Zs is
                                                4963B3B5 F596751F
        D360FFCA DD1178E3 15BC8C92 225361D6 920CD5C8 F1B01417
        D86D43D2 CF2D1376 E32CB0DE 3D888912 0315BAE4 CB902D88
        C8E4B634 70B4BD83 9D704E17 D9805DEE 10D3C927 EA605637
        39F30B6C FD06AEAB 0AFED5D2 64ABFC1A 04530BCC 71C47958
        FA2191C3 682C55AA E0B30B5A 44DBB431 FBC262D3 4B12DC9A

Ze is
                                                43C96FD0 1E78BEBF
        7A3394CA 9C61CDEC 27896216 55FDA3DF ADAFBDA7 B37CB00D
        E434D917 93C00ABA 7D93CF7E 2E47E9A4 9BCE9704 4FDAF332
        AD4EEBA3 B047F557 F4074C33 52582BB7 C234E03A 8EAC7298
        5FBA57EC A38F96CF 18854EF3 B5BA8B81 CA969D41 1F894C93
        4A034826 79827027 DF2D4932 168804F8 2FA3AE12 641D850B

Z is
                        43C96FD0 1E78BEBF 7A3394CA 9C61CDEC
        27896216 55FDA3DF ADAFBDA7 B37CB00D E434D917 93C00ABA
        7D93CF7E 2E47E9A4 9BCE9704 4FDAF332 AD4EEBA3 B047F557
        F4074C33 52582BB7 C234E03A 8EAC7298 5FBA57EC A38F96CF
        18854EF3 B5BA8B81 CA969D41 1F894C93 4A034826 79827027
        DF2D4932 168804F8 2FA3AE12 641D850B 4963B3B5 F596751F
        D360FFCA DD1178E3 15BC8C92 225361D6 920CD5C8 F1B01417
        D86D43D2 CF2D1376 E32CB0DE 3D888912 0315BAE4 CB902D88
        C8E4B634 70B4BD83 9D704E17 D9805DEE 10D3C927 EA605637

```
        39F30B6C FD06AEAB 0AFED5D2 64ABFC1A 04530BCC 71C47958
        FA2191C3 682C55AA E0B30B5A 44DBB431 FBC262D3 4B12DC9A


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


KDFval is
                                                            5E12
        13662D4E E074234B 060FA7A3 63F06A1F A9AE7A1F 438B15F9
        BAB055D0 F54959C5 96C588C5 6FA6F4ED 6EB23FA7 97E65D6D


U2V
----------------
MacData is
                 4B435F32 5F55414C 49434542 4F424259 934C1B90
        64E384DD F3DB7BCA 92EF41C1 7DB545FB AEB43977 094F49FD
        09F570DF D8DF7BCA E8CBC893 FBA990B5 437750AF 390EAC68
        2F358FEC 39A98504 0011E12F F3B6BA29 5A8A3245 7777E57A
        3E9C897D F022338F FF2969F0 67724BF4 AEA72B6B 6C0C3FCA
        6D2AB282 8F97D522 4C522EDB 2EA66475 5E772467 04696E88
        64931FFC 022317D7 3E524030 88978832 60503412 339FBB62


MacKey is
                                        5E12 13662D4E E074234B


Mtag is
                                        89F8 E349BE32 6DAD0F5A


V2U
----------------
MacData is
                 4B435F32 5F56424F 42425941 4C494345 022317D7
        3E524030 88978832 60503412 339FBB62 934C1B90 64E384DD
        F3DB7BCA 92EF41C1 7DB545FB AEB43977 094F49FD 09F570DF
        D8DF7BCA E8CBC893 FBA990B5 437750AF 390EAC68 2F358FEC
        39A98504 0011E12F F3B6BA29 5A8A3245 7777E57A 3E9C897D
        F022338F FF2969F0 67724BF4 AEA72B6B 6C0C3FCA 6D2AB282
        8F97D522 4C522EDB 2EA66475 5E772467 04696E88 64931FFC
```

MacKey is
                                        5E12 13662D4E E074234B

Mtag is
                                        1BEE FD3B730A 077D8716

KeyData is
                          060FA7A3 63F06A1F A9AE7A1F 438B15F9
        BAB055D0 F54959C5 96C588C5 6FA6F4ED 6EB23FA7 97E65D6D

==========

MQV1(160)
----
xU is
                B515A4C2 98A6EE82 2E38FEF1 28BCB86D 8821EF07

yU is
                                                3BCE0DC6 11FA403D
        65C63A16 8898F3B9 E1DD0CE2 B499B5BB 392645E5 5505B4B6
        1324CA27 8BF01D83 639D5CD4 84100247 4AE292CD 3009F8DC
        C437006D B18159BE 62B5F91A 87172657 F67F9AD9 88343543
        603D2410 A9755B25 95D11523 ACC58675 A90CE0FC B2350790
        2F043D04 95B0175E 1F124A6B E22127D9 103E3155 8ADDE02A

xV is
                D7ABD322 836EE57F E8F5E8C0 E8089927 B8784F3F

yV is
                                                000F75DD BC54E220
        6BF316B5 7042511F C98F8E33 1DB57C82 3E84351A E55F7CB0
        309E6F49 340DE8E9 157B6152 808982B7 2B178CEE 1C27D303
        6F7B9386 EFC0B9CC F6E09E6A 223DDF14 3637C3FB 37BCB44B
        A50DF56D C6500E20 C4A0C5BA 69338DA6 903F9CBA 33B6BC5F
        072AF0D0 73DA2999 1086924A 6E38EFCE 281F2407 F24D79E5

rU is
                79AF360A 7ECD013B 0CAF3E59 69368F99 354E8A9B

```
tU is
                                                1B7A300C 73871A6F
        E15296FC 2FA46B00 7194BDD9 8202CD00 ACDDE2B6 27AEEC96
        77B4873E 097011E7 CC5587A1 A07160AE 5787421C E265FEE2
        B8110052 441B8242 5D2B0F56 7030355B 7D95E68B B188F002
        9BC087A4 A9434520 A39FA96D 5BAA6F10 A2E0EB98 C34EBE0E
        3D2B1B3E 05F7D4F9 0ED4C673 5429BE02 774BDDA2 50D77663



------------------------------------------------------------
no Key Confirmation
Z is
                                                2C1520E9 F6E64010
        6D0A271E D122E2CA EC3F1FCD AF7F86EE A7885668 140F3DD7
        11138E51 690E250B 36F364E1 2D28693B 67ACDC8B 29272DD5
        6C5ABF72 5D3F8759 85BBF6E9 36AC9AB7 6A079728 61546608
        0B2F256B AC34FF06 A8A98A51 39010A55 8144921D 9A9D59DD
        4F40F921 7121A0C4 B55CFC1D 34EA5145 A409A12D 559E8D9F


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


KDFval is
                         EFF113B5 8CD39487 3456BABA C5FD08B7
        AE45E3FA AEE7A7ED 0139C888 90982DA3 1A4BDF0E 920D1874


KeyData is
                         EFF113B5 8CD39487 3456BABA C5FD08B7
        AE45E3FA AEE7A7ED 0139C888 90982DA3 1A4BDF0E 920D1874



------------------------------------------------------------
Scheme Initiator, Key Confirmation Provider: U to V
NonceV is
                EB36943A 9E86D81E CCFF2B87 0B2D42EF 8BCC96F4
```

Z is
                                                2C1520E9 F6E64010
        6D0A271E D122E2CA EC3F1FCD AF7F86EE A7885668 140F3DD7
        11138E51 690E250B 36F364E1 2D28693B 67ACDC8B 29272DD5
        6C5ABF72 5D3F8759 85BBF6E9 36AC9AB7 6A079728 61546608
        0B2F256B AC34FF06 A8A98A51 39010A55 8144921D 9A9D59DD
        4F40F921 7121A0C4 B55CFC1D 34EA5145 A409A12D 559E8D9F

OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536

KDFval is
                                                            EFF1
        13B58CD3 94873456 BABAC5FD 08B7AE45 E3FAAEE7 A7ED0139
        C8889098 2DA31A4B DF0E920D 187441A8 3FC26D36 C5E31B87

MacData is
                 4B435F31 5F55414C 49434542 4F424259 1B7A300C
        73871A6F E15296FC 2FA46B00 7194BDD9 8202CD00 ACDDE2B6
        27AEEC96 77B4873E 097011E7 CC5587A1 A07160AE 5787421C
        E265FEE2 B8110052 441B8242 5D2B0F56 7030355B 7D95E68B
        B188F002 9BC087A4 A9434520 A39FA96D 5BAA6F10 A2E0EB98
        C34EBE0E 3D2B1B3E 05F7D4F9 0ED4C673 5429BE02 774BDDA2
        50D77663 EB36943A 9E86D81E CCFF2B87 0B2D42EF 8BCC96F4

MacKey is
                                        EFF1 13B58CD3 94873456

Mtag is
                                        930C C0BBE3FA A7FB9EAF

KeyData is
                            BABAC5FD 08B7AE45 E3FAAEE7 A7ED0139
        C8889098 2DA31A4B DF0E920D 187441A8 3FC26D36 C5E31B87

Scheme Responder, Key Confirmation Provider: V to U

NonceU is
EB36943A 9E86D81E CCFF2B87 0B2D42EF 8BCC96F4

Z is
2C1520E9 F6E64010
6D0A271E D122E2CA EC3F1FCD AF7F86EE A7885668 140F3DD7
11138E51 690E250B 36F364E1 2D28693B 67ACDC8B 29272DD5
6C5ABF72 5D3F8759 85BBF6E9 36AC9AB7 6A079728 61546608
0B2F256B AC34FF06 A8A98A51 39010A55 8144921D 9A9D59DD
4F40F921 7121A0C4 B55CFC1D 34EA5145 A409A12D 559E8D9F

OtherInfo is
12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536

KDFval is
EFF1
13B58CD3 94873456 BABAC5FD 08B7AE45 E3FAAEE7 A7ED0139
C8889098 2DA31A4B DF0E920D 187441A8 3FC26D36 C5E31B87

MacData is
4B435F31 5F56424F 42425941 4C494345 1B7A300C 73871A6F
E15296FC 2FA46B00 7194BDD9 8202CD00 ACDDE2B6 27AEEC96
77B4873E 097011E7 CC5587A1 A07160AE 5787421C E265FEE2
B8110052 441B8242 5D2B0F56 7030355B 7D95E68B B188F002
9BC087A4 A9434520 A39FA96D 5BAA6F10 A2E0EB98 C34EBE0E
3D2B1B3E 05F7D4F9 0ED4C673 5429BE02 774BDDA2 50D77663

MacKey is
EFF1 13B58CD3 94873456

Mtag is
A591 EF9E20BC 814EC98A

KeyData is
BABAC5FD 08B7AE45 E3FAAEE7 A7ED0139
C8889098 2DA31A4B DF0E920D 187441A8 3FC26D36 C5E31B87

```
------------------------------------------------------------
Scheme Initiator, Key Confirmation Bilateral
NonceV is
                EB36943A 9E86D81E CCFF2B87 0B2D42EF 8BCC96F4


Z is
                                           2C1520E9 F6E64010
        6D0A271E D122E2CA EC3F1FCD AF7F86EE A7885668 140F3DD7
        11138E51 690E250B 36F364E1 2D28693B 67ACDC8B 29272DD5
        6C5ABF72 5D3F8759 85BBF6E9 36AC9AB7 6A079728 61546608
        0B2F256B AC34FF06 A8A98A51 39010A55 8144921D 9A9D59DD
        4F40F921 7121A0C4 B55CFC1D 34EA5145 A409A12D 559E8D9F


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


KDFval is
                                                       EFF1
        13B58CD3 94873456 BABAC5FD 08B7AE45 E3FAAEE7 A7ED0139
        C8889098 2DA31A4B DF0E920D 187441A8 3FC26D36 C5E31B87


U2V
----------------
MacData is
                4B435F32 5F55414C 49434542 4F424259 1B7A300C
        73871A6F E15296FC 2FA46B00 7194BDD9 8202CD00 ACDDE2B6
        27AEEC96 77B4873E 097011E7 CC5587A1 A07160AE 5787421C
        E265FEE2 B8110052 441B8242 5D2B0F56 7030355B 7D95E68B
        B188F002 9BC087A4 A9434520 A39FA96D 5BAA6F10 A2E0EB98
        C34EBE0E 3D2B1B3E 05F7D4F9 0ED4C673 5429BE02 774BDDA2
        50D77663 EB36943A 9E86D81E CCFF2B87 0B2D42EF 8BCC96F4


MacKey is
                                      EFF1 13B58CD3 94873456


Mtag is
                                      2B7B C781436C CB534414
```

```
V2U
----------------
MacData is
                 4B435F32 5F56424F 42425941 4C494345 EB36943A
        9E86D81E CCFF2B87 0B2D42EF 8BCC96F4 1B7A300C 73871A6F
        E15296FC 2FA46B00 7194BDD9 8202CD00 ACDDE2B6 27AEEC96
        77B4873E 097011E7 CC5587A1 A07160AE 5787421C E265FEE2
        B8110052 441B8242 5D2B0F56 7030355B 7D95E68B B188F002
        9BC087A4 A9434520 A39FA96D 5BAA6F10 A2E0EB98 C34EBE0E
        3D2B1B3E 05F7D4F9 0ED4C673 5429BE02 774BDDA2 50D77663


MacKey is
                                        EFF1 13B58CD3 94873456


Mtag is
                                        E816 0B80D361 4AB0441B


KeyData is
                         BABAC5FD 08B7AE45 E3FAAEE7 A7ED0139
        C8889098 2DA31A4B DF0E920D 187441A8 3FC26D36 C5E31B87


================================================================


dhOneFlow(160)
----------------------------------------------------------
xV is
                 E528FA84 60B15299 8E831CC6 CCAFD479 C6BA1E69


yV is
                                                A813FAB0 D6ED8CFD
        6F537B8B 0889C6D2 1628390B 207C0B44 5950BEC9 33F1DDE5
        1C89C244 B55F0777 0E0D3DB7 F9439E36 0ADFA9CB 9D9498C7
        01E82A1E 7F882AE3 DB8CF53A 6E5B6D9D AD68EA5D D7784E73
        04E57990 D5E998CF 708CC45C 6A1DF607 0ADE2E4B D13B6C65
        8E879FF1 63479AE2 B013B5C5 2EE840E1 AF510187 97DD2F49


rU is
                 CE8F98BF 078C7BC6 AD2D47AA AB922027 C1DA13B0
```

```
tU is
                                                A52A62D3 6F8F3A6E
        9EDB1D32 10764148 56131945 0A74AE11 2E828AD8 64E92E6F
        6D85F037 547B9DC7 62204A74 7408F792 2246A5E0 971A4E58
        B4E3678A 6348D15D DA9FF4E8 7900CE9C 041623C4 F6CB4A7B
        B256181F A6666ACA 814C7C45 F15A31DA 137D222B EA166A06
        F7D78D47 64871B0F 083366C8 9573D42D 60115168 9DB31D3A



------------------------------------------------------------
no Key Confirmation
Z is
                                                1477FFC2 6CF71C25
        76DDDCD7 7A058DAE 07F2973A 080540AC 2F00B330 E4AE17C0
        D514AA06 F831E273 D257C031 424111A7 9312C6F5 85893EA8
        8748D903 516D592F 00B594E8 D51D39BE C98A2161 67265EA1
        D3807333 E709C2F7 F372D747 FBF4F6AD 4574D682 840ECFF4
        7BD27116 987FDB7D 1B26E5F6 BA894663 02496D6C CD785D9B


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


KDFval is
                         A40564E2 72BEFDF7 0BF49068 1EDC2F26
        0139E7D5 0EAFD9C1 3FA905E2 7EDFC8F0 72CADDEC ECAA17DF


KeyData is
                         A40564E2 72BEFDF7 0BF49068 1EDC2F26
        0139E7D5 0EAFD9C1 3FA905E2 7EDFC8F0 72CADDEC ECAA17DF



------------------------------------------------------------
Scheme Responder, Key Confirmation Provider: V to U
Z is
                                                1477FFC2 6CF71C25
        76DDDCD7 7A058DAE 07F2973A 080540AC 2F00B330 E4AE17C0
        D514AA06 F831E273 D257C031 424111A7 9312C6F5 85893EA8
        8748D903 516D592F 00B594E8 D51D39BE C98A2161 67265EA1
```

```
        D3807333 E709C2F7 F372D747 FBF4F6AD 4574D682 840ECFF4
        7BD27116 987FDB7D 1B26E5F6 BA894663 02496D6C CD785D9B


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


KDFval is
                                                          A405
        64E272BE FDF70BF4 90681EDC 2F260139 E7D50EAF D9C13FA9
        05E27EDF C8F072CA DDECECAA 17DFA1CB DF456074 840F16C3


MacData is
        4B435F31 5F56424F 42425941 4C494345 A52A62D3 6F8F3A6E
        9EDB1D32 10764148 56131945 0A74AE11 2E828AD8 64E92E6F
        6D85F037 547B9DC7 62204A74 7408F792 2246A5E0 971A4E58
        B4E3678A 6348D15D DA9FF4E8 7900CE9C 041623C4 F6CB4A7B
        B256181F A6666ACA 814C7C45 F15A31DA 137D222B EA166A06
        F7D78D47 64871B0F 083366C8 9573D42D 60115168 9DB31D3A


MacKey is
                                      A405 64E272BE FDF70BF4


Mtag is
                                      1345 2B4AE564 57DD81A2


KeyData is
                           90681EDC 2F260139 E7D50EAF D9C13FA9
        05E27EDF C8F072CA DDECECAA 17DFA1CB DF456074 840F16C3


============================================================


dhStatic(160)
------------------------------------------------------------
xU is
                 31636705 CBDF6631 7192DEE2 AF8E0AD8 6E98106A


yU is
```

```
                                                1239098F E47C411C
        F7C81737 0606C1A5 2AE7EB47 11483B07 890958F3 265D0351
        4AE9F736 D7DCBE26 6C33AE43 5E1C9053 EE4AB285 A67A76BC
        C6DA61CF 35CED654 2C26F1C3 42EEBF79 27D68DE2 DB53A2A8
        05E8D3D9 124CB84D C453A363 30AE0AC5 08AF3C33 CBEFBA5B
        86EEBBDF 029BCB7C D37F97B3 7AD7F641 A1C16AA6 1936EFC4


xV is
                1FDE83F3 D2A9513D A438C170 D4E89BAE 1CD3D97D


yV is
                                                44986C33 F7F9FC1E
        60CB1340 E043C63D B6D5CABC E861A056 3DC1D498 CC37F9D7
        97B001E2 AAE29C40 F41C0C51 7CA23CB3 0ABC79C3 4710BAE3
        48A5B2A7 EFD238C2 8EF97DCB A687443F A72AC9A0 A12006BF
        3ECF170E 7A533A0C 2BBF0BEB BD8F52E8 BF7F356B 44266025
        98DE34FD 135517BE D78C270D 3EA9BA26 78EC9696 AEF8A10C




------------------------------------------------------------
no Key Confirmation
NonceU is
                D1F6B3AD 0294B18A FF5824CD 604EC87B 15E8CB0F


Z is
                                                44440BB1 5487FDD1
        66ACD88F 77A4C7FD 23D7F71B 8BCF72B1 701A6D9F E79B542F
        AAD6EE7B 3C5F88DD EFA6500F D83BFCCA C47DE9A7 C659189C
        59B27905 708F5CBA 5FA4AD2F 59A9B05F 461B8D8D D48B468D
        0A9A43B3 4B5CC6BB 9CAFBBED C6D01880 F34FDCEE E5033E7E
        67427CFA F4B9DFA3 9F140F32 71C78B42 8A11B18C A207F191


OtherInfo is
            1234 56789ABC DEF0414C 49434531 32330014 D1F6B3AD
        0294B18A FF5824CD 604EC87B 15E8CB0F 424F4242 59343536


KDFval is
                            C98D510B F17E524E 2F02C54E 445B563E
        AEEB2392 DD31239E 436335F6 62C04D19 EC051118 E5B3DAEA
```

```
KeyData is
                         C98D510B F17E524E 2F02C54E 445B563E
        AEEB2392 DD31239E 436335F6 62C04D19 EC051118 E5B3DAEA



------------------------------------------------------------
Scheme Initiator, Key Confirmation Provider: U to V
NonceU is
                D1F6B3AD 0294B18A FF5824CD 604EC87B 15E8CB0F


NonceV is
                0BE12640 844801F5 51D2CABB 1B591B3F DB3762C8


Z is
                                            44440BB1 5487FDD1
        66ACD88F 77A4C7FD 23D7F71B 8BCF72B1 701A6D9F E79B542F
        AAD6EE7B 3C5F88DD EFA6500F D83BFCCA C47DE9A7 C659189C
        59B27905 708F5CBA 5FA4AD2F 59A9B05F 461B8D8D D48B468D
        0A9A43B3 4B5CC6BB 9CAFBBED C6D01880 F34FDCEE E5033E7E
        67427CFA F4B9DFA3 9F140F32 71C78B42 8A11B18C A207F191


OtherInfo is
            1234 56789ABC DEF0414C 49434531 32330014 D1F6B3AD
        0294B18A FF5824CD 604EC87B 15E8CB0F 424F4242 59343536


KDFval is
                                                      C98D
        510BF17E 524E2F02 C54E445B 563EAEEB 2392DD31 239E4363
        35F662C0 4D19EC05 1118E5B3 DAEAE2BE 4AF13B7D ABA1D36E


MacData is
                                            4B435F31 5F55414C
        49434542 4F424259 D1F6B3AD 0294B18A FF5824CD 604EC87B
        15E8CB0F 0BE12640 844801F5 51D2CABB 1B591B3F DB3762C8


MacKey is
```

```
                                        C98D 510BF17E 524E2F02


Mtag is
                                        B2CA 1F0037A8 581017EF


KeyData is
                            C54E445B 563EAEEB 2392DD31 239E4363
        35F662C0 4D19EC05 1118E5B3 DAEAE2BE 4AF13B7D ABA1D36E




------------------------------------------------------------
Scheme Responder, Key Confirmation Provider: V to U
NonceV is
                0BE12640 844801F5 51D2CABB 1B591B3F DB3762C8


NonceU is
                D1F6B3AD 0294B18A FF5824CD 604EC87B 15E8CB0F


Z is
                                                44440BB1 5487FDD1
        66ACD88F 77A4C7FD 23D7F71B 8BCF72B1 701A6D9F E79B542F
        AAD6EE7B 3C5F88DD EFA6500F D83BFCCA C47DE9A7 C659189C
        59B27905 708F5CBA 5FA4AD2F 59A9B05F 461B8D8D D48B468D
        0A9A43B3 4B5CC6BB 9CAFBBED C6D01880 F34FDCEE E5033E7E
        67427CFA F4B9DFA3 9F140F32 71C78B42 8A11B18C A207F191


OtherInfo is
            1234 56789ABC DEF0414C 49434531 32330014 D1F6B3AD
        0294B18A FF5824CD 604EC87B 15E8CB0F 424F4242 59343536


KDFval is
                                                        C98D
        510BF17E 524E2F02 C54E445B 563EAEEB 2392DD31 239E4363
        35F662C0 4D19EC05 1118E5B3 DAEAE2BE 4AF13B7D ABA1D36E


MacData is
                                    4B435F31 5F56424F 42425941
```

4C494345 D1F6B3AD 0294B18A FF5824CD 604EC87B 15E8CB0F

MacKey is
C98D 510BF17E 524E2F02

Mtag is
65F2 76C0AF47 7EFB7FAD

KeyData is
C54E445B 563EAEEB 2392DD31 239E4363
35F662C0 4D19EC05 1118E5B3 DAEAE2BE 4AF13B7D ABA1D36E

Scheme Initiator, Key Confirmation Bilateral
NonceU is
D1F6B3AD 0294B18A FF5824CD 604EC87B 15E8CB0F

NonceV is
0BE12640 844801F5 51D2CABB 1B591B3F DB3762C8

Z is
44440BB1 5487FDD1
66ACD88F 77A4C7FD 23D7F71B 8BCF72B1 701A6D9F E79B542F
AAD6EE7B 3C5F88DD EFA6500F D83BFCCA C47DE9A7 C659189C
59B27905 708F5CBA 5FA4AD2F 59A9B05F 461B8D8D D48B468D
0A9A43B3 4B5CC6BB 9CAFBBED C6D01880 F34FDCEE E5033E7E
67427CFA F4B9DFA3 9F140F32 71C78B42 8A11B18C A207F191

OtherInfo is
1234 56789ABC DEF0414C 49434531 32330014 D1F6B3AD
0294B18A FF5824CD 604EC87B 15E8CB0F 424F4242 59343536

KDFval is
C98D
510BF17E 524E2F02 C54E445B 563EAEEB 2392DD31 239E4363
35F662C0 4D19EC05 1118E5B3 DAEAE2BE 4AF13B7D ABA1D36E

```
U2V
----------------
MacData is
                                              4B435F32 5F55414C
        49434542 4F424259 D1F6B3AD 0294B18A FF5824CD 604EC87B
        15E8CB0F 0BE12640 844801F5 51D2CABB 1B591B3F DB3762C8


MacKey is
                                       C98D 510BF17E 524E2F02


Mtag is
                                       F0E7 A1163D4E A1361B3A


V2U
----------------
MacData is
                                              4B435F32 5F56424F
        42425941 4C494345 0BE12640 844801F5 51D2CABB 1B591B3F
        DB3762C8 D1F6B3AD 0294B18A FF5824CD 604EC87B 15E8CB0F


MacKey is
                                       C98D 510BF17E 524E2F02


Mtag is
                                       266C 363418F3 6EDC710D


KeyData is
                          C54E445B 563EAEEB 2392DD31 239E4363
        35F662C0 4D19EC05 1118E5B3 DAEAE2BE 4AF13B7D ABA1D36E
```

```
#############################################################

Key Establishment Schemes for Finite Field Cryptography
plen: 2048
qlen: 224
Hash algorithm used: SHA-224
KDF: Contatenation KDF
DKM len: 448
MacKey length: 112
MacTag len: 112
ID_U: "ALICE"
ID_V: "BOBBY"

P is
                        AD107E1E 9123A9D0 D660FAA7 9559C51F
        A20D64E5 683B9FD1 B54B1597 B61D0A75 E6FA141D F95A56DB
        AF9A3C40 7BA1DF15 EB3D688A 309C180E 1DE6B85A 1274A0A6
        6D3F8152 AD6AC212 9037C9ED EFDA4DF8 D91E8FEF 55B7394B
        7AD5B7D0 B6C12207 C9F98D11 ED34DBF6 C6BA0B2C 8BBC27BE
        6A00E0A0 B9C49708 B3BF8A31 70918836 81286130 BC8985DB
        1602E714 415D9330 278273C7 DE31EFDC 7310F712 1FD5A074
        15987D9A DC0A486D CDF93ACC 44328387 315D75E1 98C641A4
        80CD86A1 B9E587E8 BE60E69C C928B2B9 C52172E4 13042E9B
        23F10B0E 16E79763 C9B53DCF 4BA80A29 E3FB73C1 6B8E75B9
        7EF363E2 FFA31F71 CF9DE538 4E71B81C 0AC4DFFE 0C10E64F


Q is
                                                    801C0D34
        C58D93FE 99717710 1F80535A 4738CEBC BF389A99 B36371EB


G is
                        AC4032EF 4F2D9AE3 9DF30B5C 8FFDAC50
        6CDEBE7B 89998CAF 74866A08 CFE4FFE3 A6824A4E 10B9A6F0
        DD921F01 A70C4AFA AB739D77 00C29F52 C57DB17C 620A8652
        BE5E9001 A8D66AD7 C1766910 1999024A F4D02727 5AC1348B
        B8A762D0 521BC98A E2471504 22EA1ED4 09939D54 DA7460CD
        B5F6C6B2 50717CBE F180EB34 118E98D1 19529A45 D6F83456
        6E3025E3 16A330EF BB77A86F 0C1AB15B 051AE3D4 28C8F8AC
        B70A8137 150B8EEB 10E183ED D19963DD D9E263E4 770589EF
        6AA21E7F 5F2FF381 B539CCE3 409D13CD 566AFBB4 8D6C0191
        81E1BCFE 94B30269 EDFE72FE 9B6AA4BD 7B5A0F1C 71CFFF4C
        19C418E1 F6EC0179 81BC087F 2A7065B3 84B890D3 191F2BFA
```

```
################################################################


dhHybrid1(224)
----------------------------------------------------------------
xU is
                                                        0D8A6270
        3F144F1A 1B1CC187 E8097F35 EA469D45 28D49B80 39A98C4E


yU is
                         7690757B 2E775434 D0057E3F 69081D96
        3B8FC229 5520C8FE 3FFF5C0A 09AAB1EC 7FB76BC5 B5EDF2EB
        749C71C4 2FE6C1E1 BE5ABFA5 E9D8F0F7 47E336C3 29CF2467
        809B4435 132E99C0 9FAD924E 804F0E6C 248FD1BC 55A0F81E
        D6839D3B 8DC14B32 48E184C7 95CFAA3E 443F83FA 3D76A26C
        D50FD9FB FA232678 D1F64D34 91BD79D3 180FD256 A7931B39
        373AB231 78A3939C 645A4BE8 B80D882B 8C968BC7 45300EBB
        554A920F 1309C5B3 7D8709FC AE0AC8F5 A9336E20 38C401D5
        93162664 C16561D8 1D6B9076 9A954DEC FA18D2AA 25FEDBDC
        8E952F5A EA073656 79722A70 2D192EE0 F8D8FE24 734EA590
        1466A824 6F87CCC5 6D117567 EF00F883 B0ACE979 E57F2A90


xV is
                                                        4913C204
        5FFD92B2 DB364623 DF125B0A 37463D46 D1D6D57D BFDEADBC


yV is
                         8F59EDE9 D9A5A681 7D95671B 8622D089
        D31A817A 927ABE58 C585D8F3 ACBAFF62 B79EE8DC 4ADD2E49
        F4E07CFE 9037E2F6 3841E9FE 52C6B3BE C79D163C 66C1074F
        8E7F1256 EEA5C044 EBEAF233 638F7AED 65E3FD7C A062F983
        7E29E6F2 86BA6F3C 4DD6DA53 6A9AAAFE 80AB7D02 84625699
        757A2FD1 08FCF8AD 692F4D9C EEEECCDC 5DD1E105 A500DD10
        EEF769E3 A8007660 A90A4901 816C215C 0A8133AA 84C6FA08
        F113C983 0D89BFCD 36372FCE 09DCCA8E BA26DFD9 0B3A2253
        45B2D851 8C71349F 6A12E961 8CC273FD 0D8BDF63 29B42D61
        F02815BC 714D164F 318AF35E A9FEEB11 3A7376A7 71B34017
        B358672A 275BD504 C2EBBD6C 39C618E8 88FA09D4 094B2B52


rU is
                                                        28E3323B
```

6D361E41 050B8487 3D48FF88 C6C250A1 C3896228 6FE90E4E

tU is
3DB2F114 B59BF6D9 9458F3F6 BE6072B0
106ED031 25BFF741 FF8BDC96 D0C541AF AB1DF7AB 694F77CB
962D0AB7 435B1A3A 8E93AE97 F182606D 3CE9DCA3 A6F00EBD
6C47D81D 6AD58008 49490CAF C34A9C8D D6D7EDA8 03A96614
25637D99 84075711 2FBC01DF 76D83F99 E3E97EF9 9090596A
1287BB2E 0B00911F E27FFBD2 87C5D024 5AE8631C D9C8A10E
E236BF8A F5E0CE4E D27DE78D 12206A15 AEF1AAA6 951247B1
525F3E94 4743C5CD 4B13D244 A1644C09 A2697ED0 8714416E
7FF1BD24 D3151A7B 797C368C A7D14D9D 1975CB3A 065CAE9D
89A26E39 BD698089 51786674 BA9711E0 DED299CA 06B9B90E
A02B6A8B C0BAAE9F B6AA5A89 3436B9CD 14CCD6FF 365E6F68

rV is
574914DA
B9035611 941E52BE 30725480 51CF3F15 23D5BBE0 3511EBB1

tV is
7F6CB1D0 F8F22C63 BA888121 41F5D895
BB92301D BF843F29 2A67B862 A60A568C 7719D90C 529CE89A
78B3A8E1 EB18DDCB 30BBD675 9251F33E 46A98B97 84D392B6
A3B73F49 71F3D939 0E27EAC8 28006098 1FC3876F 83C3B99D
CD71EB2D B4CC9AC3 24AD405C A0DC2692 C05D9363 D4B65F68
C2C9D8D8 F674D09D EB19A933 2D5A9FE0 CB77E949 271B8BD7
4A1AEC9D 79DF7493 FB860673 9B586A81 C8FFED24 2A94C1A7
669CCF40 34AB3852 82610EF4 687E887E EB640CDC 48C42BDF
F192AB2E C3B4F93D 0152307D 00A12FD3 6FF10FDD B7275FDE
75C6814D 963FB5E6 E3204025 86FCB749 260D7918 08D12589
39D0690A 9ECE0CD5 7A5C4C16 B58B242C A724CD15 8AF16C49

---
no Key Confirmation
Zs is
2458D1C0 CA244341 0CF3B47C 0C254C7D
C8ECB43E 6C2364E1 C06219CC 7EFBFFBB 63D7FFFC 745812FD
240C33D4 96B9992F 9680A63C 07963C0C 49F3C1BA EFECAF32
E2AA8A2F 7CD30D8F 051EE2F5 0FBF05AB 1396A4EA 87447D7B
981B5E46 14281871 A6F0F6BF 1FE0022F 7EA132BE 0AE91926

AB12AF6D C45064AA D56B84B9 0C700837 09CFF7E3 1B548FB7
FB2CF75A BF96E01C CD3E942E ED91480D 4C24C6B7 F979FBBE
5DA239B3 76167D68 573524FF CB509954 CC80A0E1 A71C40C4
DA17B8D1 572B2158 7A8D66CC 621C7CD1 0F49ABD5 EF863113
E6192108 6FAC2531 2B741C11 A8FBC1E3 3C34D9DA 14A82247
7FCC3666 7025C4F1 30AE100E 36F15DA0 0374CE87 41679F61

Ze is

8C5D6E5D 360683BA 55B09DB1 696D7C64
02FF8788 5FF50770 F2767B75 5460207E D5C743FD 27E7EB1D
0CA591F8 56389311 730744F2 04D2E55B 8BD446CE CA031F7B
ACCFF1A7 1B683459 CC54D501 DABF4A84 CDB86DFA DAFF310F
BDBAF74D D51BA1E1 E1191AF1 4C9BF894 43BF588E 9CE33034
AF5E89BF 6FFC47D7 D9CA4A5E 8FF8A050 20BB0F95 BCDE0156
D87FB860 BD4083FA 5B531A08 A4FB7EE0 201AE8B3 CCFFE99F
270BC353 4BAACFC0 01CDD80A D87CCE71 F091E766 CA5CC275
CB49145A 5EE6162E CCF558CE C4D3EE53 1E91E9A5 2969634D
3AF8D26F 8D15DC0D 6F6E0A97 4BE4341B 68A01990 DBB86495
891AD3AF C1E4CEDF 4C6AE1F1 CD6081CD EED8E6B3 264EC3BE

Z is

8C5D6E5D 360683BA
55B09DB1 696D7C64 02FF8788 5FF50770 F2767B75 5460207E
D5C743FD 27E7EB1D 0CA591F8 56389311 730744F2 04D2E55B
8BD446CE CA031F7B ACCFF1A7 1B683459 CC54D501 DABF4A84
CDB86DFA DAFF310F BDBAF74D D51BA1E1 E1191AF1 4C9BF894
43BF588E 9CE33034 AF5E89BF 6FFC47D7 D9CA4A5E 8FF8A050
20BB0F95 BCDE0156 D87FB860 BD4083FA 5B531A08 A4FB7EE0
201AE8B3 CCFFE99F 270BC353 4BAACFC0 01CDD80A D87CCE71
F091E766 CA5CC275 CB49145A 5EE6162E CCF558CE C4D3EE53
1E91E9A5 2969634D 3AF8D26F 8D15DC0D 6F6E0A97 4BE4341B
68A01990 DBB86495 891AD3AF C1E4CEDF 4C6AE1F1 CD6081CD
EED8E6B3 264EC3BE 2458D1C0 CA244341 0CF3B47C 0C254C7D
C8ECB43E 6C2364E1 C06219CC 7EFBFFBB 63D7FFFC 745812FD
240C33D4 96B9992F 9680A63C 07963C0C 49F3C1BA EFECAF32
E2AA8A2F 7CD30D8F 051EE2F5 0FBF05AB 1396A4EA 87447D7B
981B5E46 14281871 A6F0F6BF 1FE0022F 7EA132BE 0AE91926
AB12AF6D C45064AA D56B84B9 0C700837 09CFF7E3 1B548FB7
FB2CF75A BF96E01C CD3E942E ED91480D 4C24C6B7 F979FBBE
5DA239B3 76167D68 573524FF CB509954 CC80A0E1 A71C40C4
DA17B8D1 572B2158 7A8D66CC 621C7CD1 0F49ABD5 EF863113
E6192108 6FAC2531 2B741C11 A8FBC1E3 3C34D9DA 14A82247
7FCC3666 7025C4F1 30AE100E 36F15DA0 0374CE87 41679F61

```
OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


KeyData is
                                                4B996A60 C04A35C5
        E6D474B1 0A258D56 2EA6DC52 F6C69BF3 9EF88C89 E3CC8A54
        DA2F3C0B 561B53FE 76551363 D69C3CEF 74E34FE8 8EB3AC51




------------------------------------------------------------
Scheme Initiator, Key Confirmation Provider: U to V
Zs is
                        2458D1C0 CA244341 0CF3B47C 0C254C7D
        C8ECB43E 6C2364E1 C06219CC 7EFBFFBB 63D7FFFC 745812FD
        240C33D4 96B9992F 9680A63C 07963C0C 49F3C1BA EFECAF32
        E2AA8A2F 7CD30D8F 051EE2F5 0FBF05AB 1396A4EA 87447D7B
        981B5E46 14281871 A6F0F6BF 1FE0022F 7EA132BE 0AE91926
        AB12AF6D C45064AA D56B84B9 0C700837 09CFF7E3 1B548FB7
        FB2CF75A BF96E01C CD3E942E ED91480D 4C24C6B7 F979FBBE
        5DA239B3 76167D68 573524FF CB509954 CC80A0E1 A71C40C4
        DA17B8D1 572B2158 7A8D66CC 621C7CD1 0F49ABD5 EF863113
        E6192108 6FAC2531 2B741C11 A8FBC1E3 3C34D9DA 14A82247
        7FCC3666 7025C4F1 30AE100E 36F15DA0 0374CE87 41679F61


Ze is
                        8C5D6E5D 360683BA 55B09DB1 696D7C64
        02FF8788 5FF50770 F2767B75 5460207E D5C743FD 27E7EB1D
        0CA591F8 56389311 730744F2 04D2E55B 8BD446CE CA031F7B
        ACCFF1A7 1B683459 CC54D501 DABF4A84 CDB86DFA DAFF310F
        BDBAF74D D51BA1E1 E1191AF1 4C9BF894 43BF588E 9CE33034
        AF5E89BF 6FFC47D7 D9CA4A5E 8FF8A050 20BB0F95 BCDE0156
        D87FB860 BD4083FA 5B531A08 A4FB7EE0 201AE8B3 CCFFE99F
        270BC353 4BAACFC0 01CDD80A D87CCE71 F091E766 CA5CC275
        CB49145A 5EE6162E CCF558CE C4D3EE53 1E91E9A5 2969634D
        3AF8D26F 8D15DC0D 6F6E0A97 4BE4341B 68A01990 DBB86495
        891AD3AF C1E4CEDF 4C6AE1F1 CD6081CD EED8E6B3 264EC3BE


Z is
                                                8C5D6E5D 360683BA
        55B09DB1 696D7C64 02FF8788 5FF50770 F2767B75 5460207E
```

D5C743FD 27E7EB1D 0CA591F8 56389311 730744F2 04D2E55B
8BD446CE CA031F7B ACCFF1A7 1B683459 CC54D501 DABF4A84
CDB86DFA DAFF310F BDBAF74D D51BA1E1 E1191AF1 4C9BF894
43BF588E 9CE33034 AF5E89BF 6FFC47D7 D9CA4A5E 8FF8A050
20BB0F95 BCDE0156 D87FB860 BD4083FA 5B531A08 A4FB7EE0
201AE8B3 CCFFE99F 270BC353 4BAACFC0 01CDD80A D87CCE71
F091E766 CA5CC275 CB49145A 5EE6162E CCF558CE C4D3EE53
1E91E9A5 2969634D 3AF8D26F 8D15DC0D 6F6E0A97 4BE4341B
68A01990 DBB86495 891AD3AF C1E4CEDF 4C6AE1F1 CD6081CD
EED8E6B3 264EC3BE 2458D1C0 CA244341 0CF3B47C 0C254C7D
C8ECB43E 6C2364E1 C06219CC 7EFBFFBB 63D7FFFC 745812FD
240C33D4 96B9992F 9680A63C 07963C0C 49F3C1BA EFECAF32
E2AA8A2F 7CD30D8F 051EE2F5 0FBF05AB 1396A4EA 87447D7B
981B5E46 14281871 A6F0F6BF 1FE0022F 7EA132BE 0AE91926
AB12AF6D C45064AA D56B84B9 0C700837 09CFF7E3 1B548FB7
FB2CF75A BF96E01C CD3E942E ED91480D 4C24C6B7 F979FBBE
5DA239B3 76167D68 573524FF CB509954 CC80A0E1 A71C40C4
DA17B8D1 572B2158 7A8D66CC 621C7CD1 0F49ABD5 EF863113
E6192108 6FAC2531 2B741C11 A8FBC1E3 3C34D9DA 14A82247
7FCC3666 7025C4F1 30AE100E 36F15DA0 0374CE87 41679F61

OtherInfo is
12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536

MacData is
4B435F31 5F55414C 49434542 4F424259 3DB2F114 B59BF6D9
9458F3F6 BE6072B0 106ED031 25BFF741 FF8BDC96 D0C541AF
AB1DF7AB 694F77CB 962D0AB7 435B1A3A 8E93AE97 F182606D
3CE9DCA3 A6F00EBD 6C47D81D 6AD58008 49490CAF C34A9C8D
D6D7EDA8 03A96614 25637D99 84075711 2FBC01DF 76D83F99
E3E97EF9 9090596A 1287BB2E 0B00911F E27FFBD2 87C5D024
5AE8631C D9C8A10E E236BF8A F5E0CE4E D27DE78D 12206A15
AEF1AAA6 951247B1 525F3E94 4743C5CD 4B13D244 A1644C09
A2697ED0 8714416E 7FF1BD24 D3151A7B 797C368C A7D14D9D
1975CB3A 065CAE9D 89A26E39 BD698089 51786674 BA9711E0
DED299CA 06B9B90E A02B6A8B C0BAAE9F B6AA5A89 3436B9CD
14CCD6FF 365E6F68 7F6CB1D0 F8F22C63 BA888121 41F5D895
BB92301D BF843F29 2A67B862 A60A568C 7719D90C 529CE89A
78B3A8E1 EB18DDCB 30BBD675 9251F33E 46A98B97 84D392B6
A3B73F49 71F3D939 0E27EAC8 28006098 1FC3876F 83C3B99D
CD71EB2D B4CC9AC3 24AD405C A0DC2692 C05D9363 D4B65F68
C2C9D8D8 F674D09D EB19A933 2D5A9FE0 CB77E949 271B8BD7
4A1AEC9D 79DF7493 FB860673 9B586A81 C8FFED24 2A94C1A7
669CCF40 34AB3852 82610EF4 687E887E EB640CDC 48C42BDF

F192AB2E C3B4F93D 0152307D 00A12FD3 6FF10FDD B7275FDE
75C6814D 963FB5E6 E3204025 86FCB749 260D7918 08D12589
39D0690A 9ECE0CD5 7A5C4C16 B58B242C A724CD15 8AF16C49

MacKey is
4B99 6A60C04A 35C5E6D4 74B10A25

Mtag is
899B F1B801A8 19DB592F 01E5E93B

KeyData is
8D562EA6 DC52F6C6
9BF39EF8 8C89E3CC 8A54DA2F 3C0B561B 53FE7655 1363D69C
3CEF74E3 4FE88EB3 AC514334 6D96B320 7872CCCC 2C443E0E

Scheme Responder, Key Confirmation Provider: V to U
Zs is
2458D1C0 CA244341 0CF3B47C 0C254C7D
C8ECB43E 6C2364E1 C06219CC 7EFBFFBB 63D7FFFC 745812FD
240C33D4 96B9992F 9680A63C 07963C0C 49F3C1BA EFECAF32
E2AA8A2F 7CD30D8F 051EE2F5 0FBF05AB 1396A4EA 87447D7B
981B5E46 14281871 A6F0F6BF 1FE0022F 7EA132BE 0AE91926
AB12AF6D C45064AA D56B84B9 0C700837 09CFF7E3 1B548FB7
FB2CF75A BF96E01C CD3E942E ED91480D 4C24C6B7 F979FBBE
5DA239B3 76167D68 573524FF CB509954 CC80A0E1 A71C40C4
DA17B8D1 572B2158 7A8D66CC 621C7CD1 0F49ABD5 EF863113
E6192108 6FAC2531 2B741C11 A8FBC1E3 3C34D9DA 14A82247
7FCC3666 7025C4F1 30AE100E 36F15DA0 0374CE87 41679F61

Ze is
8C5D6E5D 360683BA 55B09DB1 696D7C64
02FF8788 5FF50770 F2767B75 5460207E D5C743FD 27E7EB1D
0CA591F8 56389311 730744F2 04D2E55B 8BD446CE CA031F7B
ACCFF1A7 1B683459 CC54D501 DABF4A84 CDB86DFA DAFF310F
BDBAF74D D51BA1E1 E1191AF1 4C9BF894 43BF588E 9CE33034
AF5E89BF 6FFC47D7 D9CA4A5E 8FF8A050 20BB0F95 BCDE0156
D87FB860 BD4083FA 5B531A08 A4FB7EE0 201AE8B3 CCFFE99F
270BC353 4BAACFC0 01CDD80A D87CCE71 F091E766 CA5CC275

CB49145A 5EE6162E CCF558CE C4D3EE53 1E91E9A5 2969634D
3AF8D26F 8D15DC0D 6F6E0A97 4BE4341B 68A01990 DBB86495
891AD3AF C1E4CEDF 4C6AE1F1 CD6081CD EED8E6B3 264EC3BE

Z is

8C5D6E5D 360683BA
55B09DB1 696D7C64 02FF8788 5FF50770 F2767B75 5460207E
D5C743FD 27E7EB1D 0CA591F8 56389311 730744F2 04D2E55B
8BD446CE CA031F7B ACCFF1A7 1B683459 CC54D501 DABF4A84
CDB86DFA DAFF310F BDBAF74D D51BA1E1 E1191AF1 4C9BF894
43BF588E 9CE33034 AF5E89BF 6FFC47D7 D9CA4A5E 8FF8A050
20BB0F95 BCDE0156 D87FB860 BD4083FA 5B531A08 A4FB7EE0
201AE8B3 CCFFE99F 270BC353 4BAACFC0 01CDD80A D87CCE71
F091E766 CA5CC275 CB49145A 5EE6162E CCF558CE C4D3EE53
1E91E9A5 2969634D 3AF8D26F 8D15DC0D 6F6E0A97 4BE4341B
68A01990 DBB86495 891AD3AF C1E4CEDF 4C6AE1F1 CD6081CD
EED8E6B3 264EC3BE 2458D1C0 CA244341 0CF3B47C 0C254C7D
C8ECB43E 6C2364E1 C06219CC 7EFBFFBB 63D7FFFC 745812FD
240C33D4 96B9992F 9680A63C 07963C0C 49F3C1BA EFECAF32
E2AA8A2F 7CD30D8F 051EE2F5 0FBF05AB 1396A4EA 87447D7B
981B5E46 14281871 A6F0F6BF 1FE0022F 7EA132BE 0AE91926
AB12AF6D C45064AA D56B84B9 0C700837 09CFF7E3 1B548FB7
FB2CF75A BF96E01C CD3E942E ED91480D 4C24C6B7 F979FBBE
5DA239B3 76167D68 573524FF CB509954 CC80A0E1 A71C40C4
DA17B8D1 572B2158 7A8D66CC 621C7CD1 0F49ABD5 EF863113
E6192108 6FAC2531 2B741C11 A8FBC1E3 3C34D9DA 14A82247
7FCC3666 7025C4F1 30AE100E 36F15DA0 0374CE87 41679F61

OtherInfo is
12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536

MacData is
4B435F31 5F56424F 42425941 4C494345 7F6CB1D0 F8F22C63
BA888121 41F5D895 BB92301D BF843F29 2A67B862 A60A568C
7719D90C 529CE89A 78B3A8E1 EB18DDCB 30BBD675 9251F33E
46A98B97 84D392B6 A3B73F49 71F3D939 0E27EAC8 28006098
1FC3876F 83C3B99D CD71EB2D B4CC9AC3 24AD405C A0DC2692
C05D9363 D4B65F68 C2C9D8D8 F674D09D EB19A933 2D5A9FE0
CB77E949 271B8BD7 4A1AEC9D 79DF7493 FB860673 9B586A81
C8FFED24 2A94C1A7 669CCF40 34AB3852 82610EF4 687E887E
EB640CDC 48C42BDF F192AB2E C3B4F93D 0152307D 00A12FD3
6FF10FDD B7275FDE 75C6814D 963FB5E6 E3204025 86FCB749
260D7918 08D12589 39D0690A 9ECE0CD5 7A5C4C16 B58B242C

A724CD15 8AF16C49 3DB2F114 B59BF6D9 9458F3F6 BE6072B0
106ED031 25BFF741 FF8BDC96 D0C541AF AB1DF7AB 694F77CB
962D0AB7 435B1A3A 8E93AE97 F182606D 3CE9DCA3 A6F00EBD
6C47D81D 6AD58008 49490CAF C34A9C8D D6D7EDA8 03A96614
25637D99 84075711 2FBC01DF 76D83F99 E3E97EF9 9090596A
1287BB2E 0B00911F E27FFBD2 87C5D024 5AE8631C D9C8A10E
E236BF8A F5E0CE4E D27DE78D 12206A15 AEF1AAA6 951247B1
525F3E94 4743C5CD 4B13D244 A1644C09 A2697ED0 8714416E
7FF1BD24 D3151A7B 797C368C A7D14D9D 1975CB3A 065CAE9D
89A26E39 BD698089 51786674 BA9711E0 DED299CA 06B9B90E
A02B6A8B C0BAAE9F B6AA5A89 3436B9CD 14CCD6FF 365E6F68

MacKey is
4B99 6A60C04A 35C5E6D4 74B10A25

Mtag is
A8BD A7471C90 52DF66D2 591E671A

KeyData is
8D562EA6 DC52F6C6
9BF39EF8 8C89E3CC 8A54DA2F 3C0B561B 53FE7655 1363D69C
3CEF74E3 4FE88EB3 AC514334 6D96B320 7872CCCC 2C443E0E

Scheme Initiator, Key Confirmation Bilateral
Zs is
2458D1C0 CA244341 0CF3B47C 0C254C7D
C8ECB43E 6C2364E1 C06219CC 7EFBFFBB 63D7FFFC 745812FD
240C33D4 96B9992F 9680A63C 07963C0C 49F3C1BA EFECAF32
E2AA8A2F 7CD30D8F 051EE2F5 0FBF05AB 1396A4EA 87447D7B
981B5E46 14281871 A6F0F6BF 1FE0022F 7EA132BE 0AE91926
AB12AF6D C45064AA D56B84B9 0C700837 09CFF7E3 1B548FB7
FB2CF75A BF96E01C CD3E942E ED91480D 4C24C6B7 F979FBBE
5DA239B3 76167D68 573524FF CB509954 CC80A0E1 A71C40C4
DA17B8D1 572B2158 7A8D66CC 621C7CD1 0F49ABD5 EF863113
E6192108 6FAC2531 2B741C11 A8FBC1E3 3C34D9DA 14A82247
7FCC3666 7025C4F1 30AE100E 36F15DA0 0374CE87 41679F61

Ze is

```
                        8C5D6E5D 360683BA 55B09DB1 696D7C64
        02FF8788 5FF50770 F2767B75 5460207E D5C743FD 27E7EB1D
        0CA591F8 56389311 730744F2 04D2E55B 8BD446CE CA031F7B
        ACCFF1A7 1B683459 CC54D501 DABF4A84 CDB86DFA DAFF310F
        BDBAF74D D51BA1E1 E1191AF1 4C9BF894 43BF588E 9CE33034
        AF5E89BF 6FFC47D7 D9CA4A5E 8FF8A050 20BB0F95 BCDE0156
        D87FB860 BD4083FA 5B531A08 A4FB7EE0 201AE8B3 CCFFE99F
        270BC353 4BAACFC0 01CDD80A D87CCE71 F091E766 CA5CC275
        CB49145A 5EE6162E CCF558CE C4D3EE53 1E91E9A5 2969634D
        3AF8D26F 8D15DC0D 6F6E0A97 4BE4341B 68A01990 DBB86495
        891AD3AF C1E4CEDF 4C6AE1F1 CD6081CD EED8E6B3 264EC3BE


Z is
                                                8C5D6E5D 360683BA
        55B09DB1 696D7C64 02FF8788 5FF50770 F2767B75 5460207E
        D5C743FD 27E7EB1D 0CA591F8 56389311 730744F2 04D2E55B
        8BD446CE CA031F7B ACCFF1A7 1B683459 CC54D501 DABF4A84
        CDB86DFA DAFF310F BDBAF74D D51BA1E1 E1191AF1 4C9BF894
        43BF588E 9CE33034 AF5E89BF 6FFC47D7 D9CA4A5E 8FF8A050
        20BB0F95 BCDE0156 D87FB860 BD4083FA 5B531A08 A4FB7EE0
        201AE8B3 CCFFE99F 270BC353 4BAACFC0 01CDD80A D87CCE71
        F091E766 CA5CC275 CB49145A 5EE6162E CCF558CE C4D3EE53
        1E91E9A5 2969634D 3AF8D26F 8D15DC0D 6F6E0A97 4BE4341B
        68A01990 DBB86495 891AD3AF C1E4CEDF 4C6AE1F1 CD6081CD
        EED8E6B3 264EC3BE 2458D1C0 CA244341 0CF3B47C 0C254C7D
        C8ECB43E 6C2364E1 C06219CC 7EFBFFBB 63D7FFFC 745812FD
        240C33D4 96B9992F 9680A63C 07963C0C 49F3C1BA EFECAF32
        E2AA8A2F 7CD30D8F 051EE2F5 0FBF05AB 1396A4EA 87447D7B
        981B5E46 14281871 A6F0F6BF 1FE0022F 7EA132BE 0AE91926
        AB12AF6D C45064AA D56B84B9 0C700837 09CFF7E3 1B548FB7
        FB2CF75A BF96E01C CD3E942E ED91480D 4C24C6B7 F979FBBE
        5DA239B3 76167D68 573524FF CB509954 CC80A0E1 A71C40C4
        DA17B8D1 572B2158 7A8D66CC 621C7CD1 0F49ABD5 EF863113
        E6192108 6FAC2531 2B741C11 A8FBC1E3 3C34D9DA 14A82247
        7FCC3666 7025C4F1 30AE100E 36F15DA0 0374CE87 41679F61


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


U2V
----------------
MacData is
        4B435F32 5F55414C 49434542 4F424259 3DB2F114 B59BF6D9
```

```
        9458F3F6 BE6072B0 106ED031 25BFF741 FF8BDC96 D0C541AF
        AB1DF7AB 694F77CB 962D0AB7 435B1A3A 8E93AE97 F182606D
        3CE9DCA3 A6F00EBD 6C47D81D 6AD58008 49490CAF C34A9C8D
        D6D7EDA8 03A96614 25637D99 84075711 2FBC01DF 76D83F99
        E3E97EF9 9090596A 1287BB2E 0B00911F E27FFBD2 87C5D024
        5AE8631C D9C8A10E E236BF8A F5E0CE4E D27DE78D 12206A15
        AEF1AAA6 951247B1 525F3E94 4743C5CD 4B13D244 A1644C09
        A2697ED0 8714416E 7FF1BD24 D3151A7B 797C368C A7D14D9D
        1975CB3A 065CAE9D 89A26E39 BD698089 51786674 BA9711E0
        DED299CA 06B9B90E A02B6A8B C0BAAE9F B6AA5A89 3436B9CD
        14CCD6FF 365E6F68 7F6CB1D0 F8F22C63 BA888121 41F5D895
        BB92301D BF843F29 2A67B862 A60A568C 7719D90C 529CE89A
        78B3A8E1 EB18DDCB 30BBD675 9251F33E 46A98B97 84D392B6
        A3B73F49 71F3D939 0E27EAC8 28006098 1FC3876F 83C3B99D
        CD71EB2D B4CC9AC3 24AD405C A0DC2692 C05D9363 D4B65F68
        C2C9D8D8 F674D09D EB19A933 2D5A9FE0 CB77E949 271B8BD7
        4A1AEC9D 79DF7493 FB860673 9B586A81 C8FFED24 2A94C1A7
        669CCF40 34AB3852 82610EF4 687E887E EB640CDC 48C42BDF
        F192AB2E C3B4F93D 0152307D 00A12FD3 6FF10FDD B7275FDE
        75C6814D 963FB5E6 E3204025 86FCB749 260D7918 08D12589
        39D0690A 9ECE0CD5 7A5C4C16 B58B242C A724CD15 8AF16C49


MacKey is
                              4B99 6A60C04A 35C5E6D4 74B10A25


Mtag is
                              0C42 C6D19ADD DBA36343 E4051E8C


V2U
----------------
MacData is
        4B435F32 5F56424F 42425941 4C494345 7F6CB1D0 F8F22C63
        BA888121 41F5D895 BB92301D BF843F29 2A67B862 A60A568C
        7719D90C 529CE89A 78B3A8E1 EB18DDCB 30BBD675 9251F33E
        46A98B97 84D392B6 A3B73F49 71F3D939 0E27EAC8 28006098
        1FC3876F 83C3B99D CD71EB2D B4CC9AC3 24AD405C A0DC2692
        C05D9363 D4B65F68 C2C9D8D8 F674D09D EB19A933 2D5A9FE0
        CB77E949 271B8BD7 4A1AEC9D 79DF7493 FB860673 9B586A81
        C8FFED24 2A94C1A7 669CCF40 34AB3852 82610EF4 687E887E
        EB640CDC 48C42BDF F192AB2E C3B4F93D 0152307D 00A12FD3
        6FF10FDD B7275FDE 75C6814D 963FB5E6 E3204025 86FCB749
        260D7918 08D12589 39D0690A 9ECE0CD5 7A5C4C16 B58B242C
        A724CD15 8AF16C49 3DB2F114 B59BF6D9 9458F3F6 BE6072B0
```

```
        106ED031 25BFF741 FF8BDC96 D0C541AF AB1DF7AB 694F77CB
        962D0AB7 435B1A3A 8E93AE97 F182606D 3CE9DCA3 A6F00EBD
        6C47D81D 6AD58008 49490CAF C34A9C8D D6D7EDA8 03A96614
        25637D99 84075711 2FBC01DF 76D83F99 E3E97EF9 9090596A
        1287BB2E 0B00911F E27FFBD2 87C5D024 5AE8631C D9C8A10E
        E236BF8A F5E0CE4E D27DE78D 12206A15 AEF1AAA6 951247B1
        525F3E94 4743C5CD 4B13D244 A1644C09 A2697ED0 8714416E
        7FF1BD24 D3151A7B 797C368C A7D14D9D 1975CB3A 065CAE9D
        89A26E39 BD698089 51786674 BA9711E0 DED299CA 06B9B90E
        A02B6A8B C0BAAE9F B6AA5A89 3436B9CD 14CCD6FF 365E6F68


MacKey is
                            4B99 6A60C04A 35C5E6D4 74B10A25


Mtag is
                            7F2E A5491E9B 1F26E410 53A2597B


KeyData is
                                          8D562EA6 DC52F6C6
        9BF39EF8 8C89E3CC 8A54DA2F 3C0B561B 53FE7655 1363D69C
        3CEF74E3 4FE88EB3 AC514334 6D96B320 7872CCCC 2C443E0E


============================================================


MQV2(224)
------------------------------------------------------------
xU is
                                                    2666818A
        5BA33D39 5A8C9B07 F134ACBB 9A14D295 7583B08F 8C142683


yU is
                           17B43410 5DD13943 3ABE206B EFBCD21E
        CC9F60CE F35FC052 49630A91 73A828D5 B5EC45BB 90CEC175
        197E1DDF 4A5629D3 1DF7A88D A584F5B6 9CBE0453 149C982D
        06556D4C 6E1FACB6 448BBCA2 0B384B17 2333A9F4 570817F1
        41D9AE04 28B10A52 24F5B908 498433BB 69263009 304C0534
        6DA23329 29F0FC2A 252F0F82 69DF7B6D 61752764 EEB6E3BB
        A5153673 03C0C5E8 F3CFA6C1 70B47E1B 65B5C890 82616C0E
        C09690B7 41460355 86734E56 227C2D2C 80438555 150FE564
        6BEC9B47 90C869ED C404F7A1 EF6449B5 5ACC3B16 6D9B989A
```

634E584C 0F120D30 C48CD320 5D40EAE8 FC0281A9 F0D5D912
4C3E0789 417008AA 6869458D 2835CD22 236A2B7B 3E94FBE2

xV is
7CC07D78
B25CBA43 D1559D17 F01D5FC6 050C0FC0 6E33B176 791D0A36

yV is
80E725D7 AF47E25D 6765C233 93433A61
A1E4F54D 94A924E4 FF8B6375 E5F13B2A 38FE4496 BBB6B434
6EDF545D 1A4E1C55 2D7F9234 0BD5018E 54E83D0C C5CC83D1
775CE8EE 41E8ACA0 4FCAFF10 4A8A29C0 0DA96636 D7A566FF
838AC8ED 2A2B4724 61BCCB1A E99FDF7B B69960EA 153B9D17
70F83A62 CB7A493B 6E673F7E 033F2D0A 09886E02 5A423060
7E74A00A 421234E5 A3DBE855 F6BAF97F 2C6E40F6 D2D5BEF6
7CAEB1AF 03CC3135 00304E36 CC171547 FD2B75C8 457936A0
546EF48F 4486876E 771B4B10 CD4517B9 A8CF5599 E2CADCF6
E2A152DD 8CDE46CE 53762609 898D29DB 6D39A30C 22219FE9
6E36DA04 3224528C 2538837E 30173BBE DC313CA2 C8B53FE7

rU is
361C05EC
AC22DAD4 263E7630 A0E7B118 4A60A494 8EFA3B47 95E36962

tU is
642FC401 6BF8DBAE 210004C9 9FF9DE60
983B419A 841447C8 329D55E3 2F635737 2B83FB5D 9DB37A94
74A257B7 9234C89C B53E3CC9 87A8FEC1 37DC0ABB 606E2857
A0B6245C 7BE12ADC 1CD92A13 D18BADB5 BF68F3EA AB104713
ADE442E6 8DBB7E8E CF81F2F3 F1F90253 88E7EBD6 4748C336
A8F670FA 56A79545 A9431A83 9E44626D EA90F3D7 0AA77F6A
23200C47 CC2073C6 5E558BE5 DEFEBC0E 6F1FD465 63CAACDF
211106BF CC07AB22 033266CA E205F7AC E4A2AFCE 9714315E
49636B82 D86AB401 8529F1A1 EC710EF6 CCBC7A97 763AE94E
E12E764E 95D4A187 8B5933EC 6FB33E08 48E5B968 D37D51AD
588397EF F8B23FAD 7265702A D907DF4D 01812839 15DE47F8

rV is
354E23E0
F786BF7B D374B0A9 F66974F9 94CDDCDF 9700D1F8 3C1044F7

```
tV is
                          5D7CA0F4 CF2593CE 07FCA45A D035EC89
        FF7FB8D8 97743F5F 8FEC20AF 057ACC72 FE5EAD8C D1731424
        87D92447 51B58CDC 7B8F9034 614C0864 BAB74310 D6F5E2F1
        2B9B3918 E6669DE2 3C7BBA7F F5F8A3C3 5D4F08B0 838EC458
        49C1E187 3A2A8D28 187907AA 92FB4E24 6F368BE3 0ED1B68C
        A984BA32 09CC8FE0 7824F864 C46170E7 0B1A621C 871FB873
        FD64DC4B 0A1D844C 2C8C3DB4 0CD79A03 38458370 5B178A42
        E0F404B0 18D941CF 76A3DC9A 8205D75A FA859F80 66138D39
        05B3D126 9ACED1F9 837CBA95 3E290B0F 704F0F44 C8C0E284
        0B2DBA78 736A8336 EF9126BE 0FA5E8DC E03B126A E0FFFB91
        B156BA56 01160B9F 2BA01109 719EBFAC 60CAD21F B9724846



------------------------------------------------------------
no Key Confirmation
Z is
                          97ED780D 4EA6EDBA EE8363D4 4656BD89
        5708EDB3 2359FAF1 C8FBACB8 FFD5CDFD CCE0EDF6 1E69F179
        0069A049 1ADA5F78 1C44AD60 1AF6E1F6 1EF9BB42 3C5B6B7C
        B6ED8783 21F90A59 3D942698 71E2F430 71E56473 C4B2959A
        86AC55C2 4F6DAF78 E8AEF03C 3A65C6EB 2CEBA3D9 87E8514F
        F961209A 03340B6D 1305DFC1 BC721A59 A8332282 8FE883BD
        194EE0AD F0914FA4 FEBB9EC5 29E47AA7 CA57C0D2 97022139
        43308FFB 105CDFA4 0E34CE42 60509044 AEFDD5B1 E83A608E
        DCA1DF31 E4D84F5A F2669713 308009A5 7DA5055F D8236595
        E0F69CCA 38A3343D 54122EB5 63B5380C 8F8EC844 13B6B9CA
        68751F51 6E86C892 EF88798A 4717FC87 CCF7385C EE1D9378


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


KDFval is
                                                  5E45D05A 8893A091
        649AB638 0F9C32F7 28CC3A65 004783BE 5F13CFB5 9D694FB7
        7A9F2B20 221FB582 9A8D5592 5232AC4F CE9DE197 7245D804


KeyData is
                                                  5E45D05A 8893A091
        649AB638 0F9C32F7 28CC3A65 004783BE 5F13CFB5 9D694FB7
```

7A9F2B20 221FB582 9A8D5592 5232AC4F CE9DE197 7245D804

Scheme Initiator, Key Confirmation Provider: U to V
Z is
97ED780D 4EA6EDBA EE8363D4 4656BD89
5708EDB3 2359FAF1 C8FBACB8 FFD5CDFD CCE0EDF6 1E69F179
0069A049 1ADA5F78 1C44AD60 1AF6E1F6 1EF9BB42 3C5B6B7C
B6ED8783 21F90A59 3D942698 71E2F430 71E56473 C4B2959A
86AC55C2 4F6DAF78 E8AEF03C 3A65C6EB 2CEBA3D9 87E8514F
F961209A 03340B6D 1305DFC1 BC721A59 A8332282 8FE883BD
194EE0AD F0914FA4 FEBB9EC5 29E47AA7 CA57C0D2 97022139
43308FFB 105CDFA4 0E34CE42 60509044 AEFDD5B1 E83A608E
DCA1DF31 E4D84F5A F2669713 308009A5 7DA5055F D8236595
E0F69CCA 38A3343D 54122EB5 63B5380C 8F8EC844 13B6B9CA
68751F51 6E86C892 EF88798A 4717FC87 CCF7385C EE1D9378

OtherInfo is
12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536

KDFval is
5E45 D05A8893 A091649A B6380F9C 32F728CC 3A650047
83BE5F13 CFB59D69 4FB77A9F 2B20221F B5829A8D 55925232
AC4FCE9D E1977245 D8044B7E 143DFC64 BD17CE1E C821F6C9

MacData is
4B435F31 5F55414C 49434542 4F424259 642FC401 6BF8DBAE
210004C9 9FF9DE60 983B419A 841447C8 329D55E3 2F635737
2B83FB5D 9DB37A94 74A257B7 9234C89C B53E3CC9 87A8FEC1
37DC0ABB 606E2857 A0B6245C 7BE12ADC 1CD92A13 D18BADB5
BF68F3EA AB104713 ADE442E6 8DBB7E8E CF81F2F3 F1F90253
88E7EBD6 4748C336 A8F670FA 56A79545 A9431A83 9E44626D
EA90F3D7 0AA77F6A 23200C47 CC2073C6 5E558BE5 DEFEBC0E
6F1FD465 63CAACDF 211106BF CC07AB22 033266CA E205F7AC
E4A2AFCE 9714315E 49636B82 D86AB401 8529F1A1 EC710EF6
CCBC7A97 763AE94E E12E764E 95D4A187 8B5933EC 6FB33E08
48E5B968 D37D51AD 588397EF F8B23FAD 7265702A D907DF4D
01812839 15DE47F8 5D7CA0F4 CF2593CE 07FCA45A D035EC89
FF7FB8D8 97743F5F 8FEC20AF 057ACC72 FE5EAD8C D1731424
87D92447 51B58CDC 7B8F9034 614C0864 BAB74310 D6F5E2F1

2B9B3918 E6669DE2 3C7BBA7F F5F8A3C3 5D4F08B0 838EC458
49C1E187 3A2A8D28 187907AA 92FB4E24 6F368BE3 0ED1B68C
A984BA32 09CC8FE0 7824F864 C46170E7 0B1A621C 871FB873
FD64DC4B 0A1D844C 2C8C3DB4 0CD79A03 38458370 5B178A42
E0F404B0 18D941CF 76A3DC9A 8205D75A FA859F80 66138D39
05B3D126 9ACED1F9 837CBA95 3E290B0F 704F0F44 C8C0E284
0B2DBA78 736A8336 EF9126BE 0FA5E8DC E03B126A E0FFFB91
B156BA56 01160B9F 2BA01109 719EBFAC 60CAD21F B9724846

MacKey is
5E45 D05A8893 A091649A B6380F9C

Mtag is
79B4 2CE97C09 EF83CDDE F1E23EC4

KeyData is
32F728CC 3A650047
83BE5F13 CFB59D69 4FB77A9F 2B20221F B5829A8D 55925232
AC4FCE9D E1977245 D8044B7E 143DFC64 BD17CE1E C821F6C9

Scheme Responder, Key Confirmation Provider: V to U
Z is
97ED780D 4EA6EDBA EE8363D4 4656BD89
5708EDB3 2359FAF1 C8FBACB8 FFD5CDFD CCE0EDF6 1E69F179
0069A049 1ADA5F78 1C44AD60 1AF6E1F6 1EF9BB42 3C5B6B7C
B6ED8783 21F90A59 3D942698 71E2F430 71E56473 C4B2959A
86AC55C2 4F6DAF78 E8AEF03C 3A65C6EB 2CEBA3D9 87E8514F
F961209A 03340B6D 1305DFC1 BC721A59 A8332282 8FE883BD
194EE0AD F0914FA4 FEBB9EC5 29E47AA7 CA57C0D2 97022139
43308FFB 105CDFA4 0E34CE42 60509044 AEFDD5B1 E83A608E
DCA1DF31 E4D84F5A F2669713 308009A5 7DA5055F D8236595
E0F69CCA 38A3343D 54122EB5 63B5380C 8F8EC844 13B6B9CA
68751F51 6E86C892 EF88798A 4717FC87 CCF7385C EE1D9378

OtherInfo is
12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536

KDFval is
5E45 D05A8893 A091649A B6380F9C 32F728CC 3A650047
83BE5F13 CFB59D69 4FB77A9F 2B20221F B5829A8D 55925232
AC4FCE9D E1977245 D8044B7E 143DFC64 BD17CE1E C821F6C9

MacData is
4B435F31 5F56424F 42425941 4C494345 5D7CA0F4 CF2593CE
07FCA45A D035EC89 FF7FB8D8 97743F5F 8FEC20AF 057ACC72
FE5EAD8C D1731424 87D92447 51B58CDC 7B8F9034 614C0864
BAB74310 D6F5E2F1 2B9B3918 E6669DE2 3C7BBA7F F5F8A3C3
5D4F08B0 838EC458 49C1E187 3A2A8D28 187907AA 92FB4E24
6F368BE3 0ED1B68C A984BA32 09CC8FE0 7824F864 C46170E7
0B1A621C 871FB873 FD64DC4B 0A1D844C 2C8C3DB4 0CD79A03
38458370 5B178A42 E0F404B0 18D941CF 76A3DC9A 8205D75A
FA859F80 66138D39 05B3D126 9ACED1F9 837CBA95 3E290B0F
704F0F44 C8C0E284 0B2DBA78 736A8336 EF9126BE 0FA5E8DC
E03B126A E0FFFB91 B156BA56 01160B9F 2BA01109 719EBFAC
60CAD21F B9724846 642FC401 6BF8DBAE 210004C9 9FF9DE60
983B419A 841447C8 329D55E3 2F635737 2B83FB5D 9DB37A94
74A257B7 9234C89C B53E3CC9 87A8FEC1 37DC0ABB 606E2857
A0B6245C 7BE12ADC 1CD92A13 D18BADB5 BF68F3EA AB104713
ADE442E6 8DBB7E8E CF81F2F3 F1F90253 88E7EBD6 4748C336
A8F670FA 56A79545 A9431A83 9E44626D EA90F3D7 0AA77F6A
23200C47 CC2073C6 5E558BE5 DEFEBC0E 6F1FD465 63CAACDF
211106BF CC07AB22 033266CA E205F7AC E4A2AFCE 9714315E
49636B82 D86AB401 8529F1A1 EC710EF6 CCBC7A97 763AE94E
E12E764E 95D4A187 8B5933EC 6FB33E08 48E5B968 D37D51AD
588397EF F8B23FAD 7265702A D907DF4D 01812839 15DE47F8

MacKey is
5E45 D05A8893 A091649A B6380F9C

Mtag is
1339 6F7946C5 0D931ED2 6AA82055

KeyData is
32F728CC 3A650047
83BE5F13 CFB59D69 4FB77A9F 2B20221F B5829A8D 55925232
AC4FCE9D E1977245 D8044B7E 143DFC64 BD17CE1E C821F6C9

```
-----------------------------------------------------------
Scheme Initiator, Key Confirmation Bilateral
Z is
                          97ED780D 4EA6EDBA EE8363D4 4656BD89
        5708EDB3 2359FAF1 C8FBACB8 FFD5CDFD CCE0EDF6 1E69F179
        0069A049 1ADA5F78 1C44AD60 1AF6E1F6 1EF9BB42 3C5B6B7C
        B6ED8783 21F90A59 3D942698 71E2F430 71E56473 C4B2959A
        86AC55C2 4F6DAF78 E8AEF03C 3A65C6EB 2CEBA3D9 87E8514F
        F961209A 03340B6D 1305DFC1 BC721A59 A8332282 8FE883BD
        194EE0AD F0914FA4 FEBB9EC5 29E47AA7 CA57C0D2 97022139
        43308FFB 105CDFA4 0E34CE42 60509044 AEFDD5B1 E83A608E
        DCA1DF31 E4D84F5A F2669713 308009A5 7DA5055F D8236595
        E0F69CCA 38A3343D 54122EB5 63B5380C 8F8EC844 13B6B9CA
        68751F51 6E86C892 EF88798A 4717FC87 CCF7385C EE1D9378


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


KDFval is
            5E45 D05A8893 A091649A B6380F9C 32F728CC 3A650047
        83BE5F13 CFB59D69 4FB77A9F 2B20221F B5829A8D 55925232
        AC4FCE9D E1977245 D8044B7E 143DFC64 BD17CE1E C821F6C9


U2V
----------------
MacData is
        4B435F32 5F55414C 49434542 4F424259 642FC401 6BF8DBAE
        210004C9 9FF9DE60 983B419A 841447C8 329D55E3 2F635737
        2B83FB5D 9DB37A94 74A257B7 9234C89C B53E3CC9 87A8FEC1
        37DC0ABB 606E2857 A0B6245C 7BE12ADC 1CD92A13 D18BADB5
        BF68F3EA AB104713 ADE442E6 8DBB7E8E CF81F2F3 F1F90253
        88E7EBD6 4748C336 A8F670FA 56A79545 A9431A83 9E44626D
        EA90F3D7 0AA77F6A 23200C47 CC2073C6 5E558BE5 DEFEBC0E
        6F1FD465 63CAACDF 211106BF CC07AB22 033266CA E205F7AC
        E4A2AFCE 9714315E 49636B82 D86AB401 8529F1A1 EC710EF6
        CCBC7A97 763AE94E E12E764E 95D4A187 8B5933EC 6FB33E08
        48E5B968 D37D51AD 588397EF F8B23FAD 7265702A D907DF4D
        01812839 15DE47F8 5D7CA0F4 CF2593CE 07FCA45A D035EC89
        FF7FB8D8 97743F5F 8FEC20AF 057ACC72 FE5EAD8C D1731424
        87D92447 51B58CDC 7B8F9034 614C0864 BAB74310 D6F5E2F1
        2B9B3918 E6669DE2 3C7BBA7F F5F8A3C3 5D4F08B0 838EC458
        49C1E187 3A2A8D28 187907AA 92FB4E24 6F368BE3 0ED1B68C
```

A984BA32 09CC8FE0 7824F864 C46170E7 0B1A621C 871FB873
FD64DC4B 0A1D844C 2C8C3DB4 0CD79A03 38458370 5B178A42
E0F404B0 18D941CF 76A3DC9A 8205D75A FA859F80 66138D39
05B3D126 9ACED1F9 837CBA95 3E290B0F 704F0F44 C8C0E284
0B2DBA78 736A8336 EF9126BE 0FA5E8DC E03B126A E0FFFB91
B156BA56 01160B9F 2BA01109 719EBFAC 60CAD21F B9724846

MacKey is
5E45 D05A8893 A091649A B6380F9C

Mtag is
5567 0F1CBC24 1E416324 19BC6627

V2U

MacData is
4B435F32 5F56424F 42425941 4C494345 5D7CA0F4 CF2593CE
07FCA45A D035EC89 FF7FB8D8 97743F5F 8FEC20AF 057ACC72
FE5EAD8C D1731424 87D92447 51B58CDC 7B8F9034 614C0864
BAB74310 D6F5E2F1 2B9B3918 E6669DE2 3C7BBA7F F5F8A3C3
5D4F08B0 838EC458 49C1E187 3A2A8D28 187907AA 92FB4E24
6F368BE3 0ED1B68C A984BA32 09CC8FE0 7824F864 C46170E7
0B1A621C 871FB873 FD64DC4B 0A1D844C 2C8C3DB4 0CD79A03
38458370 5B178A42 E0F404B0 18D941CF 76A3DC9A 8205D75A
FA859F80 66138D39 05B3D126 9ACED1F9 837CBA95 3E290B0F
704F0F44 C8C0E284 0B2DBA78 736A8336 EF9126BE 0FA5E8DC
E03B126A E0FFFB91 B156BA56 01160B9F 2BA01109 719EBFAC
60CAD21F B9724846 642FC401 6BF8DBAE 210004C9 9FF9DE60
983B419A 841447C8 329D55E3 2F635737 2B83FB5D 9DB37A94
74A257B7 9234C89C B53E3CC9 87A8FEC1 37DC0ABB 606E2857
A0B6245C 7BE12ADC 1CD92A13 D18BADB5 BF68F3EA AB104713
ADE442E6 8DBB7E8E CF81F2F3 F1F90253 88E7EBD6 4748C336
A8F670FA 56A79545 A9431A83 9E44626D EA90F3D7 0AA77F6A
23200C47 CC2073C6 5E558BE5 DEFEBC0E 6F1FD465 63CAACDF
211106BF CC07AB22 033266CA E205F7AC E4A2AFCE 9714315E
49636B82 D86AB401 8529F1A1 EC710EF6 CCBC7A97 763AE94E
E12E764E 95D4A187 8B5933EC 6FB33E08 48E5B968 D37D51AD
588397EF F8B23FAD 7265702A D907DF4D 01812839 15DE47F8

MacKey is
5E45 D05A8893 A091649A B6380F9C

Mtag is
                              FF34 357B7B2C 137FE95F B69D704A

KeyData is
                                                  32F728CC 3A650047
        83BE5F13 CFB59D69 4FB77A9F 2B20221F B5829A8D 55925232
        AC4FCE9D E1977245 D8044B7E 143DFC64 BD17CE1E C821F6C9

==

dhEphem(224)
----
rU is
                                                        22E62601
        DBFFD067 08A680F7 47F361F7 6D8F4F72 1A0548E4 83294B0C

tU is
                         1B3A6345 1BD886E6 99E67B49 4E288BD7
        F8E0D370 BADDA7A0 EFD2FDE7 D8F66145 CC9F2804 19975EB8
        08877C8A 4C0C8E0B D48D4A54 01EB1E87 76BFEEE1 34C03831
        AC273CD9 D635AB0C E006A42A 887E3F52 FB8766B6 50F38078
        BC8EE858 0CEFE243 968CFC4F 8DC3DB08 4554171D 41BF2E86
        1B7BB4D6 9DD0E01E A387CBAA 5CA672AF CBE8BDB9 D62D4CE1
        5F17DD36 F91ED1EE DD65CA4A 06455CB9 4CD40A52 EC360E84
        B3C926E2 2C4380A3 BF309D56 849768B7 F52CFDF6 55FD053A
        7EF70697 9E7E5806 B17DFAE5 3AD2A5BC 568EBB52 9A7A61D6
        8D256F8F C97C074A 861D827E 2EBC8C61 34553115 B70E7103
        920AA16D 85E52BCB AB8D786A 68178FA8 FF7C2F5C 71648D6F

rV is
                                                        4FF3BC96
        C7FC6A6D 71D3B363 800A7CDF EF6FC41B 4417EA15 353B7590

tV is
                         4DCEE992 A9762A13 F2F83844 AD3D77EE
        0E31C971 8B3DB6C2 035D3961 182C3E0B A247EC41 82D760CD
        48D99599 970622A1 881BBA2D C822939C 78C3912C 6661FA54
        38B20766 222B75E2 4C2E3AD0 C7287236 129525EE 15B5DD79
        98AA04C4 A9696CAC D7172083 A97A8166 4EAD2C47 9E444E4C

```
        0654CC19 E28D7703 CEE8DACD 6126F5D6 65EC52C6 7255DB92
        014B037E B621A2AC 8E365DE0 71FFC140 0ACF077A 12913DD8
        DE894734 37AB7BA3 46743C1B 215DD9C1 2164A7E4 053118D1
        99BEC8EF 6FC56117 0C84C87D 10EE9A67 4A1FA8FF E13BDFBA
        1D44DE48 946D68DC 0CDD7776 35A7AB5B FB1E4BB7 B856F968
        27734C18 4138E915 D9C3002E BCE53120 546A7E20 02142B6C



-------------------------------------------------------------
no Key Confirmation
Z is
                         34D9BDDC 1B42176C 313FEA03 4C21034D
        074A6313 BB4ECDB3 703FFF42 4567A46B DF75530E DE0A9DA5
        229DE7D7 6732286C BC0F91DA 4C3C852F C099C679 531D94C7
        8AB03D9D ECB0A4E4 CA8B2BB4 591C4021 CF8CE3A2 0A541D33
        994017D0 200AE2C9 516E2FF5 14577926 9E862B0F B474A2D5
        6DC31ED5 69A7700B 4C4AB16B 22A45513 531EF523 D7121207
        7B5A169B DEFFAD7A D9608284 C7795B6D 5A5183B8 7066DE17
        D8D671C9 EBD8EC89 544D45EC 061593D4 42C62AB9 CE3B1CB9
        943A1D23 A5EA3BCF 21A01471 E67E003E 7F8A69C7 28BE490B
        2FC88CFE B92DB6A2 15E5D03C 17C464C9 AC1A46E2 03E13F95
        2995FB03 C69D3CC4 7FCB510B 6998FFD3 AA6DE73C F9F63869


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


KDFval is
                                                 062C10DC 635B39E6
        A0BE7414 3E031B66 73C867AC E155864C 258B1CD3 E41EE590
        451402BE E00CF4F9 3F1991A8 3D6A07E8 4A327801 E3FEA3F5


KeyData is
                                                 062C10DC 635B39E6
        A0BE7414 3E031B66 73C867AC E155864C 258B1CD3 E41EE590
        451402BE E00CF4F9 3F1991A8 3D6A07E8 4A327801 E3FEA3F5


=============================================================


dhHybridOneFlow(224)
```

```
------------------------------------------------------------
xU is
                                                       147DEE0E
        D04013C1 4CCAF302 3D22FD5A 80EBAEEF 077D14B8 73E55A1E


yU is
                         7908A13F 426095A1 95A5FBAD 256B967B
        7D3D37DD 65B14752 6ED82F08 86B3DB04 DF03E558 68BCCAD1
        5BC5D7F5 0E9E1EE4 49B2FE5F 61244C47 7ADD70CA 7DA75E02
        CBCA84F0 392D5A3B 16CA7EE7 56566719 26104BE5 0E0FD043
        22DA8CA7 A63061AB 223C2556 79C20FB6 DC9B7532 05290E59
        92DDB4CE 1EB53E85 B95EB988 5874D8F1 D4E7A048 C44F0BCC
        FD4690B2 6553E6CE 66C22057 3117358B B319E46C A3B1DBAA
        117B4E15 81289705 B09742B2 379942AB 47A35D23 24CB5107
        14887475 34367E1E 06FC6012 2F8DD7A9 A0207BF9 A9731CA8
        B14633F3 BE05DA09 C80439DC 394A92DE 78EE9E92 76C4E65A
        BDE526AB 7E943F7A 1735BD00 2440F7DB 6BBBFA62 FAC0CC24


xV is
                                                       60C7AC5C
        F2BFE13D 1DB44D52 7FB33335 F054E016 A1D6DF9D 6682FCBC


yV is
                         70FA12EE D2A6B419 9200DA88 4199FAB6
        3BB53763 E0C464BD 764F826F 96A9DECF 3B1E24CC 470D7B7B
        9AFECD60 24FF9CC6 B5810F1B 5D01C458 0CBA59B6 57160889
        D4B198D7 9208FF15 7AA2FA99 B4DF704B DAF4D142 9D2635A6
        77A2DBEC 79440000 268750DB A341B5E7 069DA17C B0A8DDB3
        FF0FCEE7 D01EC6AF 72F934C6 95DFB6E7 88863DA8 48724078
        3FDDE1CE CB957949 678AE03A 273AC142 DF71A7B5 757A3E2C
        6A8D74E4 45D27C59 AA12E74C 20223529 E0DBE35C 2FC76E07
        E606DAF1 78DDC103 DAEA3477 8C4EFF11 7FD5DF02 AC3AECC9
        F2B3FD8F 966C9C80 CB8622D6 18F18539 FEFCB1EC B5AA8BF8
        2E58A6BF DE373924 22CB464D 5162C4FA E6CF8FC4 596F0E9A


rU is
                                                       0905FE81
        D37940A5 189BC17D 6EE881B7 7C9271D7 FA841B58 FD0C837C


tU is
                         1B4AFAEE 9FDC0C0C 88FC3EB8 0A9A3B7A
```

5655AA13 AA88070F 06CA2C59 D4C3E62C 807D23E8 725A1207
DEA68C47 84AC5FB9 0817CB04 03CA14E4 F4C24024 9E1665B0
B94A30AC 5C169EBE 944F178A 6E26BBF9 14F3FC66 446641CE
A707807C 10A73CAF 2D761BEC 02199C0F 8C934252 2EE0FE15
59D6DD50 0178A25E 0CC0AC04 24D51417 0BD09D5C D4991A31
317C5C6A D4D0DFF9 7476661A 6C2F8A4C A0624C48 135B5861
5FC869FC 06C13554 5F98C7F3 8FCE584D E44640A2 B8EA8E1B
3A39E842 EDAAF1B3 010BA92D 9A233570 F405B2E5 A7989C95
E11888B0 15C6ED9E 98A7DBE7 35774D74 3360DE86 0EFF2B7A
161D2E46 83BEC19D 07906FD7 576E385C 1110475C A3BEBF79

---

no Key Confirmation
Zs is

3CE884B2 2C752D6F 28AB68AC 44D80AAA
8FD3F7F8 9A8DEAFB A40E1029 FDCE4F4E 94607DD1 2A20EDBD
83B51666 125DAC13 B026FBDA 601190A9 FD246710 02C2A100
7C3639EA 07CA589D F798FB23 719E16DD 3A62EDC4 2AA88AAA
59E358F9 F6184A12 9885874D F0223592 9A42D45F 229F56DD
04860EC7 D15F96E2 65AEDF68 40CD2E90 42620FA4 34299D36
4B927224 07879F3A A7C1F221 EB8741A7 E08F8ECD 754F44BF
9CB955C1 5C309784 276F9281 D631A2FD 1CBBE095 5E7F04C1
E41C04CA FD6B4297 500788A8 BC472608 95475D46 A0BE7F80
C5E350D0 F93F27F6 3D430BAB 9D4B9ACC D173786B FC1A5AF9
FA463833 C5DB27C1 1B3C77FC 0F8088CE C6A39606 88A6637A

Ze is

191F1D5F 78E099FF 59DC903D 3D9712FF
6D59B729 BB88DE8A 99F264B9 6B7B8B43 9E717E4E B70065AE
1CE8117D 5ED3EC3A 00C05B5A 2B17856F 04769676 3613057B
B92A5893 7E2C2202 C8059A35 008BC825 9256B092 90089BEE
D21B4696 F892FE67 E512B918 3C28BE5A E0003A80 2956FB27
11C6867C 9FD56862 9B674D77 1E6571DA 66C95DB6 FB27561D
F802000F 8AD3492D 9C5FFD75 83705DEA 11D8F05C D3F0659D
3E2980AA 48A0EEAF 92B37FA0 5DDDC006 624F95DB 296597E0
BA8F4EFC 0F8DA4E9 739B547A E7FD1494 B384CF84 CDBA7723
87816F97 CFBF8D0E 97397E53 161C4174 4ACE28CA 70629E59
8BB86E2A A2FB1405 C24B9100 3715C6D0 9CE27EA2 AA8E55CB

Z is

191F1D5F 78E099FF

59DC903D 3D9712FF 6D59B729 BB88DE8A 99F264B9 6B7B8B43
9E717E4E B70065AE 1CE8117D 5ED3EC3A 00C05B5A 2B17856F
04769676 3613057B B92A5893 7E2C2202 C8059A35 008BC825
9256B092 90089BEE D21B4696 F892FE67 E512B918 3C28BE5A
E0003A80 2956FB27 11C6867C 9FD56862 9B674D77 1E6571DA
66C95DB6 FB27561D F802000F 8AD3492D 9C5FFD75 83705DEA
11D8F05C D3F0659D 3E2980AA 48A0EEAF 92B37FA0 5DDDC006
624F95DB 296597E0 BA8F4EFC 0F8DA4E9 739B547A E7FD1494
B384CF84 CDBA7723 87816F97 CFBF8D0E 97397E53 161C4174
4ACE28CA 70629E59 8BB86E2A A2FB1405 C24B9100 3715C6D0
9CE27EA2 AA8E55CB 3CE884B2 2C752D6F 28AB68AC 44D80AAA
8FD3F7F8 9A8DEAFB A40E1029 FDCE4F4E 94607DD1 2A20EDBD
83B51666 125DAC13 B026FBDA 601190A9 FD246710 02C2A100
7C3639EA 07CA589D F798FB23 719E16DD 3A62EDC4 2AA88AAA
59E358F9 F6184A12 9885874D F0223592 9A42D45F 229F56DD
04860EC7 D15F96E2 65AEDF68 40CD2E90 42620FA4 34299D36
4B927224 07879F3A A7C1F221 EB8741A7 E08F8ECD 754F44BF
9CB955C1 5C309784 276F9281 D631A2FD 1CBBE095 5E7F04C1
E41C04CA FD6B4297 500788A8 BC472608 95475D46 A0BE7F80
C5E350D0 F93F27F6 3D430BAB 9D4B9ACC D173786B FC1A5AF9
FA463833 C5DB27C1 1B3C77FC 0F8088CE C6A39606 88A6637A

OtherInfo is
12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536

KDFval is
8253DF51 0388F119
8F32DB01 F8CD48C2 86636520 5EB6F0C9 88EA95C5 7654AE06
1BCC4D3B 1CFFD8CC F47CDDE9 6B03156A 7F20733E C6D71700

KeyData is
8253DF51 0388F119
8F32DB01 F8CD48C2 86636520 5EB6F0C9 88EA95C5 7654AE06
1BCC4D3B 1CFFD8CC F47CDDE9 6B03156A 7F20733E C6D71700

Scheme Initiator, Key Confirmation Provider: U to V
NonceV is
65C7DF84
727EA13C 1BE01470 9BB3DA9B A463BBC2 EBEFD0C9 347D93A3

Zs is

```
                    3CE884B2 2C752D6F 28AB68AC 44D80AAA
        8FD3F7F8 9A8DEAFB A40E1029 FDCE4F4E 94607DD1 2A20EDBD
        83B51666 125DAC13 B026FBDA 601190A9 FD246710 02C2A100
        7C3639EA 07CA589D F798FB23 719E16DD 3A62EDC4 2AA88AAA
        59E358F9 F6184A12 9885874D F0223592 9A42D45F 229F56DD
        04860EC7 D15F96E2 65AEDF68 40CD2E90 42620FA4 34299D36
        4B927224 07879F3A A7C1F221 EB8741A7 E08F8ECD 754F44BF
        9CB955C1 5C309784 276F9281 D631A2FD 1CBBE095 5E7F04C1
        E41C04CA FD6B4297 500788A8 BC472608 95475D46 A0BE7F80
        C5E350D0 F93F27F6 3D430BAB 9D4B9ACC D173786B FC1A5AF9
        FA463833 C5DB27C1 1B3C77FC 0F8088CE C6A39606 88A6637A
```

Ze is

```
                    191F1D5F 78E099FF 59DC903D 3D9712FF
        6D59B729 BB88DE8A 99F264B9 6B7B8B43 9E717E4E B70065AE
        1CE8117D 5ED3EC3A 00C05B5A 2B17856F 04769676 3613057B
        B92A5893 7E2C2202 C8059A35 008BC825 9256B092 90089BEE
        D21B4696 F892FE67 E512B918 3C28BE5A E0003A80 2956FB27
        11C6867C 9FD56862 9B674D77 1E6571DA 66C95DB6 FB27561D
        F802000F 8AD3492D 9C5FFD75 83705DEA 11D8F05C D3F0659D
        3E2980AA 48A0EEAF 92B37FA0 5DDDC006 624F95DB 296597E0
        BA8F4EFC 0F8DA4E9 739B547A E7FD1494 B384CF84 CDBA7723
        87816F97 CFBF8D0E 97397E53 161C4174 4ACE28CA 70629E59
        8BB86E2A A2FB1405 C24B9100 3715C6D0 9CE27EA2 AA8E55CB
```

Z is

```
                                        191F1D5F 78E099FF
        59DC903D 3D9712FF 6D59B729 BB88DE8A 99F264B9 6B7B8B43
        9E717E4E B70065AE 1CE8117D 5ED3EC3A 00C05B5A 2B17856F
        04769676 3613057B B92A5893 7E2C2202 C8059A35 008BC825
        9256B092 90089BEE D21B4696 F892FE67 E512B918 3C28BE5A
        E0003A80 2956FB27 11C6867C 9FD56862 9B674D77 1E6571DA
        66C95DB6 FB27561D F802000F 8AD3492D 9C5FFD75 83705DEA
        11D8F05C D3F0659D 3E2980AA 48A0EEAF 92B37FA0 5DDDC006
        624F95DB 296597E0 BA8F4EFC 0F8DA4E9 739B547A E7FD1494
        B384CF84 CDBA7723 87816F97 CFBF8D0E 97397E53 161C4174
        4ACE28CA 70629E59 8BB86E2A A2FB1405 C24B9100 3715C6D0
        9CE27EA2 AA8E55CB 3CE884B2 2C752D6F 28AB68AC 44D80AAA
        8FD3F7F8 9A8DEAFB A40E1029 FDCE4F4E 94607DD1 2A20EDBD
        83B51666 125DAC13 B026FBDA 601190A9 FD246710 02C2A100
        7C3639EA 07CA589D F798FB23 719E16DD 3A62EDC4 2AA88AAA
```

59E358F9 F6184A12 9885874D F0223592 9A42D45F 229F56DD
04860EC7 D15F96E2 65AEDF68 40CD2E90 42620FA4 34299D36
4B927224 07879F3A A7C1F221 EB8741A7 E08F8ECD 754F44BF
9CB955C1 5C309784 276F9281 D631A2FD 1CBBE095 5E7F04C1
E41C04CA FD6B4297 500788A8 BC472608 95475D46 A0BE7F80
C5E350D0 F93F27F6 3D430BAB 9D4B9ACC D173786B FC1A5AF9
FA463833 C5DB27C1 1B3C77FC 0F8088CE C6A39606 88A6637A

OtherInfo is
12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536

KDFval is
8253 DF510388 F1198F32 DB01F8CD 48C28663 65205EB6
F0C988EA 95C57654 AE061BCC 4D3B1CFF D8CCF47C DDE96B03
156A7F20 733EC6D7 17002293 8048587B AA3108E4 132D7798

MacData is
4B435F31 5F55414C 49434542
4F424259 1B4AFAEE 9FDC0C0C 88FC3EB8 0A9A3B7A 5655AA13
AA88070F 06CA2C59 D4C3E62C 807D23E8 725A1207 DEA68C47
84AC5FB9 0817CB04 03CA14E4 F4C24024 9E1665B0 B94A30AC
5C169EBE 944F178A 6E26BBF9 14F3FC66 446641CE A707807C
10A73CAF 2D761BEC 02199C0F 8C934252 2EE0FE15 59D6DD50
0178A25E 0CC0AC04 24D51417 0BD09D5C D4991A31 317C5C6A
D4D0DFF9 7476661A 6C2F8A4C A0624C48 135B5861 5FC869FC
06C13554 5F98C7F3 8FCE584D E44640A2 B8EA8E1B 3A39E842
EDAAF1B3 010BA92D 9A233570 F405B2E5 A7989C95 E11888B0
15C6ED9E 98A7DBE7 35774D74 3360DE86 0EFF2B7A 161D2E46
83BEC19D 07906FD7 576E385C 1110475C A3BEBF79 65C7DF84
727EA13C 1BE01470 9BB3DA9B A463BBC2 EBEFD0C9 347D93A3

MacKey is
8253 DF510388 F1198F32 DB01F8CD

Mtag is
657F B818EF8D C8C15D36 F61B49A1

KeyData is
48C28663 65205EB6
F0C988EA 95C57654 AE061BCC 4D3B1CFF D8CCF47C DDE96B03

156A7F20 733EC6D7 17002293 8048587B AA3108E4 132D7798

Scheme Responder, Key Confirmation Provider: V to U
NonceU is

65C7DF84
727EA13C 1BE01470 9BB3DA9B A463BBC2 EBEFD0C9 347D93A3

Zs is

3CE884B2 2C752D6F 28AB68AC 44D80AAA
8FD3F7F8 9A8DEAFB A40E1029 FDCE4F4E 94607DD1 2A20EDBD
83B51666 125DAC13 B026FBDA 601190A9 FD246710 02C2A100
7C3639EA 07CA589D F798FB23 719E16DD 3A62EDC4 2AA88AAA
59E358F9 F6184A12 9885874D F0223592 9A42D45F 229F56DD
04860EC7 D15F96E2 65AEDF68 40CD2E90 42620FA4 34299D36
4B927224 07879F3A A7C1F221 EB8741A7 E08F8ECD 754F44BF
9CB955C1 5C309784 276F9281 D631A2FD 1CBBE095 5E7F04C1
E41C04CA FD6B4297 500788A8 BC472608 95475D46 A0BE7F80
C5E350D0 F93F27F6 3D430BAB 9D4B9ACC D173786B FC1A5AF9
FA463833 C5DB27C1 1B3C77FC 0F8088CE C6A39606 88A6637A

Ze is

191F1D5F 78E099FF 59DC903D 3D9712FF
6D59B729 BB88DE8A 99F264B9 6B7B8B43 9E717E4E B70065AE
1CE8117D 5ED3EC3A 00C05B5A 2B17856F 04769676 3613057B
B92A5893 7E2C2202 C8059A35 008BC825 9256B092 90089BEE
D21B4696 F892FE67 E512B918 3C28BE5A E0003A80 2956FB27
11C6867C 9FD56862 9B674D77 1E6571DA 66C95DB6 FB27561D
F802000F 8AD3492D 9C5FFD75 83705DEA 11D8F05C D3F0659D
3E2980AA 48A0EEAF 92B37FA0 5DDDC006 624F95DB 296597E0
BA8F4EFC 0F8DA4E9 739B547A E7FD1494 B384CF84 CDBA7723
87816F97 CFBF8D0E 97397E53 161C4174 4ACE28CA 70629E59
8BB86E2A A2FB1405 C24B9100 3715C6D0 9CE27EA2 AA8E55CB

Z is

191F1D5F 78E099FF
59DC903D 3D9712FF 6D59B729 BB88DE8A 99F264B9 6B7B8B43
9E717E4E B70065AE 1CE8117D 5ED3EC3A 00C05B5A 2B17856F
04769676 3613057B B92A5893 7E2C2202 C8059A35 008BC825
9256B092 90089BEE D21B4696 F892FE67 E512B918 3C28BE5A

E0003A80 2956FB27 11C6867C 9FD56862 9B674D77 1E6571DA
66C95DB6 FB27561D F802000F 8AD3492D 9C5FFD75 83705DEA
11D8F05C D3F0659D 3E2980AA 48A0EEAF 92B37FA0 5DDDC006
624F95DB 296597E0 BA8F4EFC 0F8DA4E9 739B547A E7FD1494
B384CF84 CDBA7723 87816F97 CFBF8D0E 97397E53 161C4174
4ACE28CA 70629E59 8BB86E2A A2FB1405 C24B9100 3715C6D0
9CE27EA2 AA8E55CB 3CE884B2 2C752D6F 28AB68AC 44D80AAA
8FD3F7F8 9A8DEAFB A40E1029 FDCE4F4E 94607DD1 2A20EDBD
83B51666 125DAC13 B026FBDA 601190A9 FD246710 02C2A100
7C3639EA 07CA589D F798FB23 719E16DD 3A62EDC4 2AA88AAA
59E358F9 F6184A12 9885874D F0223592 9A42D45F 229F56DD
04860EC7 D15F96E2 65AEDF68 40CD2E90 42620FA4 34299D36
4B927224 07879F3A A7C1F221 EB8741A7 E08F8ECD 754F44BF
9CB955C1 5C309784 276F9281 D631A2FD 1CBBE095 5E7F04C1
E41C04CA FD6B4297 500788A8 BC472608 95475D46 A0BE7F80
C5E350D0 F93F27F6 3D430BAB 9D4B9ACC D173786B FC1A5AF9
FA463833 C5DB27C1 1B3C77FC 0F8088CE C6A39606 88A6637A

OtherInfo is
12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536

KDFval is
8253 DF510388 F1198F32 DB01F8CD 48C28663 65205EB6
F0C988EA 95C57654 AE061BCC 4D3B1CFF D8CCF47C DDE96B03
156A7F20 733EC6D7 17002293 8048587B AA3108E4 132D7798

MacData is
4B435F31 5F56424F
42425941 4C494345 1B4AFAEE 9FDC0C0C 88FC3EB8 0A9A3B7A
5655AA13 AA88070F 06CA2C59 D4C3E62C 807D23E8 725A1207
DEA68C47 84AC5FB9 0817CB04 03CA14E4 F4C24024 9E1665B0
B94A30AC 5C169EBE 944F178A 6E26BBF9 14F3FC66 446641CE
A707807C 10A73CAF 2D761BEC 02199C0F 8C934252 2EE0FE15
59D6DD50 0178A25E 0CC0AC04 24D51417 0BD09D5C D4991A31
317C5C6A D4D0DFF9 7476661A 6C2F8A4C A0624C48 135B5861
5FC869FC 06C13554 5F98C7F3 8FCE584D E44640A2 B8EA8E1B
3A39E842 EDAAF1B3 010BA92D 9A233570 F405B2E5 A7989C95
E11888B0 15C6ED9E 98A7DBE7 35774D74 3360DE86 0EFF2B7A
161D2E46 83BEC19D 07906FD7 576E385C 1110475C A3BEBF79

MacKey is
8253 DF510388 F1198F32 DB01F8CD

Mtag is
                              8AC9 9B360F90 9951E275 5936107C

KeyData is
                                                48C28663 65205EB6
        F0C988EA 95C57654 AE061BCC 4D3B1CFF D8CCF47C DDE96B03
        156A7F20 733EC6D7 17002293 8048587B AA3108E4 132D7798

Scheme Initiator, Key Confirmation Bilateral
NonceV is
                                                              65C7DF84
        727EA13C 1BE01470 9BB3DA9B A463BBC2 EBEFD0C9 347D93A3

Zs is
                             3CE884B2 2C752D6F 28AB68AC 44D80AAA
        8FD3F7F8 9A8DEAFB A40E1029 FDCE4F4E 94607DD1 2A20EDBD
        83B51666 125DAC13 B026FBDA 601190A9 FD246710 02C2A100
        7C3639EA 07CA589D F798FB23 719E16DD 3A62EDC4 2AA88AAA
        59E358F9 F6184A12 9885874D F0223592 9A42D45F 229F56DD
        04860EC7 D15F96E2 65AEDF68 40CD2E90 42620FA4 34299D36
        4B927224 07879F3A A7C1F221 EB8741A7 E08F8ECD 754F44BF
        9CB955C1 5C309784 276F9281 D631A2FD 1CBBE095 5E7F04C1
        E41C04CA FD6B4297 500788A8 BC472608 95475D46 A0BE7F80
        C5E350D0 F93F27F6 3D430BAB 9D4B9ACC D173786B FC1A5AF9
        FA463833 C5DB27C1 1B3C77FC 0F8088CE C6A39606 88A6637A

Ze is
                             191F1D5F 78E099FF 59DC903D 3D9712FF
        6D59B729 BB88DE8A 99F264B9 6B7B8B43 9E717E4E B70065AE
        1CE8117D 5ED3EC3A 00C05B5A 2B17856F 04769676 3613057B
        B92A5893 7E2C2202 C8059A35 008BC825 9256B092 90089BEE
        D21B4696 F892FE67 E512B918 3C28BE5A E0003A80 2956FB27
        11C6867C 9FD56862 9B674D77 1E6571DA 66C95DB6 FB27561D
        F802000F 8AD3492D 9C5FFD75 83705DEA 11D8F05C D3F0659D
        3E2980AA 48A0EEAF 92B37FA0 5DDDC006 624F95DB 296597E0
        BA8F4EFC 0F8DA4E9 739B547A E7FD1494 B384CF84 CDBA7723
        87816F97 CFBF8D0E 97397E53 161C4174 4ACE28CA 70629E59

```
        8BB86E2A A2FB1405 C24B9100 3715C6D0 9CE27EA2 AA8E55CB


Z is
                                                191F1D5F 78E099FF
        59DC903D 3D9712FF 6D59B729 BB88DE8A 99F264B9 6B7B8B43
        9E717E4E B70065AE 1CE8117D 5ED3EC3A 00C05B5A 2B17856F
        04769676 3613057B B92A5893 7E2C2202 C8059A35 008BC825
        9256B092 90089BEE D21B4696 F892FE67 E512B918 3C28BE5A
        E0003A80 2956FB27 11C6867C 9FD56862 9B674D77 1E6571DA
        66C95DB6 FB27561D F802000F 8AD3492D 9C5FFD75 83705DEA
        11D8F05C D3F0659D 3E2980AA 48A0EEAF 92B37FA0 5DDDC006
        624F95DB 296597E0 BA8F4EFC 0F8DA4E9 739B547A E7FD1494
        B384CF84 CDBA7723 87816F97 CFBF8D0E 97397E53 161C4174
        4ACE28CA 70629E59 8BB86E2A A2FB1405 C24B9100 3715C6D0
        9CE27EA2 AA8E55CB 3CE884B2 2C752D6F 28AB68AC 44D80AAA
        8FD3F7F8 9A8DEAFB A40E1029 FDCE4F4E 94607DD1 2A20EDBD
        83B51666 125DAC13 B026FBDA 601190A9 FD246710 02C2A100
        7C3639EA 07CA589D F798FB23 719E16DD 3A62EDC4 2AA88AAA
        59E358F9 F6184A12 9885874D F0223592 9A42D45F 229F56DD
        04860EC7 D15F96E2 65AEDF68 40CD2E90 42620FA4 34299D36
        4B927224 07879F3A A7C1F221 EB8741A7 E08F8ECD 754F44BF
        9CB955C1 5C309784 276F9281 D631A2FD 1CBBE095 5E7F04C1
        E41C04CA FD6B4297 500788A8 BC472608 95475D46 A0BE7F80
        C5E350D0 F93F27F6 3D430BAB 9D4B9ACC D173786B FC1A5AF9
        FA463833 C5DB27C1 1B3C77FC 0F8088CE C6A39606 88A6637A


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


KDFval is
            8253 DF510388 F1198F32 DB01F8CD 48C28663 65205EB6
        F0C988EA 95C57654 AE061BCC 4D3B1CFF D8CCF47C DDE96B03
        156A7F20 733EC6D7 17002293 8048587B AA3108E4 132D7798


U2V
----------------
MacData is
                                    4B435F32 5F55414C 49434542
        4F424259 1B4AFAEE 9FDC0C0C 88FC3EB8 0A9A3B7A 5655AA13
        AA88070F 06CA2C59 D4C3E62C 807D23E8 725A1207 DEA68C47
        84AC5FB9 0817CB04 03CA14E4 F4C24024 9E1665B0 B94A30AC
        5C169EBE 944F178A 6E26BBF9 14F3FC66 446641CE A707807C
```

```
        10A73CAF 2D761BEC 02199C0F 8C934252 2EE0FE15 59D6DD50
        0178A25E 0CC0AC04 24D51417 0BD09D5C D4991A31 317C5C6A
        D4D0DFF9 7476661A 6C2F8A4C A0624C48 135B5861 5FC869FC
        06C13554 5F98C7F3 8FCE584D E44640A2 B8EA8E1B 3A39E842
        EDAAF1B3 010BA92D 9A233570 F405B2E5 A7989C95 E11888B0
        15C6ED9E 98A7DBE7 35774D74 3360DE86 0EFF2B7A 161D2E46
        83BEC19D 07906FD7 576E385C 1110475C A3BEBF79 65C7DF84
        727EA13C 1BE01470 9BB3DA9B A463BBC2 EBEFD0C9 347D93A3


MacKey is
                            8253 DF510388 F1198F32 DB01F8CD


Mtag is
                            74C6 ACB9F15B B50A82BB 0E7ED0BA


V2U
----------------
MacData is
                                  4B435F32 5F56424F 42425941
        4C494345 65C7DF84 727EA13C 1BE01470 9BB3DA9B A463BBC2
        EBEFD0C9 347D93A3 1B4AFAEE 9FDC0C0C 88FC3EB8 0A9A3B7A
        5655AA13 AA88070F 06CA2C59 D4C3E62C 807D23E8 725A1207
        DEA68C47 84AC5FB9 0817CB04 03CA14E4 F4C24024 9E1665B0
        B94A30AC 5C169EBE 944F178A 6E26BBF9 14F3FC66 446641CE
        A707807C 10A73CAF 2D761BEC 02199C0F 8C934252 2EE0FE15
        59D6DD50 0178A25E 0CC0AC04 24D51417 0BD09D5C D4991A31
        317C5C6A D4D0DFF9 7476661A 6C2F8A4C A0624C48 135B5861
        5FC869FC 06C13554 5F98C7F3 8FCE584D E44640A2 B8EA8E1B
        3A39E842 EDAAF1B3 010BA92D 9A233570 F405B2E5 A7989C95
        E11888B0 15C6ED9E 98A7DBE7 35774D74 3360DE86 0EFF2B7A
        161D2E46 83BEC19D 07906FD7 576E385C 1110475C A3BEBF79


MacKey is
                            8253 DF510388 F1198F32 DB01F8CD


Mtag is
                            0AB8 F4DA3366 AA310AEF 3FA6C2BF


KeyData is
                                        48C28663 65205EB6
```

```
        F0C988EA 95C57654 AE061BCC 4D3B1CFF D8CCF47C DDE96B03
        156A7F20 733EC6D7 17002293 8048587B AA3108E4 132D7798


================================================================


MQV1(224)
----------------------------------------------------------
xU is
                                                        7011F347
        CC4234FA 9A2205DA FBF9A35E C01527E5 A2A89D3A 680B0E13


yU is
                         4A543193 3B31F5A8 B0829C97 41E58570
        F7AFDFBF 11E9BB1F 51B7DDC7 60F09BBD 48E97778 8665286A
        5B2F0E39 5C526C80 428FF9D6 A203C89D 5EF45FD9 9DFDD462
        E57996C7 7BE8C1BE 2F7C93F5 86A5D2D5 F9F06635 148F2952
        DE1C32B0 DAFF608D 32079B52 69AE920F 786A9F36 DDDFA1BE
        A068BB81 7658B1BA 71F3DE9E 85E3FD40 81F11413 23D6263A
        9773C8B6 8B0FD7E2 2C392286 96EABC81 BCCD7C9E 894F0C35
        159FDEDC FC51F8B9 26E95812 470C267F 9FE19B89 9C5F0252
        5289A099 A69A09D6 70D7D26E 0B9D0DB8 16952A4A 338E1D86
        366FD1CC 3F494013 C3DC6E14 5CEE2ECE 8FC7A9A9 CEB62AF6
        413AF549 49B57A0B 90CBDE67 EF14EF80 B8FDF31A 652CC2CE


xV is
                                                        27CFF260
        FC0A0905 0E2324F2 2C2691AE 5E620E80 5D0F19D3 645D8C7B


yV is
                         8B06AEAE AC698CF1 E19131F3 0BD33AE1
        4FF96FCF A323F12F 76195A67 0FA8A15B D022464F 123D34C6
        250B9C51 086A9634 4098492F 38EC7EBF F60E96A0 FA572C97
        7F2531DA 0AD7990D C3C0F4B3 071FCB25 0168DFF9 4C8C2A4E
        1BEC1589 7BD7FEEF 32F7720E 263C4958 CB9353AD 6AF7EBA8
        C225B84F DC307B6F 2317B343 A461D9B7 86B3617B 31DA29BF
        E04A105C F2ABBACC CBC03A8A A5499C15 3620CF3B 32025D81
        3EB5E820 DBF1B22B 111011DD 634DCFA5 7F3E80AA 5464027C
        18E8CF80 7EBBE5E4 C443D050 12DD7523 A40E0B5C E6B55F13
        1ED2857C 9A0B3070 C511BB1A F61B5FFC 03B3742D 88B82F70
        C019A938 D3CBE254 C39F8DB0 62CECEEE 0C3C9C1A 65278877
```

rU is
                                                        0FDE3975
        CD9E579A C7CDC63B A875ED66 4984E5EA 6C020A7C 7261FB9B

tU is
                          92E3125F ED0C73CF AF28B25D E8347B7F
        4D5E4C35 503530D3 B698A1C0 108C8F37 36221083 3AB916CC
        73EC7E63 032A69A4 BA64E164 5D422D0A 65D7BE7F 7E5310E2
        CCAA619B 38D96A5B 7B654B4C 35DC3069 4D13387B 2BFE163E
        4667E5E9 5448A815 9391C34E F503144F 35BCFB80 2FA416FF
        49CAA6D1 96ED4D1E F34BC9E7 01652795 9D7E7A3B 7D1093FD
        6A45A494 38E2CF44 911F40DC AE1519EF E2BD9715 BF3260DD
        945E32D6 9483E172 B96C261C B17965A5 727E237E 2B0D7387
        3ED981B8 66473722 E3E711CC 5C8F7699 764F205F 006494EB
        EB94CDFD FA7F5FAB 50BB772F F287F6AD 816B64F9 890C48E3
        F7826CF1 E878F4D8 5D92B858 DF4FF3FA 8D812FF1 80620A8E

----
no Key Confirmation
Z is
                          3037E3FB D736E213 F5A0D5C4 E8E5BFC4
        3C6349B0 5BA28B6F 8672E95C 57D66310 7DFF7FFA 9B0266D5
        165C1D28 C97E9161 98E974C7 BFDB210F C61F50BB DFB0FCF5
        5EFC16B1 9175CFEF A56E02D1 13364300 0EE5F2F1 8F62C995
        56CFC970 072B4851 91661083 E3560803 96B42E9D 1EAA7AA1
        2246ACE1 49DDB16E 67461986 A39902CF BC1ADA0F C90A4FA2
        3B0E86C4 8366C32A 0D02EF7A D48D61AA 868881FF 27978865
        FD3EFCA6 21C44642 95A22B59 B5B83C9B D7DEFCD1 3144BE1D
        16EF45DF 27C73F07 2DD31298 397B6CD8 F001660D 7B8537B1
        3EEA8E89 66514117 587BD35E EA304D9D 63A476D2 8B4755BB
        D69B2275 77072462 89AA4991 5342B4D0 13F7B24C D407C45E

OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536

KDFval is
                                                3ED26991 1118E045
        08B9BFB5 90F989BA ED03C40F 8496DF28 1883A6FE 6B26D626
        198D87B5 0225D783 152D275A A288BF43 1ED7415B A0C66D4B

KeyData is
                                                3ED26991 1118E045
        08B9BFB5 90F989BA ED03C40F 8496DF28 1883A6FE 6B26D626
        198D87B5 0225D783 152D275A A288BF43 1ED7415B A0C66D4B

Scheme Initiator, Key Confirmation Provider: U to V
NonceV is
                                                        09FFA29C
        B0E33CD4 F24CBC12 D0C9B56C FD461582 3D3F429B 56210155

Z is
                            3037E3FB D736E213 F5A0D5C4 E8E5BFC4
        3C6349B0 5BA28B6F 8672E95C 57D66310 7DFF7FFA 9B0266D5
        165C1D28 C97E9161 98E974C7 BFDB210F C61F50BB DFB0FCF5
        5EFC16B1 9175CFEF A56E02D1 13364300 0EE5F2F1 8F62C995
        56CFC970 072B4851 91661083 E3560803 96B42E9D 1EAA7AA1
        2246ACE1 49DDB16E 67461986 A39902CF BC1ADA0F C90A4FA2
        3B0E86C4 8366C32A 0D02EF7A D48D61AA 868881FF 27978865
        FD3EFCA6 21C44642 95A22B59 B5B83C9B D7DEFCD1 3144BE1D
        16EF45DF 27C73F07 2DD31298 397B6CD8 F001660D 7B8537B1
        3EEA8E89 66514117 587BD35E EA304D9D 63A476D2 8B4755BB
        D69B2275 77072462 89AA4991 5342B4D0 13F7B24C D407C45E

OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536

KDFval is
            3ED2 69911118 E04508B9 BFB590F9 89BAED03 C40F8496
        DF281883 A6FE6B26 D626198D 87B50225 D783152D 275AA288
        BF431ED7 415BA0C6 6D4B9724 E20FE516 F811C654 870F330E

MacData is
                                    4B435F31 5F55414C 49434542
        4F424259 92E3125F ED0C73CF AF28B25D E8347B7F 4D5E4C35
        503530D3 B698A1C0 108C8F37 36221083 3AB916CC 73EC7E63
        032A69A4 BA64E164 5D422D0A 65D7BE7F 7E5310E2 CCAA619B

```
        38D96A5B 7B654B4C 35DC3069 4D13387B 2BFE163E 4667E5E9
        5448A815 9391C34E F503144F 35BCFB80 2FA416FF 49CAA6D1
        96ED4D1E F34BC9E7 01652795 9D7E7A3B 7D1093FD 6A45A494
        38E2CF44 911F40DC AE1519EF E2BD9715 BF3260DD 945E32D6
        9483E172 B96C261C B17965A5 727E237E 2B0D7387 3ED981B8
        66473722 E3E711CC 5C8F7699 764F205F 006494EB EB94CDFD
        FA7F5FAB 50BB772F F287F6AD 816B64F9 890C48E3 F7826CF1
        E878F4D8 5D92B858 DF4FF3FA 8D812FF1 80620A8E 09FFA29C
        B0E33CD4 F24CBC12 D0C9B56C FD461582 3D3F429B 56210155


MacKey is
                            3ED2 69911118 E04508B9 BFB590F9


Mtag is
                            5B61 B254CC2C 9450FB6D 05183980


KeyData is
                                          89BAED03 C40F8496
        DF281883 A6FE6B26 D626198D 87B50225 D783152D 275AA288
        BF431ED7 415BA0C6 6D4B9724 E20FE516 F811C654 870F330E




------------------------------------------------------------
Scheme Responder, Key Confirmation Provider: V to U
NonceU is
                                                    09FFA29C
        B0E33CD4 F24CBC12 D0C9B56C FD461582 3D3F429B 56210155


Z is
                          3037E3FB D736E213 F5A0D5C4 E8E5BFC4
        3C6349B0 5BA28B6F 8672E95C 57D66310 7DFF7FFA 9B0266D5
        165C1D28 C97E9161 98E974C7 BFDB210F C61F50BB DFB0FCF5
        5EFC16B1 9175CFEF A56E02D1 13364300 0EE5F2F1 8F62C995
        56CFC970 072B4851 91661083 E3560803 96B42E9D 1EAA7AA1
        2246ACE1 49DDB16E 67461986 A39902CF BC1ADA0F C90A4FA2
        3B0E86C4 8366C32A 0D02EF7A D48D61AA 868881FF 27978865
        FD3EFCA6 21C44642 95A22B59 B5B83C9B D7DEFCD1 3144BE1D
        16EF45DF 27C73F07 2DD31298 397B6CD8 F001660D 7B8537B1
        3EEA8E89 66514117 587BD35E EA304D9D 63A476D2 8B4755BB
        D69B2275 77072462 89AA4991 5342B4D0 13F7B24C D407C45E
```

```
OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


KDFval is
            3ED2 69911118 E04508B9 BFB590F9 89BAED03 C40F8496
        DF281883 A6FE6B26 D626198D 87B50225 D783152D 275AA288
        BF431ED7 415BA0C6 6D4B9724 E20FE516 F811C654 870F330E


MacData is
                                            4B435F31 5F56424F
        42425941 4C494345 92E3125F ED0C73CF AF28B25D E8347B7F
        4D5E4C35 503530D3 B698A1C0 108C8F37 36221083 3AB916CC
        73EC7E63 032A69A4 BA64E164 5D422D0A 65D7BE7F 7E5310E2
        CCAA619B 38D96A5B 7B654B4C 35DC3069 4D13387B 2BFE163E
        4667E5E9 5448A815 9391C34E F503144F 35BCFB80 2FA416FF
        49CAA6D1 96ED4D1E F34BC9E7 01652795 9D7E7A3B 7D1093FD
        6A45A494 38E2CF44 911F40DC AE1519EF E2BD9715 BF3260DD
        945E32D6 9483E172 B96C261C B17965A5 727E237E 2B0D7387
        3ED981B8 66473722 E3E711CC 5C8F7699 764F205F 006494EB
        EB94CDFD FA7F5FAB 50BB772F F287F6AD 816B64F9 890C48E3
        F7826CF1 E878F4D8 5D92B858 DF4FF3FA 8D812FF1 80620A8E


MacKey is
                                3ED2 69911118 E04508B9 BFB590F9


Mtag is
                                58BF 62914394 5EC13797 0FAAA2B0


KeyData is
                                            89BAED03 C40F8496
        DF281883 A6FE6B26 D626198D 87B50225 D783152D 275AA288
        BF431ED7 415BA0C6 6D4B9724 E20FE516 F811C654 870F330E




-------------------------------------------------------------
Scheme Initiator, Key Confirmation Bilateral
NonceV is
```

```
                                                        09FFA29C
        B0E33CD4 F24CBC12 D0C9B56C FD461582 3D3F429B 56210155


Z is
                         3037E3FB D736E213 F5A0D5C4 E8E5BFC4
        3C6349B0 5BA28B6F 8672E95C 57D66310 7DFF7FFA 9B0266D5
        165C1D28 C97E9161 98E974C7 BFDB210F C61F50BB DFB0FCF5
        5EFC16B1 9175CFEF A56E02D1 13364300 0EE5F2F1 8F62C995
        56CFC970 072B4851 91661083 E3560803 96B42E9D 1EAA7AA1
        2246ACE1 49DDB16E 67461986 A39902CF BC1ADA0F C90A4FA2
        3B0E86C4 8366C32A 0D02EF7A D48D61AA 868881FF 27978865
        FD3EFCA6 21C44642 95A22B59 B5B83C9B D7DEFCD1 3144BE1D
        16EF45DF 27C73F07 2DD31298 397B6CD8 F001660D 7B8537B1
        3EEA8E89 66514117 587BD35E EA304D9D 63A476D2 8B4755BB
        D69B2275 77072462 89AA4991 5342B4D0 13F7B24C D407C45E


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


KDFval is
            3ED2 69911118 E04508B9 BFB590F9 89BAED03 C40F8496
        DF281883 A6FE6B26 D626198D 87B50225 D783152D 275AA288
        BF431ED7 415BA0C6 6D4B9724 E20FE516 F811C654 870F330E


U2V
----------------
MacData is
                                    4B435F32 5F55414C 49434542
        4F424259 92E3125F ED0C73CF AF28B25D E8347B7F 4D5E4C35
        503530D3 B698A1C0 108C8F37 36221083 3AB916CC 73EC7E63
        032A69A4 BA64E164 5D422D0A 65D7BE7F 7E5310E2 CCAA619B
        38D96A5B 7B654B4C 35DC3069 4D13387B 2BFE163E 4667E5E9
        5448A815 9391C34E F503144F 35BCFB80 2FA416FF 49CAA6D1
        96ED4D1E F34BC9E7 01652795 9D7E7A3B 7D1093FD 6A45A494
        38E2CF44 911F40DC AE1519EF E2BD9715 BF3260DD 945E32D6
        9483E172 B96C261C B17965A5 727E237E 2B0D7387 3ED981B8
        66473722 E3E711CC 5C8F7699 764F205F 006494EB EB94CDFD
        FA7F5FAB 50BB772F F287F6AD 816B64F9 890C48E3 F7826CF1
        E878F4D8 5D92B858 DF4FF3FA 8D812FF1 80620A8E 09FFA29C
        B0E33CD4 F24CBC12 D0C9B56C FD461582 3D3F429B 56210155
```

```
MacKey is
                              3ED2 69911118 E04508B9 BFB590F9


Mtag is
                              0038 FA4CC17E F4F359E2 A94C1262


V2U
----------------
MacData is
                                    4B435F32 5F56424F 42425941
        4C494345 09FFA29C B0E33CD4 F24CBC12 D0C9B56C FD461582
        3D3F429B 56210155 92E3125F ED0C73CF AF28B25D E8347B7F
        4D5E4C35 503530D3 B698A1C0 108C8F37 36221083 3AB916CC
        73EC7E63 032A69A4 BA64E164 5D422D0A 65D7BE7F 7E5310E2
        CCAA619B 38D96A5B 7B654B4C 35DC3069 4D13387B 2BFE163E
        4667E5E9 5448A815 9391C34E F503144F 35BCFB80 2FA416FF
        49CAA6D1 96ED4D1E F34BC9E7 01652795 9D7E7A3B 7D1093FD
        6A45A494 38E2CF44 911F40DC AE1519EF E2BD9715 BF3260DD
        945E32D6 9483E172 B96C261C B17965A5 727E237E 2B0D7387
        3ED981B8 66473722 E3E711CC 5C8F7699 764F205F 006494EB
        EB94CDFD FA7F5FAB 50BB772F F287F6AD 816B64F9 890C48E3
        F7826CF1 E878F4D8 5D92B858 DF4FF3FA 8D812FF1 80620A8E


MacKey is
                              3ED2 69911118 E04508B9 BFB590F9


Mtag is
                              B667 31F9DF6D 33B314DB 139B908D


KeyData is
                                                    89BAED03 C40F8496
        DF281883 A6FE6B26 D626198D 87B50225 D783152D 275AA288
        BF431ED7 415BA0C6 6D4B9724 E20FE516 F811C654 870F330E


================================================================


dhOneFlow(224)
----------------------------------------------------------
xV is
```

```
                                                        416AF830
        73842CB6 29468903 B28057F2 C090F872 68C3DBB4 DC203362


yV is
                        7B246ADB 8E0D2311 1AEFBB79 33EDD0DE
        6CE94958 A0EFBA64 8D1ED05F 8FEC2489 F14FDC58 CF6B0851
        44F25732 2FE6D74D FE66A906 5511A270 94AF8A57 9C355BE7
        57847610 F5F36520 8510E4BF D7BFDC7D AE6FEF86 C6BFD7CB
        49E879E6 57DF2D58 3C62D896 39A105B3 AAD295BC 8CEAB3B9
        C437B82D C53C2573 2D468592 11C90475 75C016BA 1219880A
        75EFCF8A 473D4123 0D103F35 AC89F1A7 78095299 EECA2C3C
        56E08236 3EF99A1C A55B8C34 19F311CF 8F2D4433 85018501
        DE948330 815F08E1 D585BEFE AFED6D43 7D8057CE F601DEA8
        CE83C7B6 4F85A71F C2C625A2 C496E7CA 94F20A55 02016832
        66AEF1D5 9319550C DC20F90C 55EDA930 6370B61B 528EF175


rU is
                                                        6DA42BD9
        EA18E9D3 213DC3AA 20DFFE05 A60C46E3 6419FDD5 2691C521


tU is
                        7B61EEE6 3497854B BE476A62 9023A6CA
        5A1EF158 8F9B2C43 4D74CFE3 0D9C14F6 6E18E0A3 FBAB126E
        1F9234B1 F3F7D009 1517A56A C68E0A53 A6F6B0D0 A32BBCFA
        2920CCDC AE2D3CF7 C31E46A6 471B2AFA AEB1EC7C 8E90837C
        8ED1FE8D 2F9134D2 67752225 2DF90079 D5E57818 263B7841
        DB730C79 48D436F1 65DAF613 101C60EF 43092CF1 E8AC300D
        B10DE9BF 852F1FA3 81A6BAE1 67FEA4B8 C60750E5 AF2198D2
        F706BC53 51AA4837 95626C22 C8A4D944 6A7358FB 985FB2D2
        68A44E3F DA996C4D 3C6B03C0 352304B0 711EDDF5 37E97652
        27862D50 66DE99A2 6335606B A04CA815 981638E9 9B625F1D
        D04B1B03 67A363CC 2BA53606 A359BE1B 2C34A4CD C6303FF3




------------------------------------------------------------
no Key Confirmation
Z is
                        2438E8C3 7E8C2524 EDE4D662 C6C365CF
        25014B4E B2E1AE99 96E349C0 221A7349 8B17ADF0 65F79C90
        42C3CB84 D7B46139 863FAC23 7FE3D829 A3C15E32 C697EF4A
        279E4431 971483AB 7959D298 F0035AFA F0A763B6 8E8041CC
```

AC8BE1A1 09D6E300 FB5C5AE0 E2341B81 FD56CB89 8A08CB05
56DD6949 D4896E1C 064AC20A 6B99DEC1 1AB0C99A 78FC5128
070645EC A06641A4 65EEBE2B AF4DC6BC F931EC82 DF1ADD34
72089C63 5FE6135E 06C96E34 212AED8F 66C6C5CB CE0BA6E8
CA43FC93 D5C51F58 7E6C67B8 1BD3E5F7 7527D905 6D4F9AAE
112690DD 07BE2AD0 0DB4A7F5 5D91CCF7 953214EE 4867D29D
60C83441 33FB2BF0 7C4DDAB3 7FF5AA1C 56A272E6 7B1B3945

OtherInfo is
12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536

KDFval is
76E4ECC4 FB7A2AAC
99356AA2 9E4606CD E00D3EDA 3963248C 2E6C4427 A9BC38D7
AFC67A8E 53FD7E09 332F970F DA861DB0 7B5DA918 43197FB6

KeyData is
76E4ECC4 FB7A2AAC
99356AA2 9E4606CD E00D3EDA 3963248C 2E6C4427 A9BC38D7
AFC67A8E 53FD7E09 332F970F DA861DB0 7B5DA918 43197FB6

Scheme Responder, Key Confirmation Provider: V to U
Z is
2438E8C3 7E8C2524 EDE4D662 C6C365CF
25014B4E B2E1AE99 96E349C0 221A7349 8B17ADF0 65F79C90
42C3CB84 D7B46139 863FAC23 7FE3D829 A3C15E32 C697EF4A
279E4431 971483AB 7959D298 F0035AFA F0A763B6 8E8041CC
AC8BE1A1 09D6E300 FB5C5AE0 E2341B81 FD56CB89 8A08CB05
56DD6949 D4896E1C 064AC20A 6B99DEC1 1AB0C99A 78FC5128
070645EC A06641A4 65EEBE2B AF4DC6BC F931EC82 DF1ADD34
72089C63 5FE6135E 06C96E34 212AED8F 66C6C5CB CE0BA6E8
CA43FC93 D5C51F58 7E6C67B8 1BD3E5F7 7527D905 6D4F9AAE
112690DD 07BE2AD0 0DB4A7F5 5D91CCF7 953214EE 4867D29D
60C83441 33FB2BF0 7C4DDAB3 7FF5AA1C 56A272E6 7B1B3945

OtherInfo is
12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536

```
KDFval is
            76E4 ECC4FB7A 2AAC9935 6AA29E46 06CDE00D 3EDA3963
        248C2E6C 4427A9BC 38D7AFC6 7A8E53FD 7E09332F 970FDA86
        1DB07B5D A9184319 7FB6C884 BB3AC129 5770239B CEC27D44


MacData is
                                               4B435F31 5F56424F
        42425941 4C494345 7B61EEE6 3497854B BE476A62 9023A6CA
        5A1EF158 8F9B2C43 4D74CFE3 0D9C14F6 6E18E0A3 FBAB126E
        1F9234B1 F3F7D009 1517A56A C68E0A53 A6F6B0D0 A32BBCFA
        2920CCDC AE2D3CF7 C31E46A6 471B2AFA AEB1EC7C 8E90837C
        8ED1FE8D 2F9134D2 67752225 2DF90079 D5E57818 263B7841
        DB730C79 48D436F1 65DAF613 101C60EF 43092CF1 E8AC300D
        B10DE9BF 852F1FA3 81A6BAE1 67FEA4B8 C60750E5 AF2198D2
        F706BC53 51AA4837 95626C22 C8A4D944 6A7358FB 985FB2D2
        68A44E3F DA996C4D 3C6B03C0 352304B0 711EDDF5 37E97652
        27862D50 66DE99A2 6335606B A04CA815 981638E9 9B625F1D
        D04B1B03 67A363CC 2BA53606 A359BE1B 2C34A4CD C6303FF3


MacKey is
                             76E4 ECC4FB7A 2AAC9935 6AA29E46


Mtag is
                             B224 8E5755C7 B5AE0824 A5C86A4B


KeyData is
                                               06CDE00D 3EDA3963
        248C2E6C 4427A9BC 38D7AFC6 7A8E53FD 7E09332F 970FDA86
        1DB07B5D A9184319 7FB6C884 BB3AC129 5770239B CEC27D44


============================================================


dhStatic(224)
------------------------------------------------------------
xU is
                                                     4B8D39A0
        5B0538EE 5AE76AF2 0DE2368C 14294CFF C6A92D68 B2B4060A
```

yU is
                        392F0A22 C44BF5D5 C4A34D6B 59B466DF
        D765767E 4A6C3187 AB9A8D0E C068CBC2 BC6C4FA2 9A00E878
        13399A1C 0B73BE8A 5FE4B6A1 F853DC32 A88F6E57 F7765767
        8CB6DA36 9FEB9DB8 8C8103DB 65EDC465 34239291 E93AEF97
        6772E4A0 527FD7D3 A4F91BD7 CB78462B CB53FAA7 CE7EFF0C
        4082EF31 AD8EFD2B 986C0BDE CE2EB893 58425473 0897A84F
        08F1E737 FA4CBA21 C523046C 707D0AD8 8E8621DE 6870B4D6
        8DD85DC5 8B50BDD0 FFBDCB81 373C8671 AC81DE98 1ABBC1DA
        7B39A886 C02640DB 6A21EA76 EBC266A6 6259EADB C318CB6A
        124262AC BA60F3EF 1C4B9A6D 50DAB8DC 7EBB2821 2BFAAF63
        F706AACB 2E145DCB 71E701D6 2305B02D 9CA4BA93 B661B952

xV is
                                                        631F592A
        C6167B55 315EDFCE 55692231 64F43909 BE2CB379 6EA23E34

yV is
                        A77B2E97 54F4F7F2 80DF003B 7DB52CFB
        FDE05377 A5B855C7 C3BDBFC7 07C3B29D 597162B5 01C03D69
        F354D8AB 8C8ACE18 B212F58F DDBF3692 3C19E6BB 8BD060D8
        D34A31A7 34CB18C6 98E10C3C ADFA977D D5AFE370 62537ED1
        ECCCAABD 6770157A 558DE6EF D2C0ED35 BF13D56B 1E86C4E0
        934F02F4 3738AB56 F40B6BD4 D85FD5BF 528DFB40 9B284F6B
        533922FA 3976A92E 460897A1 C4F33D05 0B6E8709 A2756342
        4DF6C18A D9D2FDE6 C20BBC44 6C074629 26FFF730 0EBA0E77
        76A081B9 D8232388 DA73DE1C 4E6C6065 8D7366CE EB219E26
        2087DBA6 0522008E E5DEA7FB 2AC5B61A 4F8FFCF4 B71BD1D0
        5A995945 44BD17A8 FD6C5593 81974E51 171D3923 BEDE072C

---
no Key Confirmation
NonceU is
                                                        5C8CC978
        63DED4FE 6A409929 9F1F4BB2 5626548B 8E838A3E CD03A7A1

Z is
                        49B20245 2DBA6F17 E9AFB666 AD152A12
        E32CFD86 D717912E B11C70B1 294B09AB 6055DC4B 99EEC4A5
        291CEE27 342B342A BFBC8639 DC10584E 0223B098 9E99646A

```
        D720D69E E3F32BC1 1C3D5C40 6022D82C 6300CDEE 2F476C83
        E01D0F9D 7956C2BD E18958C9 23086DF6 3D143524 F884DAA7
        3BE35F2F FC34A290 3E886E19 A4877D00 C138B58B C1B78AA0
        2826CD66 0F51B521 50BAC53C DC19E727 66996810 BAF027C0
        CEC8DF41 D480E0E2 C99C8749 D3AC3E65 4F093CFE 86FB5862
        8F0F6D18 20ACECBF A0D6DCB5 BC6D71BF 382B3DBA 289A733A
        9E64FCFF 43C0C4AC 86DD6429 896D8026 EC701D2E 800270D4
        6CF08922 47839BB7 31C58F75 A6C88D3B FB7D40CD 3A7F7702


OtherInfo is
                                                    1234 56789ABC
        DEF0414C 49434531 3233001C 5C8CC978 63DED4FE 6A409929
        9F1F4BB2 5626548B 8E838A3E CD03A7A1 424F4242 59343536


KDFval is
                                                745FE3A7 3D4546C9
        7E424C43 ECE8B889 B2A88739 9781C6F9 2A51D8F0 3BA5644A
        B8A08747 F20C452E 91A0D5F7 0C32F56A A6A79033 FF6958E0


KeyData is
                                                745FE3A7 3D4546C9
        7E424C43 ECE8B889 B2A88739 9781C6F9 2A51D8F0 3BA5644A
        B8A08747 F20C452E 91A0D5F7 0C32F56A A6A79033 FF6958E0




-----------------------------------------------------------
Scheme Initiator, Key Confirmation Provider: U to V
NonceU is
                                                        5C8CC978
        63DED4FE 6A409929 9F1F4BB2 5626548B 8E838A3E CD03A7A1


NonceV is
                                                        03A5B235
        98A86B28 7EDB2C3D E78C71B4 447E91D4 F5C704F7 9861BBD1


Z is
                            49B20245 2DBA6F17 E9AFB666 AD152A12
        E32CFD86 D717912E B11C70B1 294B09AB 6055DC4B 99EEC4A5
        291CEE27 342B342A BFBC8639 DC10584E 0223B098 9E99646A
```

```
        D720D69E E3F32BC1 1C3D5C40 6022D82C 6300CDEE 2F476C83
        E01D0F9D 7956C2BD E18958C9 23086DF6 3D143524 F884DAA7
        3BE35F2F FC34A290 3E886E19 A4877D00 C138B58B C1B78AA0
        2826CD66 0F51B521 50BAC53C DC19E727 66996810 BAF027C0
        CEC8DF41 D480E0E2 C99C8749 D3AC3E65 4F093CFE 86FB5862
        8F0F6D18 20ACECBF A0D6DCB5 BC6D71BF 382B3DBA 289A733A
        9E64FCFF 43C0C4AC 86DD6429 896D8026 EC701D2E 800270D4
        6CF08922 47839BB7 31C58F75 A6C88D3B FB7D40CD 3A7F7702


OtherInfo is
                                                1234 56789ABC
        DEF0414C 49434531 3233001C 5C8CC978 63DED4FE 6A409929
        9F1F4BB2 5626548B 8E838A3E CD03A7A1 424F4242 59343536


KDFval is
            745F E3A73D45 46C97E42 4C43ECE8 B889B2A8 87399781
        C6F92A51 D8F03BA5 644AB8A0 8747F20C 452E91A0 D5F70C32
        F56AA6A7 9033FF69 58E00456 F26F0D80 474766CE 99FEAAAF


MacData is
        4B435F31 5F55414C 49434542 4F424259 5C8CC978 63DED4FE
        6A409929 9F1F4BB2 5626548B 8E838A3E CD03A7A1 03A5B235
        98A86B28 7EDB2C3D E78C71B4 447E91D4 F5C704F7 9861BBD1


MacKey is
                            745F E3A73D45 46C97E42 4C43ECE8


Mtag is
                            21F2 757368ED 5B0D1AA4 0C549A5F


KeyData is
                                            B889B2A8 87399781
        C6F92A51 D8F03BA5 644AB8A0 8747F20C 452E91A0 D5F70C32
        F56AA6A7 9033FF69 58E00456 F26F0D80 474766CE 99FEAAAF



-------------------------------------------------------------
Scheme Responder, Key Confirmation Provider: V to U
```

NonceV is
                                                        03A5B235
        98A86B28 7EDB2C3D E78C71B4 447E91D4 F5C704F7 9861BBD1

NonceU is
                                                        5C8CC978
        63DED4FE 6A409929 9F1F4BB2 5626548B 8E838A3E CD03A7A1

Z is
                         49B20245 2DBA6F17 E9AFB666 AD152A12
        E32CFD86 D717912E B11C70B1 294B09AB 6055DC4B 99EEC4A5
        291CEE27 342B342A BFBC8639 DC10584E 0223B098 9E99646A
        D720D69E E3F32BC1 1C3D5C40 6022D82C 6300CDEE 2F476C83
        E01D0F9D 7956C2BD E18958C9 23086DF6 3D143524 F884DAA7
        3BE35F2F FC34A290 3E886E19 A4877D00 C138B58B C1B78AA0
        2826CD66 0F51B521 50BAC53C DC19E727 66996810 BAF027C0
        CEC8DF41 D480E0E2 C99C8749 D3AC3E65 4F093CFE 86FB5862
        8F0F6D18 20ACECBF A0D6DCB5 BC6D71BF 382B3DBA 289A733A
        9E64FCFF 43C0C4AC 86DD6429 896D8026 EC701D2E 800270D4
        6CF08922 47839BB7 31C58F75 A6C88D3B FB7D40CD 3A7F7702

OtherInfo is
                                                  1234 56789ABC
        DEF0414C 49434531 3233001C 5C8CC978 63DED4FE 6A409929
        9F1F4BB2 5626548B 8E838A3E CD03A7A1 424F4242 59343536

KDFval is
            745F E3A73D45 46C97E42 4C43ECE8 B889B2A8 87399781
        C6F92A51 D8F03BA5 644AB8A0 8747F20C 452E91A0 D5F70C32
        F56AA6A7 9033FF69 58E00456 F26F0D80 474766CE 99FEAAAF

MacData is
                 4B435F31 5F56424F 42425941 4C494345 5C8CC978
        63DED4FE 6A409929 9F1F4BB2 5626548B 8E838A3E CD03A7A1

MacKey is
                              745F E3A73D45 46C97E42 4C43ECE8

Mtag is

```
                              7043 FD5B6937 528D6BF7 F90C6A15


KeyData is
                                                B889B2A8 87399781
        C6F92A51 D8F03BA5 644AB8A0 8747F20C 452E91A0 D5F70C32
        F56AA6A7 9033FF69 58E00456 F26F0D80 474766CE 99FEAAAF




------------------------------------------------------------
Scheme Initiator, Key Confirmation Bilateral
NonceU is
                                                        5C8CC978
        63DED4FE 6A409929 9F1F4BB2 5626548B 8E838A3E CD03A7A1


NonceV is
                                                        03A5B235
        98A86B28 7EDB2C3D E78C71B4 447E91D4 F5C704F7 9861BBD1


Z is
                         49B20245 2DBA6F17 E9AFB666 AD152A12
        E32CFD86 D717912E B11C70B1 294B09AB 6055DC4B 99EEC4A5
        291CEE27 342B342A BFBC8639 DC10584E 0223B098 9E99646A
        D720D69E E3F32BC1 1C3D5C40 6022D82C 6300CDEE 2F476C83
        E01D0F9D 7956C2BD E18958C9 23086DF6 3D143524 F884DAA7
        3BE35F2F FC34A290 3E886E19 A4877D00 C138B58B C1B78AA0
        2826CD66 0F51B521 50BAC53C DC19E727 66996810 BAF027C0
        CEC8DF41 D480E0E2 C99C8749 D3AC3E65 4F093CFE 86FB5862
        8F0F6D18 20ACECBF A0D6DCB5 BC6D71BF 382B3DBA 289A733A
        9E64FCFF 43C0C4AC 86DD6429 896D8026 EC701D2E 800270D4
        6CF08922 47839BB7 31C58F75 A6C88D3B FB7D40CD 3A7F7702


OtherInfo is
                                                    1234 56789ABC
        DEF0414C 49434531 3233001C 5C8CC978 63DED4FE 6A409929
        9F1F4BB2 5626548B 8E838A3E CD03A7A1 424F4242 59343536


KDFval is
            745F E3A73D45 46C97E42 4C43ECE8 B889B2A8 87399781
        C6F92A51 D8F03BA5 644AB8A0 8747F20C 452E91A0 D5F70C32
```

```
        F56AA6A7 9033FF69 58E00456 F26F0D80 474766CE 99FEAAAF


U2V
----------------
MacData is
        4B435F32 5F55414C 49434542 4F424259 5C8CC978 63DED4FE
        6A409929 9F1F4BB2 5626548B 8E838A3E CD03A7A1 03A5B235
        98A86B28 7EDB2C3D E78C71B4 447E91D4 F5C704F7 9861BBD1


MacKey is
                            745F E3A73D45 46C97E42 4C43ECE8


Mtag is
                            FAB8 363C51E3 692C1B95 F9EA9272


V2U
----------------
MacData is
        4B435F32 5F56424F 42425941 4C494345 03A5B235 98A86B28
        7EDB2C3D E78C71B4 447E91D4 F5C704F7 9861BBD1 5C8CC978
        63DED4FE 6A409929 9F1F4BB2 5626548B 8E838A3E CD03A7A1


MacKey is
                            745F E3A73D45 46C97E42 4C43ECE8


Mtag is
                            4664 AE590008 102A4ACC BE48CB6A


KeyData is
                                          B889B2A8 87399781
        C6F92A51 D8F03BA5 644AB8A0 8747F20C 452E91A0 D5F70C32
        F56AA6A7 9033FF69 58E00456 F26F0D80 474766CE 99FEAAAF
```

```
#############################################################

Key Establishment Schemes for Finite Field Cryptography
plen: 2048
qlen: 256
Hash algorithm used: SHA-256
KDF: Contatenation KDF
DKM len: 512
MacKey length: 128
MacTag len: 128
ID_U: "ALICE"
ID_V: "BOBBY"

P is
                        87A8E61D B4B6663C FFBBD19C 65195999
        8CEEF608 660DD0F2 5D2CEED4 435E3B00 E00DF8F1 D61957D4
        FAF7DF45 61B2AA30 16C3D911 34096FAA 3BF4296D 830E9A7C
        209E0C64 97517ABD 5A8A9D30 6BCF67ED 91F9E672 5B4758C0
        22E0B1EF 4275BF7B 6C5BFC11 D45F9088 B941F54E B1E59BB8
        BC39A0BF 12307F5C 4FDB70C5 81B23F76 B63ACAE1 CAA6B790
        2D525267 35488A0E F13C6D9A 51BFA4AB 3AD83477 96524D8E
        F6A167B5 A41825D9 67E144E5 14056425 1CCACB83 E6B486F6
        B3CA3F79 71506026 C0B857F6 89962856 DED4010A BD0BE621
        C3A3960A 54E710C3 75F26375 D7014103 A4B54330 C198AF12
        6116D227 6E11715F 693877FA D7EF09CA DB094AE9 1E1A1597


Q is
                                            8CF83642 A709A097
        B4479976 40129DA2 99B1A47D 1EB3750B A308B0FE 64F5FBD3


G is
                        3FB32C9B 73134D0B 2E775066 60EDBD48
        4CA7B18F 21EF2054 07F4793A 1A0BA125 10DBC150 77BE463F
        FF4FED4A AC0BB555 BE3A6C1B 0C6B47B1 BC3773BF 7E8C6F62
        901228F8 C28CBB18 A55AE313 41000A65 0196F931 C77A57F2
        DDF463E5 E9EC144B 777DE62A AAB8A862 8AC376D2 82D6ED38
        64E67982 428EBC83 1D14348F 6F2F9193 B5045AF2 767164E1
        DFC967C1 FB3F2E55 A4BD1BFF E83B9C80 D052B985 D182EA0A
        DB2A3B73 13D3FE14 C8484B1E 052588B9 B7D2BBD2 DF016199
        ECD06E15 57CD0915 B3353BBB 64E0EC37 7FD02837 0DF92B52
        C7891428 CDC67EB6 184B523D 1DB246C3 2F630784 90F00EF8
        D647D148 D4795451 5E2327CF EF98C582 664B4C0F 6CC41659
```

```
################################################################


dhHybrid1(256)
----------------------------------------------------------------
xU is
                                                  3AE68B99 B70BB90F
        B4EFC2A3 3C83AF0F 606762BF E9B34E4E EFE5C123 5F7B9FC0


yU is
                         425E4CDC BEF08130 CEEBC5E5 12EA6D40
        A9434062 CAD43B23 D5E23AA3 914F34BB 36F32F97 6E5465A2
        9747554C F016D7D5 F95ED81B 9A4983EC 4611D5B2 D9CFFDCB
        83E853E7 1F746271 05DC9E45 AA2DFC1A F2DEDF7F 6D18349A
        53241AD1 92229984 F6441FB4 DD70AD81 CBAE7447 67CF3474
        761F16DD 91CB8768 44814686 10728163 12B70D89 6990781B
        CB48CE2D E73B8099 8A136A7B 98CCF739 00E8A9C5 B333345B
        474C818C 8D1C481E BC2ADA0B 4AC5CE4D 7804096E E7DAB63B
        5A195A09 3E2EF1A1 8C2FF6B1 3B1DB21A B4A64FE7 68EC0544
        15EC86EB 32161939 B165807C 929528CC FE5E10B1 F402491B
        01F1B286 122C645F C81C0503 4B66E28F 00E53D84 3A501CE2


xV is
                                                  2CE2DCDB 3B767F9E
        BD883178 1A74DB8F 9BCD9FA2 3E589630 DDDD3F9A A7F1B027


yV is
                         73AC4BAD 1AEF0782 F019EB87 7CCEA247
        F95B158A 8177CF91 DF5469CB F013EDCE E30550A9 C668B8DE
        B44FC2D6 91934EDE 1DF8F702 C19A85E6 823EEE05 D04BF274
        EE62AEF1 68497B57 A1489B78 DC84EFB7 4411533E BEC049F1
        3DADC407 382EEF46 7C4FF8FD 71006723 0B5B54C2 DB379504
        8659907C 5859914C A743150E 09255C59 C65BFC74 EB03DF03
        27594A83 DF2BA7E5 7FDD989A 46B68990 387FC520 022625C3
        74FE7657 95569B53 F0BE89DC FBFA736D A73A97F8 471F24FC
        C2EEB4D7 6E0FE0A7 AD81F1AB ADC256F8 50FDF19A 42D4488F
        6FA7F34A 041DCDE9 ACB98F27 AE74DCA9 40D7D0FF 7AEEF1E7
        EBB0C97A 39E9CD1C F0A19929 D04582CB F8B55784 828E911A


rU is
                                                  6D12B3DB 72105EEF
```

```
        40DA18C7 66D54EFC BF49D1EC D9143B81 29FD50C3 454AC0F8


tU is
                         776204C1 DD00AE99 470F7152 5455E518
        ABE02404 29D3D679 96E522DC A1030D20 F824CFB2 3FC5AA31
        47D9B353 05EB2303 791965DD BC84F1A0 1182AED4 3D56BA0E
        00405304 032DB61E 5DCA9E6C 8921BAF3 B010DA93 BFB36747
        96F44D29 CCA6AE4E F11FA51C 11F34406 60E7639B 9F9819CA
        D2746734 79A5CF97 8E03F8C1 C7D6EC48 39B3D0C3 6EA5C34A
        46D3C921 DB7EDCD0 B39185D2 E89143EB 0B5A03EB AF12A8EE
        0D6333C4 9259CAA2 5FCA903C 39388750 2561A135 28503FDD
        77B658ED F4278F34 8A8B548E 489EF357 71A25DE9 B0647F4F
        CDC5F5E4 D73DACD6 44C00D2F 15206A17 D10D34FC B48C0292
        2180D348 9686CCAF 9DC63837 46DFDA1C 124E433C E5B5158A


rV is
                                           284F486A A9679306
        70565602 B10A1CD9 AF2A27C4 96730BA1 32044D00 2F6A0417


tV is
                         7D04B9E5 3FEF9586 CE9507B2 3B0AE337
        5B09663D D3A1D03B 230826E9 D57828E7 5B438123 09CBD78A
        8DC8926C 7E66B2F1 05DEDAF3 27936800 E54E8DEC 52F3829B
        6005CED6 5BB8BEFB 65704C21 73D14759 B35AD5B0 64B86C4B
        D3915A0A 956160C0 91AA14AC D96D1DD8 66C9C015 31054F9A
        EA307E3F 71E109FD A0BD9692 B7F79D30 C8763242 490F444E
        84C71956 4A8A52E3 6650FC33 FAB25E2D A54E0A4D 6EA23179
        18A5A5DF 2298BA39 8EA2DCFC D51C5C3B E2F969F8 82A2EDA3
        B4BF129A 52088943 97537C84 A3BE67E9 8948B333 A388E3E9
        14223F03 6EE75218 0CB13DCD 57191D83 4FAE396D 6F6242A3
        D292BA77 D3EE9DEE 140FFD68 548AB5F9 F2D9D1A7 B896008E




------------------------------------------------------------
no Key Confirmation
Zs is
                         0D82485C F7D62FFC EA343388 CFEC1527
        3A394B84 32EEB632 1BE31D4F CD1615C8 1C6937C0 8D92416E
        DBDD2010 FA8B6E0A 8A603DAD E010BC9C D76B14E3 E2190E3B
        A300E71A DDBF244C F8062949 76EAF07D 023BDB57 FC5D1964
        C7D4206E 72061BFE 1EE4EEBC 9200E13A 6CBA3286 9DBE8082
```

CDF3645B 5A727DD2 7CA503F4 EDEB73E8 8A3A552C 7E00D4EE
72421372 36A0965C 1EC3EBC0 B48C2B46 7EB84241 5A283F55
E220FFD1 8819256D A2474D28 FC3B04E0 C07E4D25 C1749341
D2229701 5CD8178C 3918BE8C 5CDF0FBF BB9A5ACC DD82AF07
83EFE4DF 64A8D892 828F8DE5 8C5D569B 5B084558 96C4D3C3
4FD3CE93 C434C38E F56CED30 561C371A F9F2D864 FDC5B62F

Ze is

44F48409 F31BF350 9451DB4D 304BEBD8
3C2AD650 1C1B85E6 32BC9258 8E2D48B5 D2B84444 62AD94E8
A444941E D4975C97 9117D75A 0A2BA810 DFA8804A 0FE9426D
D7EB95F2 9CA430DA 37EFA52C 42DA1DE2 23763BDD C95E466A
A3B8D206 B8218EDF 23973D05 F3C7C22B 224653D4 F9218545
7983262F 27BC55A0 A7AEE543 5455D43C 0E0C6D80 67ADAF90
42B6B777 7E198D67 60830D96 B29A6AAE F574D75E 2D654355
0F7555CF 8982C821 C4EC9B82 662B0936 69FD246D 4DCCBFF3
1D984EF6 3C4F95D7 39C77E66 F69B6DB0 D9FC1A97 3F5233D1
1FE7154B 8A6BE150 467D92DA F0914434 F0CF176E 961B313F
E3E23BFE 378B87BA F273937F FAA68565 8B09781D 2697864B

Z is

44F48409 F31BF350
9451DB4D 304BEBD8 3C2AD650 1C1B85E6 32BC9258 8E2D48B5
D2B84444 62AD94E8 A444941E D4975C97 9117D75A 0A2BA810
DFA8804A 0FE9426D D7EB95F2 9CA430DA 37EFA52C 42DA1DE2
23763BDD C95E466A A3B8D206 B8218EDF 23973D05 F3C7C22B
224653D4 F9218545 7983262F 27BC55A0 A7AEE543 5455D43C
0E0C6D80 67ADAF90 42B6B777 7E198D67 60830D96 B29A6AAE
F574D75E 2D654355 0F7555CF 8982C821 C4EC9B82 662B0936
69FD246D 4DCCBFF3 1D984EF6 3C4F95D7 39C77E66 F69B6DB0
D9FC1A97 3F5233D1 1FE7154B 8A6BE150 467D92DA F0914434
F0CF176E 961B313F E3E23BFE 378B87BA F273937F FAA68565
8B09781D 2697864B 0D82485C F7D62FFC EA343388 CFEC1527
3A394B84 32EEB632 1BE31D4F CD1615C8 1C6937C0 8D92416E
DBDD2010 FA8B6E0A 8A603DAD E010BC9C D76B14E3 E2190E3B
A300E71A DDBF244C F8062949 76EAF07D 023BDB57 FC5D1964
C7D4206E 72061BFE 1EE4EEBC 9200E13A 6CBA3286 9DBE8082
CDF3645B 5A727DD2 7CA503F4 EDEB73E8 8A3A552C 7E00D4EE
72421372 36A0965C 1EC3EBC0 B48C2B46 7EB84241 5A283F55
E220FFD1 8819256D A2474D28 FC3B04E0 C07E4D25 C1749341
D2229701 5CD8178C 3918BE8C 5CDF0FBF BB9A5ACC DD82AF07
83EFE4DF 64A8D892 828F8DE5 8C5D569B 5B084558 96C4D3C3
4FD3CE93 C434C38E F56CED30 561C371A F9F2D864 FDC5B62F

```
OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


KeyData is
                         4235AC89 C9F33E5D BB11601A 2983E376
        E2153997 87D839A0 3855FE04 533E1A67 66915E67 C25EEB04
        0828E96C D3D6EF0A B7D17B43 1343A7F3 AAC68F0C 4A7E779B




------------------------------------------------------------
Scheme Initiator, Key Confirmation Provider: U to V
Zs is
                         0D82485C F7D62FFC EA343388 CFEC1527
        3A394B84 32EEB632 1BE31D4F CD1615C8 1C6937C0 8D92416E
        DBDD2010 FA8B6E0A 8A603DAD E010BC9C D76B14E3 E2190E3B
        A300E71A DDBF244C F8062949 76EAF07D 023BDB57 FC5D1964
        C7D4206E 72061BFE 1EE4EEBC 9200E13A 6CBA3286 9DBE8082
        CDF3645B 5A727DD2 7CA503F4 EDEB73E8 8A3A552C 7E00D4EE
        72421372 36A0965C 1EC3EBC0 B48C2B46 7EB84241 5A283F55
        E220FFD1 8819256D A2474D28 FC3B04E0 C07E4D25 C1749341
        D2229701 5CD8178C 3918BE8C 5CDF0FBF BB9A5ACC DD82AF07
        83EFE4DF 64A8D892 828F8DE5 8C5D569B 5B084558 96C4D3C3
        4FD3CE93 C434C38E F56CED30 561C371A F9F2D864 FDC5B62F


Ze is
                         44F48409 F31BF350 9451DB4D 304BEBD8
        3C2AD650 1C1B85E6 32BC9258 8E2D48B5 D2B84444 62AD94E8
        A444941E D4975C97 9117D75A 0A2BA810 DFA8804A 0FE9426D
        D7EB95F2 9CA430DA 37EFA52C 42DA1DE2 23763BDD C95E466A
        A3B8D206 B8218EDF 23973D05 F3C7C22B 224653D4 F9218545
        7983262F 27BC55A0 A7AEE543 5455D43C 0E0C6D80 67ADAF90
        42B6B777 7E198D67 60830D96 B29A6AAE F574D75E 2D654355
        0F7555CF 8982C821 C4EC9B82 662B0936 69FD246D 4DCCBFF3
        1D984EF6 3C4F95D7 39C77E66 F69B6DB0 D9FC1A97 3F5233D1
        1FE7154B 8A6BE150 467D92DA F0914434 F0CF176E 961B313F
        E3E23BFE 378B87BA F273937F FAA68565 8B09781D 2697864B


Z is
                                                 44F48409 F31BF350
        9451DB4D 304BEBD8 3C2AD650 1C1B85E6 32BC9258 8E2D48B5
```

D2B84444 62AD94E8 A444941E D4975C97 9117D75A 0A2BA810
DFA8804A 0FE9426D D7EB95F2 9CA430DA 37EFA52C 42DA1DE2
23763BDD C95E466A A3B8D206 B8218EDF 23973D05 F3C7C22B
224653D4 F9218545 7983262F 27BC55A0 A7AEE543 5455D43C
0E0C6D80 67ADAF90 42B6B777 7E198D67 60830D96 B29A6AAE
F574D75E 2D654355 0F7555CF 8982C821 C4EC9B82 662B0936
69FD246D 4DCCBFF3 1D984EF6 3C4F95D7 39C77E66 F69B6DB0
D9FC1A97 3F5233D1 1FE7154B 8A6BE150 467D92DA F0914434
F0CF176E 961B313F E3E23BFE 378B87BA F273937F FAA68565
8B09781D 2697864B 0D82485C F7D62FFC EA343388 CFEC1527
3A394B84 32EEB632 1BE31D4F CD1615C8 1C6937C0 8D92416E
DBDD2010 FA8B6E0A 8A603DAD E010BC9C D76B14E3 E2190E3B
A300E71A DDBF244C F8062949 76EAF07D 023BDB57 FC5D1964
C7D4206E 72061BFE 1EE4EEBC 9200E13A 6CBA3286 9DBE8082
CDF3645B 5A727DD2 7CA503F4 EDEB73E8 8A3A552C 7E00D4EE
72421372 36A0965C 1EC3EBC0 B48C2B46 7EB84241 5A283F55
E220FFD1 8819256D A2474D28 FC3B04E0 C07E4D25 C1749341
D2229701 5CD8178C 3918BE8C 5CDF0FBF BB9A5ACC DD82AF07
83EFE4DF 64A8D892 828F8DE5 8C5D569B 5B084558 96C4D3C3
4FD3CE93 C434C38E F56CED30 561C371A F9F2D864 FDC5B62F

OtherInfo is
12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536

MacData is
4B435F31 5F55414C 49434542 4F424259 776204C1 DD00AE99
470F7152 5455E518 ABE02404 29D3D679 96E522DC A1030D20
F824CFB2 3FC5AA31 47D9B353 05EB2303 791965DD BC84F1A0
1182AED4 3D56BA0E 00405304 032DB61E 5DCA9E6C 8921BAF3
B010DA93 BFB36747 96F44D29 CCA6AE4E F11FA51C 11F34406
60E7639B 9F9819CA D2746734 79A5CF97 8E03F8C1 C7D6EC48
39B3D0C3 6EA5C34A 46D3C921 DB7EDCD0 B39185D2 E89143EB
0B5A03EB AF12A8EE 0D6333C4 9259CAA2 5FCA903C 39388750
2561A135 28503FDD 77B658ED F4278F34 8A8B548E 489EF357
71A25DE9 B0647F4F CDC5F5E4 D73DACD6 44C00D2F 15206A17
D10D34FC B48C0292 2180D348 9686CCAF 9DC63837 46DFDA1C
124E433C E5B5158A 7D04B9E5 3FEF9586 CE9507B2 3B0AE337
5B09663D D3A1D03B 230826E9 D57828E7 5B438123 09CBD78A
8DC8926C 7E66B2F1 05DEDAF3 27936800 E54E8DEC 52F3829B
6005CED6 5BB8BEFB 65704C21 73D14759 B35AD5B0 64B86C4B
D3915A0A 956160C0 91AA14AC D96D1DD8 66C9C015 31054F9A
EA307E3F 71E109FD A0BD9692 B7F79D30 C8763242 490F444E
84C71956 4A8A52E3 6650FC33 FAB25E2D A54E0A4D 6EA23179
18A5A5DF 2298BA39 8EA2DCFC D51C5C3B E2F969F8 82A2EDA3

B4BF129A 52088943 97537C84 A3BE67E9 8948B333 A388E3E9
14223F03 6EE75218 0CB13DCD 57191D83 4FAE396D 6F6242A3
D292BA77 D3EE9DEE 140FFD68 548AB5F9 F2D9D1A7 B896008E

MacKey is
4235AC89 C9F33E5D BB11601A 2983E376

Mtag is
A9D7D7F9 439C737C 97D65250 7F4CDEFE

KeyData is
E2153997 87D839A0 3855FE04 533E1A67
66915E67 C25EEB04 0828E96C D3D6EF0A B7D17B43 1343A7F3
AAC68F0C 4A7E779B 97D127D7 5ACF286F 72E62DDB 881F4634

Scheme Responder, Key Confirmation Provider: V to U
Zs is
0D82485C F7D62FFC EA343388 CFEC1527
3A394B84 32EEB632 1BE31D4F CD1615C8 1C6937C0 8D92416E
DBDD2010 FA8B6E0A 8A603DAD E010BC9C D76B14E3 E2190E3B
A300E71A DDBF244C F8062949 76EAF07D 023BDB57 FC5D1964
C7D4206E 72061BFE 1EE4EEBC 9200E13A 6CBA3286 9DBE8082
CDF3645B 5A727DD2 7CA503F4 EDEB73E8 8A3A552C 7E00D4EE
72421372 36A0965C 1EC3EBC0 B48C2B46 7EB84241 5A283F55
E220FFD1 8819256D A2474D28 FC3B04E0 C07E4D25 C1749341
D2229701 5CD8178C 3918BE8C 5CDF0FBF BB9A5ACC DD82AF07
83EFE4DF 64A8D892 828F8DE5 8C5D569B 5B084558 96C4D3C3
4FD3CE93 C434C38E F56CED30 561C371A F9F2D864 FDC5B62F

Ze is
44F48409 F31BF350 9451DB4D 304BEBD8
3C2AD650 1C1B85E6 32BC9258 8E2D48B5 D2B84444 62AD94E8
A444941E D4975C97 9117D75A 0A2BA810 DFA8804A 0FE9426D
D7EB95F2 9CA430DA 37EFA52C 42DA1DE2 23763BDD C95E466A
A3B8D206 B8218EDF 23973D05 F3C7C22B 224653D4 F9218545
7983262F 27BC55A0 A7AEE543 5455D43C 0E0C6D80 67ADAF90
42B6B777 7E198D67 60830D96 B29A6AAE F574D75E 2D654355
0F7555CF 8982C821 C4EC9B82 662B0936 69FD246D 4DCCBFF3

```
        1D984EF6 3C4F95D7 39C77E66 F69B6DB0 D9FC1A97 3F5233D1
        1FE7154B 8A6BE150 467D92DA F0914434 F0CF176E 961B313F
        E3E23BFE 378B87BA F273937F FAA68565 8B09781D 2697864B


Z is
                                            44F48409 F31BF350
        9451DB4D 304BEBD8 3C2AD650 1C1B85E6 32BC9258 8E2D48B5
        D2B84444 62AD94E8 A444941E D4975C97 9117D75A 0A2BA810
        DFA8804A 0FE9426D D7EB95F2 9CA430DA 37EFA52C 42DA1DE2
        23763BDD C95E466A A3B8D206 B8218EDF 23973D05 F3C7C22B
        224653D4 F9218545 7983262F 27BC55A0 A7AEE543 5455D43C
        0E0C6D80 67ADAF90 42B6B777 7E198D67 60830D96 B29A6AAE
        F574D75E 2D654355 0F7555CF 8982C821 C4EC9B82 662B0936
        69FD246D 4DCCBFF3 1D984EF6 3C4F95D7 39C77E66 F69B6DB0
        D9FC1A97 3F5233D1 1FE7154B 8A6BE150 467D92DA F0914434
        F0CF176E 961B313F E3E23BFE 378B87BA F273937F FAA68565
        8B09781D 2697864B 0D82485C F7D62FFC EA343388 CFEC1527
        3A394B84 32EEB632 1BE31D4F CD1615C8 1C6937C0 8D92416E
        DBDD2010 FA8B6E0A 8A603DAD E010BC9C D76B14E3 E2190E3B
        A300E71A DDBF244C F8062949 76EAF07D 023BDB57 FC5D1964
        C7D4206E 72061BFE 1EE4EEBC 9200E13A 6CBA3286 9DBE8082
        CDF3645B 5A727DD2 7CA503F4 EDEB73E8 8A3A552C 7E00D4EE
        72421372 36A0965C 1EC3EBC0 B48C2B46 7EB84241 5A283F55
        E220FFD1 8819256D A2474D28 FC3B04E0 C07E4D25 C1749341
        D2229701 5CD8178C 3918BE8C 5CDF0FBF BB9A5ACC DD82AF07
        83EFE4DF 64A8D892 828F8DE5 8C5D569B 5B084558 96C4D3C3
        4FD3CE93 C434C38E F56CED30 561C371A F9F2D864 FDC5B62F


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


MacData is
        4B435F31 5F56424F 42425941 4C494345 7D04B9E5 3FEF9586
        CE9507B2 3B0AE337 5B09663D D3A1D03B 230826E9 D57828E7
        5B438123 09CBD78A 8DC8926C 7E66B2F1 05DEDAF3 27936800
        E54E8DEC 52F3829B 6005CED6 5BB8BEFB 65704C21 73D14759
        B35AD5B0 64B86C4B D3915A0A 956160C0 91AA14AC D96D1DD8
        66C9C015 31054F9A EA307E3F 71E109FD A0BD9692 B7F79D30
        C8763242 490F444E 84C71956 4A8A52E3 6650FC33 FAB25E2D
        A54E0A4D 6EA23179 18A5A5DF 2298BA39 8EA2DCFC D51C5C3B
        E2F969F8 82A2EDA3 B4BF129A 52088943 97537C84 A3BE67E9
        8948B333 A388E3E9 14223F03 6EE75218 0CB13DCD 57191D83
        4FAE396D 6F6242A3 D292BA77 D3EE9DEE 140FFD68 548AB5F9
```

F2D9D1A7 B896008E 776204C1 DD00AE99 470F7152 5455E518
ABE02404 29D3D679 96E522DC A1030D20 F824CFB2 3FC5AA31
47D9B353 05EB2303 791965DD BC84F1A0 1182AED4 3D56BA0E
00405304 032DB61E 5DCA9E6C 8921BAF3 B010DA93 BFB36747
96F44D29 CCA6AE4E F11FA51C 11F34406 60E7639B 9F9819CA
D2746734 79A5CF97 8E03F8C1 C7D6EC48 39B3D0C3 6EA5C34A
46D3C921 DB7EDCD0 B39185D2 E89143EB 0B5A03EB AF12A8EE
0D6333C4 9259CAA2 5FCA903C 39388750 2561A135 28503FDD
77B658ED F4278F34 8A8B548E 489EF357 71A25DE9 B0647F4F
CDC5F5E4 D73DACD6 44C00D2F 15206A17 D10D34FC B48C0292
2180D348 9686CCAF 9DC63837 46DFDA1C 124E433C E5B5158A

MacKey is
4235AC89 C9F33E5D BB11601A 2983E376

Mtag is
1A102044 DB2D371A 6B0F4A8F 65AC2068

KeyData is
E2153997 87D839A0 3855FE04 533E1A67
66915E67 C25EEB04 0828E96C D3D6EF0A B7D17B43 1343A7F3
AAC68F0C 4A7E779B 97D127D7 5ACF286F 72E62DDB 881F4634

Scheme Initiator, Key Confirmation Bilateral
Zs is
0D82485C F7D62FFC EA343388 CFEC1527
3A394B84 32EEB632 1BE31D4F CD1615C8 1C6937C0 8D92416E
DBDD2010 FA8B6E0A 8A603DAD E010BC9C D76B14E3 E2190E3B
A300E71A DDBF244C F8062949 76EAF07D 023BDB57 FC5D1964
C7D4206E 72061BFE 1EE4EEBC 9200E13A 6CBA3286 9DBE8082
CDF3645B 5A727DD2 7CA503F4 EDEB73E8 8A3A552C 7E00D4EE
72421372 36A0965C 1EC3EBC0 B48C2B46 7EB84241 5A283F55
E220FFD1 8819256D A2474D28 FC3B04E0 C07E4D25 C1749341
D2229701 5CD8178C 3918BE8C 5CDF0FBF BB9A5ACC DD82AF07
83EFE4DF 64A8D892 828F8DE5 8C5D569B 5B084558 96C4D3C3
4FD3CE93 C434C38E F56CED30 561C371A F9F2D864 FDC5B62F

Ze is

```
                    44F48409 F31BF350 9451DB4D 304BEBD8
        3C2AD650 1C1B85E6 32BC9258 8E2D48B5 D2B84444 62AD94E8
        A444941E D4975C97 9117D75A 0A2BA810 DFA8804A 0FE9426D
        D7EB95F2 9CA430DA 37EFA52C 42DA1DE2 23763BDD C95E466A
        A3B8D206 B8218EDF 23973D05 F3C7C22B 224653D4 F9218545
        7983262F 27BC55A0 A7AEE543 5455D43C 0E0C6D80 67ADAF90
        42B6B777 7E198D67 60830D96 B29A6AAE F574D75E 2D654355
        0F7555CF 8982C821 C4EC9B82 662B0936 69FD246D 4DCCBFF3
        1D984EF6 3C4F95D7 39C77E66 F69B6DB0 D9FC1A97 3F5233D1
        1FE7154B 8A6BE150 467D92DA F0914434 F0CF176E 961B313F
        E3E23BFE 378B87BA F273937F FAA68565 8B09781D 2697864B


Z is
                                            44F48409 F31BF350
        9451DB4D 304BEBD8 3C2AD650 1C1B85E6 32BC9258 8E2D48B5
        D2B84444 62AD94E8 A444941E D4975C97 9117D75A 0A2BA810
        DFA8804A 0FE9426D D7EB95F2 9CA430DA 37EFA52C 42DA1DE2
        23763BDD C95E466A A3B8D206 B8218EDF 23973D05 F3C7C22B
        224653D4 F9218545 7983262F 27BC55A0 A7AEE543 5455D43C
        0E0C6D80 67ADAF90 42B6B777 7E198D67 60830D96 B29A6AAE
        F574D75E 2D654355 0F7555CF 8982C821 C4EC9B82 662B0936
        69FD246D 4DCCBFF3 1D984EF6 3C4F95D7 39C77E66 F69B6DB0
        D9FC1A97 3F5233D1 1FE7154B 8A6BE150 467D92DA F0914434
        F0CF176E 961B313F E3E23BFE 378B87BA F273937F FAA68565
        8B09781D 2697864B 0D82485C F7D62FFC EA343388 CFEC1527
        3A394B84 32EEB632 1BE31D4F CD1615C8 1C6937C0 8D92416E
        DBDD2010 FA8B6E0A 8A603DAD E010BC9C D76B14E3 E2190E3B
        A300E71A DDBF244C F8062949 76EAF07D 023BDB57 FC5D1964
        C7D4206E 72061BFE 1EE4EEBC 9200E13A 6CBA3286 9DBE8082
        CDF3645B 5A727DD2 7CA503F4 EDEB73E8 8A3A552C 7E00D4EE
        72421372 36A0965C 1EC3EBC0 B48C2B46 7EB84241 5A283F55
        E220FFD1 8819256D A2474D28 FC3B04E0 C07E4D25 C1749341
        D2229701 5CD8178C 3918BE8C 5CDF0FBF BB9A5ACC DD82AF07
        83EFE4DF 64A8D892 828F8DE5 8C5D569B 5B084558 96C4D3C3
        4FD3CE93 C434C38E F56CED30 561C371A F9F2D864 FDC5B62F


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


U2V
----------------
MacData is
        4B435F32 5F55414C 49434542 4F424259 776204C1 DD00AE99
```

```
        470F7152 5455E518 ABE02404 29D3D679 96E522DC A1030D20
        F824CFB2 3FC5AA31 47D9B353 05EB2303 791965DD BC84F1A0
        1182AED4 3D56BA0E 00405304 032DB61E 5DCA9E6C 8921BAF3
        B010DA93 BFB36747 96F44D29 CCA6AE4E F11FA51C 11F34406
        60E7639B 9F9819CA D2746734 79A5CF97 8E03F8C1 C7D6EC48
        39B3D0C3 6EA5C34A 46D3C921 DB7EDCD0 B39185D2 E89143EB
        0B5A03EB AF12A8EE 0D6333C4 9259CAA2 5FCA903C 39388750
        2561A135 28503FDD 77B658ED F4278F34 8A8B548E 489EF357
        71A25DE9 B0647F4F CDC5F5E4 D73DACD6 44C00D2F 15206A17
        D10D34FC B48C0292 2180D348 9686CCAF 9DC63837 46DFDA1C
        124E433C E5B5158A 7D04B9E5 3FEF9586 CE9507B2 3B0AE337
        5B09663D D3A1D03B 230826E9 D57828E7 5B438123 09CBD78A
        8DC8926C 7E66B2F1 05DEDAF3 27936800 E54E8DEC 52F3829B
        6005CED6 5BB8BEFB 65704C21 73D14759 B35AD5B0 64B86C4B
        D3915A0A 956160C0 91AA14AC D96D1DD8 66C9C015 31054F9A
        EA307E3F 71E109FD A0BD9692 B7F79D30 C8763242 490F444E
        84C71956 4A8A52E3 6650FC33 FAB25E2D A54E0A4D 6EA23179
        18A5A5DF 2298BA39 8EA2DCFC D51C5C3B E2F969F8 82A2EDA3
        B4BF129A 52088943 97537C84 A3BE67E9 8948B333 A388E3E9
        14223F03 6EE75218 0CB13DCD 57191D83 4FAE396D 6F6242A3
        D292BA77 D3EE9DEE 140FFD68 548AB5F9 F2D9D1A7 B896008E


MacKey is
                        4235AC89 C9F33E5D BB11601A 2983E376


Mtag is
                        CDE1E574 073FE04C E099E059 94E4F5D9


V2U
----------------
MacData is
        4B435F32 5F56424F 42425941 4C494345 7D04B9E5 3FEF9586
        CE9507B2 3B0AE337 5B09663D D3A1D03B 230826E9 D57828E7
        5B438123 09CBD78A 8DC8926C 7E66B2F1 05DEDAF3 27936800
        E54E8DEC 52F3829B 6005CED6 5BB8BEFB 65704C21 73D14759
        B35AD5B0 64B86C4B D3915A0A 956160C0 91AA14AC D96D1DD8
        66C9C015 31054F9A EA307E3F 71E109FD A0BD9692 B7F79D30
        C8763242 490F444E 84C71956 4A8A52E3 6650FC33 FAB25E2D
        A54E0A4D 6EA23179 18A5A5DF 2298BA39 8EA2DCFC D51C5C3B
        E2F969F8 82A2EDA3 B4BF129A 52088943 97537C84 A3BE67E9
        8948B333 A388E3E9 14223F03 6EE75218 0CB13DCD 57191D83
        4FAE396D 6F6242A3 D292BA77 D3EE9DEE 140FFD68 548AB5F9
        F2D9D1A7 B896008E 776204C1 DD00AE99 470F7152 5455E518
```

```
        ABE02404 29D3D679 96E522DC A1030D20 F824CFB2 3FC5AA31
        47D9B353 05EB2303 791965DD BC84F1A0 1182AED4 3D56BA0E
        00405304 032DB61E 5DCA9E6C 8921BAF3 B010DA93 BFB36747
        96F44D29 CCA6AE4E F11FA51C 11F34406 60E7639B 9F9819CA
        D2746734 79A5CF97 8E03F8C1 C7D6EC48 39B3D0C3 6EA5C34A
        46D3C921 DB7EDCD0 B39185D2 E89143EB 0B5A03EB AF12A8EE
        0D6333C4 9259CAA2 5FCA903C 39388750 2561A135 28503FDD
        77B658ED F4278F34 8A8B548E 489EF357 71A25DE9 B0647F4F
        CDC5F5E4 D73DACD6 44C00D2F 15206A17 D10D34FC B48C0292
        2180D348 9686CCAF 9DC63837 46DFDA1C 124E433C E5B5158A


MacKey is
                        4235AC89 C9F33E5D BB11601A 2983E376


Mtag is
                        2A5994C4 439987DA F3D0F0E2 E37B9A9E


KeyData is
                        E2153997 87D839A0 3855FE04 533E1A67
        66915E67 C25EEB04 0828E96C D3D6EF0A B7D17B43 1343A7F3
        AAC68F0C 4A7E779B 97D127D7 5ACF286F 72E62DDB 881F4634


============================================================


MQV2(256)
------------------------------------------------------------
xU is
                                                80B650EB 3F3A0756
        61E749BE 7C014D00 682414BE B5C22B02 CD5F415C 31DD714D


yU is
                        3BC0117F DBBC6876 A001AAA2 809ABAC6
        1388AD25 DE6DFC5D 51E973B7 8E5B0C83 BAA6E255 40945C98
        9A58C94E F774D371 8BF0757C B83BADD8 FF045394 09A21B4D
        E908A4D2 8BAF3D92 49C69F3A 49BE59AC FA629CE3 E956FBC0
        5E8C6E49 30094B16 AA7436B0 DDC35023 CD261566 ABCBC3DE
        BD8D11AC 92EF2358 9596216D 994C8EC4 024DC38A 4362BC3C
        8B8C0A75 C8A8D322 594D4768 B838E850 846CE1EB E338B493
        72D5C7EB B011C943 03E97FCE A6F749C9 300D6B16 225CF372
        208BC014 67D73DE3 1F0563DB F98C0C26 ACB16CA5 A2D7B394
```

C6BA26B9 7F56E49F B825F867 9B87F8BC 02AA2BC1 B30A8119
AB432088 C10D0810 628052A2 8B76F0A0 69447941 EEA0F42C

xV is
7E24A4CA 22EB375F
819A112B 3D10CA88 BEDAF368 07B7BD5C CC64D2C3 804BE42B

yV is
2D2D675D F3A5766D 56560AB7 9D082B57
48C001D8 B7470227 4539A4C0 81E0B18E 2ADEAC1D 43345847
D0DDA886 E4EA402B 44022E79 3B8552F3 92B2436D 59FAEE6B
CAB4037F 01B3DB04 F0B2FCEA 83432F8D 744F05C1 BBC9D104
73D57BEC F62EA494 1F3832BB 7BAB88FE FCB3B2F1 E3E36C1A
F2FD58E6 C0311924 80FFD804 3A3A4583 17C54636 FF94E0CE
1F0E85F6 57E36212 24401EA2 96CAEDFC AD615B93 AC135DA9
AC019790 6F12C4C0 E9080AF2 C4B562AF 8F174B7A 72287451
15AAB55D C0623506 102675DE 2667F8C0 86023726 C5D6C395
044D0ADA D5EC6AFD 4B61D1C3 0D07CCA0 F4A125AB 49A827BA
FC51C5CC 88E8B3C6 F465607D 59D54238 B7A770B6 2D3F6035

rU is
6A549A85 356D09C3
D845D365 49167D36 6D669B18 198B52A5 0E2F3A5C 0B9AE350

tU is
31BACD07 71AE01D1 58C4C5A5 EAB21226
A2AAB682 8589CD21 977C7131 D3D8CAC7 8CB1F20A C4D51391
AA42EB53 B7F6C832 D921988F 7696700D 91EF3319 4FCDC9C3
EE2B531B F9CE7329 996769F1 0636FA99 4D975709 EAF7E30F
FD7983E9 26D75E30 44559023 6FE9CB41 2CA553F8 AD3E6FD5
B52FCD92 D65AE374 0665A719 6EB9F6F9 2AFF8798 B0206839
ED1D0481 A52E5623 EB6D5C6E DCC23711 C7F66C86 EDE8E41F
A97765A5 491BF90B 6CB923C7 49173B2F E4A8C6E7 932D9B77
A15F4D2D 3DF3F181 D8A8A56B 8B7020F3 BBD1C722 826C04B8
8AEC8523 531A6FD6 D7D6EA3C 254C75E3 67723773 75598CA7
83408A65 6ECB957A F28334B9 692B7807 8725CDC7 6C524E50

rV is
89AADFB3 8E4F91AD
5D7575F6 8F41785F E17A23B5 7BA779A8 90CCDC15 D5BFD888

```
tV is
                        1F7702BA 6C10A98C 5A70D3C0 EABCFE04
        081FAE95 48FB2EFE 699999A5 9EBBEF78 044E5700 26FE5B9B
        CB33871D 0C2F494C 05AA3AE9 BB148DF4 12BC608A F22A8143
        221513ED 9326499F 2154819E ED5B113F 9BBBABF2 C9251FF1
        AC5ED293 CA17BC7B F275CF4F 57036C78 F0A410B9 E37C24CD
        ADBEBDA2 6F7B8E20 521FD698 D4D1D209 67B7669D 044C2CF3
        BB235BAF 5BC7E520 2A3EA8FC E06D355F 733B59B6 45BF9F8D
        C5EE28A4 AACCA937 C1EA47E1 6F52234C A09CCEAF 9D056954
        E0023C73 7432230A 4BDBC3CB BA99B1A0 F20CC7FE AC6A41BA
        B8C2C639 F93C7BEC F416E757 558D124D 899E20BA 2144348B
        1B7E0769 770DFFDA 9B5A8FF4 D0519705 50EBE74B 32A92119



------------------------------------------------------------
no Key Confirmation
Z is
                        5713B6EE F9D248C6 E87885EA FD7CB70A
        111AB995 9C5BDAB1 2FF68951 3DBB0154 0222DA46 ACE4FBC8
        8689BD44 844AA092 2AF444CF 9C88E35C 8BA23131 4617A5A7
        C33B4385 63A38258 C31900C1 55D4D523 F7879A67 09D84E9E
        2765DC74 459ECB26 C3646124 477D68DE 0599E25E FC26C40B
        5929D37B 8D273DE1 4D345C8A 0DC61A28 ACA556BE 431D1B54
        AAD2C2F0 81B19693 0EDFE4D0 75746094 C90A780A 66F2AEFC
        08C3E1F6 143981E4 CDDFCE1E C104A89C C770A9C8 D26B6270
        4C7C148B 481D02C1 DCC81428 7AF7F99C 9139DAA5 13B8F043
        6F656B14 65E69213 73B08EAA 553CE81D 087EA4E7 E4421A1A
        1423C47D 9818E975 8ED18470 208ACC35 E346A143 227C16BB


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


KDFval is
                        70C0460A 7E4434DD DB81874C 9F2A5A37
        B104D11B F56C2933 4F07743D C437BA2F C6DF5D93 635357DD
        1A6E780C 15A3A2CD 5E91FE49 6D8247AB 6AE7DFC9 6923261E


KeyData is
                        70C0460A 7E4434DD DB81874C 9F2A5A37
        B104D11B F56C2933 4F07743D C437BA2F C6DF5D93 635357DD
```

1A6E780C 15A3A2CD 5E91FE49 6D8247AB 6AE7DFC9 6923261E

Scheme Initiator, Key Confirmation Provider: U to V
Z is

5713B6EE F9D248C6 E87885EA FD7CB70A
111AB995 9C5BDAB1 2FF68951 3DBB0154 0222DA46 ACE4FBC8
8689BD44 844AA092 2AF444CF 9C88E35C 8BA23131 4617A5A7
C33B4385 63A38258 C31900C1 55D4D523 F7879A67 09D84E9E
2765DC74 459ECB26 C3646124 477D68DE 0599E25E FC26C40B
5929D37B 8D273DE1 4D345C8A 0DC61A28 ACA556BE 431D1B54
AAD2C2F0 81B19693 0EDFE4D0 75746094 C90A780A 66F2AEFC
08C3E1F6 143981E4 CDDFCE1E C104A89C C770A9C8 D26B6270
4C7C148B 481D02C1 DCC81428 7AF7F99C 9139DAA5 13B8F043
6F656B14 65E69213 73B08EAA 553CE81D 087EA4E7 E4421A1A
1423C47D 9818E975 8ED18470 208ACC35 E346A143 227C16BB

OtherInfo is
12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536

KDFval is

70C0460A 7E4434DD
DB81874C 9F2A5A37 B104D11B F56C2933 4F07743D C437BA2F
C6DF5D93 635357DD 1A6E780C 15A3A2CD 5E91FE49 6D8247AB
6AE7DFC9 6923261E 43EE77F1 280AE2F9 C80D75EE CBFF455A

MacData is
4B435F31 5F55414C 49434542 4F424259 31BACD07 71AE01D1
58C4C5A5 EAB21226 A2AAB682 8589CD21 977C7131 D3D8CAC7
8CB1F20A C4D51391 AA42EB53 B7F6C832 D921988F 7696700D
91EF3319 4FCDC9C3 EE2B531B F9CE7329 996769F1 0636FA99
4D975709 EAF7E30F FD7983E9 26D75E30 44559023 6FE9CB41
2CA553F8 AD3E6FD5 B52FCD92 D65AE374 0665A719 6EB9F6F9
2AFF8798 B0206839 ED1D0481 A52E5623 EB6D5C6E DCC23711
C7F66C86 EDE8E41F A97765A5 491BF90B 6CB923C7 49173B2F
E4A8C6E7 932D9B77 A15F4D2D 3DF3F181 D8A8A56B 8B7020F3
BBD1C722 826C04B8 8AEC8523 531A6FD6 D7D6EA3C 254C75E3
67723773 75598CA7 83408A65 6ECB957A F28334B9 692B7807
8725CDC7 6C524E50 1F7702BA 6C10A98C 5A70D3C0 EABCFE04
081FAE95 48FB2EFE 699999A5 9EBBEF78 044E5700 26FE5B9B

```
        CB33871D 0C2F494C 05AA3AE9 BB148DF4 12BC608A F22A8143
        221513ED 9326499F 2154819E ED5B113F 9BBBABF2 C9251FF1
        AC5ED293 CA17BC7B F275CF4F 57036C78 F0A410B9 E37C24CD
        ADBEBDA2 6F7B8E20 521FD698 D4D1D209 67B7669D 044C2CF3
        BB235BAF 5BC7E520 2A3EA8FC E06D355F 733B59B6 45BF9F8D
        C5EE28A4 AACCA937 C1EA47E1 6F52234C A09CCEAF 9D056954
        E0023C73 7432230A 4BDBC3CB BA99B1A0 F20CC7FE AC6A41BA
        B8C2C639 F93C7BEC F416E757 558D124D 899E20BA 2144348B
        1B7E0769 770DFFDA 9B5A8FF4 D0519705 50EBE74B 32A92119


MacKey is
                        70C0460A 7E4434DD DB81874C 9F2A5A37


Mtag is
                        578008F9 D8BC5E9A BF92E4AE 99EDB577


KeyData is
                        B104D11B F56C2933 4F07743D C437BA2F
        C6DF5D93 635357DD 1A6E780C 15A3A2CD 5E91FE49 6D8247AB
        6AE7DFC9 6923261E 43EE77F1 280AE2F9 C80D75EE CBFF455A




------------------------------------------------------------
Scheme Responder, Key Confirmation Provider: V to U
Z is
                        5713B6EE F9D248C6 E87885EA FD7CB70A
        111AB995 9C5BDAB1 2FF68951 3DBB0154 0222DA46 ACE4FBC8
        8689BD44 844AA092 2AF444CF 9C88E35C 8BA23131 4617A5A7
        C33B4385 63A38258 C31900C1 55D4D523 F7879A67 09D84E9E
        2765DC74 459ECB26 C3646124 477D68DE 0599E25E FC26C40B
        5929D37B 8D273DE1 4D345C8A 0DC61A28 ACA556BE 431D1B54
        AAD2C2F0 81B19693 0EDFE4D0 75746094 C90A780A 66F2AEFC
        08C3E1F6 143981E4 CDDFCE1E C104A89C C770A9C8 D26B6270
        4C7C148B 481D02C1 DCC81428 7AF7F99C 9139DAA5 13B8F043
        6F656B14 65E69213 73B08EAA 553CE81D 087EA4E7 E4421A1A
        1423C47D 9818E975 8ED18470 208ACC35 E346A143 227C16BB


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536
```

KDFval is
                                                70C0460A 7E4434DD
        DB81874C 9F2A5A37 B104D11B F56C2933 4F07743D C437BA2F
        C6DF5D93 635357DD 1A6E780C 15A3A2CD 5E91FE49 6D8247AB
        6AE7DFC9 6923261E 43EE77F1 280AE2F9 C80D75EE CBFF455A

MacData is
        4B435F31 5F56424F 42425941 4C494345 1F7702BA 6C10A98C
        5A70D3C0 EABCFE04 081FAE95 48FB2EFE 699999A5 9EBBEF78
        044E5700 26FE5B9B CB33871D 0C2F494C 05AA3AE9 BB148DF4
        12BC608A F22A8143 221513ED 9326499F 2154819E ED5B113F
        9BBBABF2 C9251FF1 AC5ED293 CA17BC7B F275CF4F 57036C78
        F0A410B9 E37C24CD ADBEBDA2 6F7B8E20 521FD698 D4D1D209
        67B7669D 044C2CF3 BB235BAF 5BC7E520 2A3EA8FC E06D355F
        733B59B6 45BF9F8D C5EE28A4 AACCA937 C1EA47E1 6F52234C
        A09CCEAF 9D056954 E0023C73 7432230A 4BDBC3CB BA99B1A0
        F20CC7FE AC6A41BA B8C2C639 F93C7BEC F416E757 558D124D
        899E20BA 2144348B 1B7E0769 770DFFDA 9B5A8FF4 D0519705
        50EBE74B 32A92119 31BACD07 71AE01D1 58C4C5A5 EAB21226
        A2AAB682 8589CD21 977C7131 D3D8CAC7 8CB1F20A C4D51391
        AA42EB53 B7F6C832 D921988F 7696700D 91EF3319 4FCDC9C3
        EE2B531B F9CE7329 996769F1 0636FA99 4D975709 EAF7E30F
        FD7983E9 26D75E30 44559023 6FE9CB41 2CA553F8 AD3E6FD5
        B52FCD92 D65AE374 0665A719 6EB9F6F9 2AFF8798 B0206839
        ED1D0481 A52E5623 EB6D5C6E DCC23711 C7F66C86 EDE8E41F
        A97765A5 491BF90B 6CB923C7 49173B2F E4A8C6E7 932D9B77
        A15F4D2D 3DF3F181 D8A8A56B 8B7020F3 BBD1C722 826C04B8
        8AEC8523 531A6FD6 D7D6EA3C 254C75E3 67723773 75598CA7
        83408A65 6ECB957A F28334B9 692B7807 8725CDC7 6C524E50

MacKey is
                        70C0460A 7E4434DD DB81874C 9F2A5A37

Mtag is
                        08CD11C2 4EA59CC3 EB95B4E3 CEADB71D

KeyData is
                        B104D11B F56C2933 4F07743D C437BA2F
        C6DF5D93 635357DD 1A6E780C 15A3A2CD 5E91FE49 6D8247AB
        6AE7DFC9 6923261E 43EE77F1 280AE2F9 C80D75EE CBFF455A

```
-----------------------------------------------------------
Scheme Initiator, Key Confirmation Bilateral
Z is
                          5713B6EE F9D248C6 E87885EA FD7CB70A
        111AB995 9C5BDAB1 2FF68951 3DBB0154 0222DA46 ACE4FBC8
        8689BD44 844AA092 2AF444CF 9C88E35C 8BA23131 4617A5A7
        C33B4385 63A38258 C31900C1 55D4D523 F7879A67 09D84E9E
        2765DC74 459ECB26 C3646124 477D68DE 0599E25E FC26C40B
        5929D37B 8D273DE1 4D345C8A 0DC61A28 ACA556BE 431D1B54
        AAD2C2F0 81B19693 0EDFE4D0 75746094 C90A780A 66F2AEFC
        08C3E1F6 143981E4 CDDFCE1E C104A89C C770A9C8 D26B6270
        4C7C148B 481D02C1 DCC81428 7AF7F99C 9139DAA5 13B8F043
        6F656B14 65E69213 73B08EAA 553CE81D 087EA4E7 E4421A1A
        1423C47D 9818E975 8ED18470 208ACC35 E346A143 227C16BB


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


KDFval is
                                                  70C0460A 7E4434DD
        DB81874C 9F2A5A37 B104D11B F56C2933 4F07743D C437BA2F
        C6DF5D93 635357DD 1A6E780C 15A3A2CD 5E91FE49 6D8247AB
        6AE7DFC9 6923261E 43EE77F1 280AE2F9 C80D75EE CBFF455A


U2V
----------------
MacData is
        4B435F32 5F55414C 49434542 4F424259 31BACD07 71AE01D1
        58C4C5A5 EAB21226 A2AAB682 8589CD21 977C7131 D3D8CAC7
        8CB1F20A C4D51391 AA42EB53 B7F6C832 D921988F 7696700D
        91EF3319 4FCDC9C3 EE2B531B F9CE7329 996769F1 0636FA99
        4D975709 EAF7E30F FD7983E9 26D75E30 44559023 6FE9CB41
        2CA553F8 AD3E6FD5 B52FCD92 D65AE374 0665A719 6EB9F6F9
        2AFF8798 B0206839 ED1D0481 A52E5623 EB6D5C6E DCC23711
        C7F66C86 EDE8E41F A97765A5 491BF90B 6CB923C7 49173B2F
        E4A8C6E7 932D9B77 A15F4D2D 3DF3F181 D8A8A56B 8B7020F3
        BBD1C722 826C04B8 8AEC8523 531A6FD6 D7D6EA3C 254C75E3
        67723773 75598CA7 83408A65 6ECB957A F28334B9 692B7807
        8725CDC7 6C524E50 1F7702BA 6C10A98C 5A70D3C0 EABCFE04
        081FAE95 48FB2EFE 699999A5 9EBBEF78 044E5700 26FE5B9B
```

CB33871D 0C2F494C 05AA3AE9 BB148DF4 12BC608A F22A8143
221513ED 9326499F 2154819E ED5B113F 9BBBABF2 C9251FF1
AC5ED293 CA17BC7B F275CF4F 57036C78 F0A410B9 E37C24CD
ADBEBDA2 6F7B8E20 521FD698 D4D1D209 67B7669D 044C2CF3
BB235BAF 5BC7E520 2A3EA8FC E06D355F 733B59B6 45BF9F8D
C5EE28A4 AACCA937 C1EA47E1 6F52234C A09CCEAF 9D056954
E0023C73 7432230A 4BDBC3CB BA99B1A0 F20CC7FE AC6A41BA
B8C2C639 F93C7BEC F416E757 558D124D 899E20BA 2144348B
1B7E0769 770DFFDA 9B5A8FF4 D0519705 50EBE74B 32A92119

MacKey is
70C0460A 7E4434DD DB81874C 9F2A5A37

Mtag is
4FF2D69D 454FCCA6 77D433B6 29921F3B

V2U

MacData is
4B435F32 5F56424F 42425941 4C494345 1F7702BA 6C10A98C
5A70D3C0 EABCFE04 081FAE95 48FB2EFE 699999A5 9EBBEF78
044E5700 26FE5B9B CB33871D 0C2F494C 05AA3AE9 BB148DF4
12BC608A F22A8143 221513ED 9326499F 2154819E ED5B113F
9BBBABF2 C9251FF1 AC5ED293 CA17BC7B F275CF4F 57036C78
F0A410B9 E37C24CD ADBEBDA2 6F7B8E20 521FD698 D4D1D209
67B7669D 044C2CF3 BB235BAF 5BC7E520 2A3EA8FC E06D355F
733B59B6 45BF9F8D C5EE28A4 AACCA937 C1EA47E1 6F52234C
A09CCEAF 9D056954 E0023C73 7432230A 4BDBC3CB BA99B1A0
F20CC7FE AC6A41BA B8C2C639 F93C7BEC F416E757 558D124D
899E20BA 2144348B 1B7E0769 770DFFDA 9B5A8FF4 D0519705
50EBE74B 32A92119 31BACD07 71AE01D1 58C4C5A5 EAB21226
A2AAB682 8589CD21 977C7131 D3D8CAC7 8CB1F20A C4D51391
AA42EB53 B7F6C832 D921988F 7696700D 91EF3319 4FCDC9C3
EE2B531B F9CE7329 996769F1 0636FA99 4D975709 EAF7E30F
FD7983E9 26D75E30 44559023 6FE9CB41 2CA553F8 AD3E6FD5
B52FCD92 D65AE374 0665A719 6EB9F6F9 2AFF8798 B0206839
ED1D0481 A52E5623 EB6D5C6E DCC23711 C7F66C86 EDE8E41F
A97765A5 491BF90B 6CB923C7 49173B2F E4A8C6E7 932D9B77
A15F4D2D 3DF3F181 D8A8A56B 8B7020F3 BBD1C722 826C04B8
8AEC8523 531A6FD6 D7D6EA3C 254C75E3 67723773 75598CA7
83408A65 6ECB957A F28334B9 692B7807 8725CDC7 6C524E50

```
MacKey is
                        70C0460A 7E4434DD DB81874C 9F2A5A37


Mtag is
                        EDA710AF E416AC09 38CCE3B3 7122F789


KeyData is
                        B104D11B F56C2933 4F07743D C437BA2F
        C6DF5D93 635357DD 1A6E780C 15A3A2CD 5E91FE49 6D8247AB
        6AE7DFC9 6923261E 43EE77F1 280AE2F9 C80D75EE CBFF455A


============================================================


dhEphem(256)
------------------------------------------------------------
rU is
                                                0881382C DB87660C
        6DC13E61 4938D5B9 C8B2F248 581CC5E3 1B354543 97FCE50E


tU is
                        2E9380C8 323AF975 45BC4941 DEB0EC37
        42C62FE0 ECE824A6 ABDBE66C 59BEE024 2911BFB9 67235CEB
        A35AE13E 4EC752BE 630B92DC 4BDE2847 A9C62CB8 15274542
        1FB7EB60 A63C0FE9 159FCCE7 26CE7CD8 523D7450 667EF840
        E4919121 EB5F01C8 C9B0D3D6 48A93BFB 75689E82 44AC134A
        F544711C E79A02DC C3422668 4780DDDC B4985941 06C37F5B
        C7985648 7AF5AB02 2A2E5E42 F09897C1 A85A11EA 0212AF04
        D9B4CEBC 937C3C1A 3E15A8A0 342E3376 15C84E7F E3B8B9B8
        7FB1E73A 15AF12A3 0D746E06 DFC34F29 0D797CE5 1AA13AA7
        85BF6658 AFF5E4B0 93003CBE AF665B3C 2E113A3A 4E905269
        341DC071 1426685F 4EF37E86 8A8126FF 3F2279B5 7CA67E29


rV is
                                                7D62A7E3 EF36DE61
        7B13D1AF B82C780D 83A23BD4 EE670564 5121F371 F546A53D


tV is
                        575F0351 BD2B1B81 7448BDF8 7A6C362C
        1E289D39 03A30B98 32C5741F A250363E 7ACBC7F7 7F3DACBC
```

```
        1F131ADD 8E03367E FF8FBBB3 E1C57844 24809B25 AFE4D226
        2A1A6FD2 FAB64105 CA30A674 E07F7809 85208863 2FC04923
        3791AD4E DD083A97 8B883EE6 18BC5E0D D047415F 2D95E683
        CF14826B 5FBE10D3 CE41C6C1 20C78AB2 0008C698 BF7F0BCA
        B9D7F407 BED0F43A FB2970F5 7F8D1204 3963E66D DD320D59
        9AD9936C 8F44137C 08B180EC 5E985CEB E186F3D5 49677E80
        607331EE 17AF3380 A725B078 2317D7DD 43F59D7A F9568A9B
        B63A84D3 65F92244 ED120988 219302F4 2924C7CA 90B89D24
        F71B0AB6 97823D7D EB1AFF5B 0E8E4A45 D49F7F53 757E1913



------------------------------------------------------------
no Key Confirmation
Z is
                        86C70BF8 D0BB81BB 01078A17 219CB7D2
        7203DB2A 19C877F1 D1F19FD7 D77EF225 46A68F00 5AD52DC8
        4553B78F C60330BE 51EA7C06 72CAC151 5E4B35C0 47B9A551
        B88F39DC 26DA14A0 9EF74774 D47C762D D177F9ED 5BC2F11E
        52C879BD 95098504 CD9EECD8 A8F9B3EF BD1F008A C5853097
        D9D1837F 2B18F77C D7BE01AF 80A7C7B5 EA3CA54C C02D0C11
        6FEE3F95 BB873993 85875D7E 86747E67 6E728938 ACBFF709
        8E05BE4D CFB24052 B83AEFFB 14783F02 9ADBDE7F 53FAE920
        84224090 E007CEE9 4D4BF2BA CE9FFD4B 57D2AF7C 724D0CAA
        19BF0501 F6F17B4A A10F425E 3EA76080 B4B9D6B3 CEFEA115
        B2CEB878 9BB8A3B0 EA87FEBE 63B6C8F8 46EC6DB0 C26C5D7C


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


KDFval is
                        43E728EE 01356F51 07F22746 CDB11B87
        92AF4120 1B337464 33196196 FB4E4985 AFACD373 761ADFA0
        CA45183D 1DA6C92B E3A11325 AA26FC53 028D70E8 EE97F203


KeyData is
                        43E728EE 01356F51 07F22746 CDB11B87
        92AF4120 1B337464 33196196 FB4E4985 AFACD373 761ADFA0
        CA45183D 1DA6C92B E3A11325 AA26FC53 028D70E8 EE97F203


============================================================
```

```
dhHybridOneFlow(256)
------------------------------------------------------------
xU is
                                                50747886 14D3894F
        98934CAD 9700E887 2E1FB6AD BFD54521 6B218FB3 244188B0


yU is
                         5DDE1EF2 670295BA A29AB5D0 CA52380D
        7C0D08C8 D7C35CA1 48F8D568 D67B5B0C FBA261E7 590ACA11
        83792006 268F5B7D DEBDFB7D 73D48940 DB60C800 13044C70
        15B63BF3 F6922D5A 9150A2BC 742520A0 4260C29E E75250CC
        E52D2794 7687C777 5F918CCD 07C98C2D 97CF4F91 78C6BEBC
        663808AA 74909264 FC14C0CA 358D3A1C 9E9394BE 3FB885BE
        B50F14D4 A77B3AA1 4623549B 8B43B864 99171F8F C74BCDA0
        B9280314 27B2491B 5B02D311 F0A6EFCD 68C5574E 7DBE00D1
        8C5EF846 52182F17 D0EB416D 36C8947D 7DAFD3FC 4EBFA9C0
        25378483 05EEE467 AAD8125B DD42356A 2F07E5E8 A5A10AB7
        547BE3A1 E487986E 47391635 BD43C762 0A560D67 F6580661


xV is
                                                8963089D B60A16FA
        B2B87138 50C9E56A 47DEC386 36AFFFFF E7C88A67 AC0A393B


yV is
                         7B88BFB5 DD684755 A822EDF2 3235EC6F
        C61DE430 30C9F0EF 38444B96 88337004 4AB21BD2 22811539
        934F92E6 F4347084 1CDC849E D61BD3EF E6413CCB F3E3FFEC
        6B629331 2690C881 10A2C1FB CA2DF7C1 96B5CD01 EA7975E2
        C525089B D2783B11 35DF884B 8F8D743F D52E874C DF401FBC
        2846AF50 2C494090 4DA7B47A 4CEFEC29 5B6EBD68 147944CC
        97773E18 2B8848F2 105E5193 B04A0E20 181B4F69 BBB98B7A
        C94D131E 2416AAB9 A5858CCC 68BFDDC4 4CA7DC22 7EA9B618
        3887658B 575C44FF 4A536BDD 2F358EAD BB37E4AF 3C0E6151
        DA73C9F7 20C6E69E 6A6EAB0E 53ED6A86 0395647B 3255BBE8
        C41FC36F 29073119 11AFC1B9 97A7BD9A 00D0362C 645E2BB8


rU is
                                                30615E1E 9F6D6B97
        28963E76 CE8ECB8B 44CE61BC 76FA4C6A 903A2E9A 70114B2B
```

tU is
0AB497C2 CDE8456F 56922239 140BED9E
1D09B5AB CCB84341 63BD4CD3 559DEC35 2F3BDE1A B3C5DCD8
42B6BEB9 009679C6 DF6D3FB5 60188FB1 255AE1AB D7CC1894
DC4413BA 139831F4 68465C89 581A6995 B6FAC3FA E945FCC3
C8C3D555 A4E950C6 00EBB058 313E44F6 3463552E 1DCA28A5
7D36E5F4 694DC67B 8CCA855C AD6750D6 0F9DF426 84EB6B1A
A0E7962E 42217AF5 7A66AC2A 8A387341 2D3A9F24 01D91CC8
8CC0C935 56C7992B 9BCB3DB3 484B5C9E 56208519 116F4BE4
E88E90D3 50B4110E 0785445A 2A506F42 73DE95AB 035A637A
5526B711 85F7B67F 6F95A608 7FF8836B 998EF574 A53072C2
2CD97F17 D4F08F40 E639B674 251BA582 67F6985E 3B606295

---

no Key Confirmation
Zs is
552B5323 50CD2FC9 0263F1ED 74DA5C37
DCCBC3A1 7C8BA769 AEC10114 8DACB80C BAFED968 DA74FE33
9C037DE5 9C0F8404 910174B7 278929BD 8509D021 6CE06DCD
C1FBAEF4 A47B4CB8 AAD97448 98DA2080 92B5E591 BD17BFA0
86C1B134 5C8F8F01 FE809A24 8A1426DD 7CA849CE E343E614
2ADA16A8 46568ADF 98BE53CD C2BEA9F1 6B98612E 416FC9D4
E882DD0D 1480B83B DBC81E30 708A24EF F1C4FD98 AD4DC843
7F16739D 92E198CE 6702C083 ED75306E 56F3837F D9EE5A0F
65FA6EA2 DCFF547B DDA5B4BD 187695F4 026417D0 767DE59C
355211C9 754D1ED8 DBFAD415 449998EF 1C635F06 ED04E7B4
D3B677E8 092BFF0B 7E3A99A0 E068B7E7 536BFB62 368002ED

Ze is
26539E6A 05909271 A3A8DFBF A6C5C1CB
EECB9B38 83CF2DA5 392955FD A44740A8 EBDCBFAA CF173787
8540DADF FBDC999C D08D32A2 CBD32350 5EECE030 B2947018
9EC79C04 3E1C26C6 15C61E43 4A8477A0 578D2772 549B11DD
4E872764 B34385F8 B1C36ECC 3FB2411F F43BA64D 8C5628A7
946CC6A7 918BF11E 5BB952E1 5A1000C2 C90AACAB 62334B3F
4FEFD46E 0A3A1232 FB286FFC 9ADF93B9 5912965F 5DE46D54
6CFE24F8 B7903FD2 EF6B123E 544E375C 3DCBA92A CDF9C93A
ABC68D87 3D3CF3C0 41528D87 6065CC6F 4258BE06 06CB79F4
C10F2CDC C126ADE1 462FED22 5192475F 7D91EF04 A3F39309
10215A1D 5D08D6A0 575419C4 8B804E96 5860FC4B 701BCA2D

Z is
                                                26539E6A 05909271
        A3A8DFBF A6C5C1CB EECB9B38 83CF2DA5 392955FD A44740A8
        EBDCBFAA CF173787 8540DADF FBDC999C D08D32A2 CBD32350
        5EECE030 B2947018 9EC79C04 3E1C26C6 15C61E43 4A8477A0
        578D2772 549B11DD 4E872764 B34385F8 B1C36ECC 3FB2411F
        F43BA64D 8C5628A7 946CC6A7 918BF11E 5BB952E1 5A1000C2
        C90AACAB 62334B3F 4FEFD46E 0A3A1232 FB286FFC 9ADF93B9
        5912965F 5DE46D54 6CFE24F8 B7903FD2 EF6B123E 544E375C
        3DCBA92A CDF9C93A ABC68D87 3D3CF3C0 41528D87 6065CC6F
        4258BE06 06CB79F4 C10F2CDC C126ADE1 462FED22 5192475F
        7D91EF04 A3F39309 10215A1D 5D08D6A0 575419C4 8B804E96
        5860FC4B 701BCA2D 552B5323 50CD2FC9 0263F1ED 74DA5C37
        DCCBC3A1 7C8BA769 AEC10114 8DACB80C BAFED968 DA74FE33
        9C037DE5 9C0F8404 910174B7 278929BD 8509D021 6CE06DCD
        C1FBAEF4 A47B4CB8 AAD97448 98DA2080 92B5E591 BD17BFA0
        86C1B134 5C8F8F01 FE809A24 8A1426DD 7CA849CE E343E614
        2ADA16A8 46568ADF 98BE53CD C2BEA9F1 6B98612E 416FC9D4
        E882DD0D 1480B83B DBC81E30 708A24EF F1C4FD98 AD4DC843
        7F16739D 92E198CE 6702C083 ED75306E 56F3837F D9EE5A0F
        65FA6EA2 DCFF547B DDA5B4BD 187695F4 026417D0 767DE59C
        355211C9 754D1ED8 DBFAD415 449998EF 1C635F06 ED04E7B4
        D3B677E8 092BFF0B 7E3A99A0 E068B7E7 536BFB62 368002ED

OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536

KDFval is
                         211E46BB CFF4502C F719C952 6D37738B
        E1173440 5ECCBC0B 64166E3F FC228556 F3758678 BDF7823E
        63C09375 04C922D0 D00CAB82 B39223C1 A2EAB529 EAC4C24E

KeyData is
                         211E46BB CFF4502C F719C952 6D37738B
        E1173440 5ECCBC0B 64166E3F FC228556 F3758678 BDF7823E
        63C09375 04C922D0 D00CAB82 B39223C1 A2EAB529 EAC4C24E

Scheme Initiator, Key Confirmation Provider: U to V

NonceV is

```
                                                08A04CED 97B00731
        33B4DD87 3DBAD54C A5B7848C 09A13B66 F2408417 218B037A
```

Zs is

```
                         552B5323 50CD2FC9 0263F1ED 74DA5C37
        DCCBC3A1 7C8BA769 AEC10114 8DACB80C BAFED968 DA74FE33
        9C037DE5 9C0F8404 910174B7 278929BD 8509D021 6CE06DCD
        C1FBAEF4 A47B4CB8 AAD97448 98DA2080 92B5E591 BD17BFA0
        86C1B134 5C8F8F01 FE809A24 8A1426DD 7CA849CE E343E614
        2ADA16A8 46568ADF 98BE53CD C2BEA9F1 6B98612E 416FC9D4
        E882DD0D 1480B83B DBC81E30 708A24EF F1C4FD98 AD4DC843
        7F16739D 92E198CE 6702C083 ED75306E 56F3837F D9EE5A0F
        65FA6EA2 DCFF547B DDA5B4BD 187695F4 026417D0 767DE59C
        355211C9 754D1ED8 DBFAD415 449998EF 1C635F06 ED04E7B4
        D3B677E8 092BFF0B 7E3A99A0 E068B7E7 536BFB62 368002ED
```

Ze is

```
                         26539E6A 05909271 A3A8DFBF A6C5C1CB
        EECB9B38 83CF2DA5 392955FD A44740A8 EBDCBFAA CF173787
        8540DADF FBDC999C D08D32A2 CBD32350 5EECE030 B2947018
        9EC79C04 3E1C26C6 15C61E43 4A8477A0 578D2772 549B11DD
        4E872764 B34385F8 B1C36ECC 3FB2411F F43BA64D 8C5628A7
        946CC6A7 918BF11E 5BB952E1 5A1000C2 C90AACAB 62334B3F
        4FEFD46E 0A3A1232 FB286FFC 9ADF93B9 5912965F 5DE46D54
        6CFE24F8 B7903FD2 EF6B123E 544E375C 3DCBA92A CDF9C93A
        ABC68D87 3D3CF3C0 41528D87 6065CC6F 4258BE06 06CB79F4
        C10F2CDC C126ADE1 462FED22 5192475F 7D91EF04 A3F39309
        10215A1D 5D08D6A0 575419C4 8B804E96 5860FC4B 701BCA2D
```

Z is

```
                                                26539E6A 05909271
        A3A8DFBF A6C5C1CB EECB9B38 83CF2DA5 392955FD A44740A8
        EBDCBFAA CF173787 8540DADF FBDC999C D08D32A2 CBD32350
        5EECE030 B2947018 9EC79C04 3E1C26C6 15C61E43 4A8477A0
        578D2772 549B11DD 4E872764 B34385F8 B1C36ECC 3FB2411F
        F43BA64D 8C5628A7 946CC6A7 918BF11E 5BB952E1 5A1000C2
        C90AACAB 62334B3F 4FEFD46E 0A3A1232 FB286FFC 9ADF93B9
        5912965F 5DE46D54 6CFE24F8 B7903FD2 EF6B123E 544E375C
        3DCBA92A CDF9C93A ABC68D87 3D3CF3C0 41528D87 6065CC6F
        4258BE06 06CB79F4 C10F2CDC C126ADE1 462FED22 5192475F
        7D91EF04 A3F39309 10215A1D 5D08D6A0 575419C4 8B804E96
        5860FC4B 701BCA2D 552B5323 50CD2FC9 0263F1ED 74DA5C37
```

```
        DCCBC3A1 7C8BA769 AEC10114 8DACB80C BAFED968 DA74FE33
        9C037DE5 9C0F8404 910174B7 278929BD 8509D021 6CE06DCD
        C1FBAEF4 A47B4CB8 AAD97448 98DA2080 92B5E591 BD17BFA0
        86C1B134 5C8F8F01 FE809A24 8A1426DD 7CA849CE E343E614
        2ADA16A8 46568ADF 98BE53CD C2BEA9F1 6B98612E 416FC9D4
        E882DD0D 1480B83B DBC81E30 708A24EF F1C4FD98 AD4DC843
        7F16739D 92E198CE 6702C083 ED75306E 56F3837F D9EE5A0F
        65FA6EA2 DCFF547B DDA5B4BD 187695F4 026417D0 767DE59C
        355211C9 754D1ED8 DBFAD415 449998EF 1C635F06 ED04E7B4
        D3B677E8 092BFF0B 7E3A99A0 E068B7E7 536BFB62 368002ED


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


KDFval is
                                                 211E46BB CFF4502C
        F719C952 6D37738B E1173440 5ECCBC0B 64166E3F FC228556
        F3758678 BDF7823E 63C09375 04C922D0 D00CAB82 B39223C1
        A2EAB529 EAC4C24E 274CF122 D9CFFBA1 BA744325 E71543C5


MacData is
                         4B435F31 5F55414C 49434542 4F424259
        0AB497C2 CDE8456F 56922239 140BED9E 1D09B5AB CCB84341
        63BD4CD3 559DEC35 2F3BDE1A B3C5DCD8 42B6BEB9 009679C6
        DF6D3FB5 60188FB1 255AE1AB D7CC1894 DC4413BA 139831F4
        68465C89 581A6995 B6FAC3FA E945FCC3 C8C3D555 A4E950C6
        00EBB058 313E44F6 3463552E 1DCA28A5 7D36E5F4 694DC67B
        8CCA855C AD6750D6 0F9DF426 84EB6B1A A0E7962E 42217AF5
        7A66AC2A 8A387341 2D3A9F24 01D91CC8 8CC0C935 56C7992B
        9BCB3DB3 484B5C9E 56208519 116F4BE4 E88E90D3 50B4110E
        0785445A 2A506F42 73DE95AB 035A637A 5526B711 85F7B67F
        6F95A608 7FF8836B 998EF574 A53072C2 2CD97F17 D4F08F40
        E639B674 251BA582 67F6985E 3B606295 08A04CED 97B00731
        33B4DD87 3DBAD54C A5B7848C 09A13B66 F2408417 218B037A


MacKey is
                         211E46BB CFF4502C F719C952 6D37738B


Mtag is
                         008116B9 5807D2CD 6DC706B7 B62D2174
```

KeyData is
                        E1173440 5ECCBC0B 64166E3F FC228556
        F3758678 BDF7823E 63C09375 04C922D0 D00CAB82 B39223C1
        A2EAB529 EAC4C24E 274CF122 D9CFFBA1 BA744325 E71543C5

Scheme Responder, Key Confirmation Provider: V to U
NonceU is
                                            08A04CED 97B00731
        33B4DD87 3DBAD54C A5B7848C 09A13B66 F2408417 218B037A

Zs is
                        552B5323 50CD2FC9 0263F1ED 74DA5C37
        DCCBC3A1 7C8BA769 AEC10114 8DACB80C BAFED968 DA74FE33
        9C037DE5 9C0F8404 910174B7 278929BD 8509D021 6CE06DCD
        C1FBAEF4 A47B4CB8 AAD97448 98DA2080 92B5E591 BD17BFA0
        86C1B134 5C8F8F01 FE809A24 8A1426DD 7CA849CE E343E614
        2ADA16A8 46568ADF 98BE53CD C2BEA9F1 6B98612E 416FC9D4
        E882DD0D 1480B83B DBC81E30 708A24EF F1C4FD98 AD4DC843
        7F16739D 92E198CE 6702C083 ED75306E 56F3837F D9EE5A0F
        65FA6EA2 DCFF547B DDA5B4BD 187695F4 026417D0 767DE59C
        355211C9 754D1ED8 DBFAD415 449998EF 1C635F06 ED04E7B4
        D3B677E8 092BFF0B 7E3A99A0 E068B7E7 536BFB62 368002ED

Ze is
                        26539E6A 05909271 A3A8DFBF A6C5C1CB
        EECB9B38 83CF2DA5 392955FD A44740A8 EBDCBFAA CF173787
        8540DADF FBDC999C D08D32A2 CBD32350 5EECE030 B2947018
        9EC79C04 3E1C26C6 15C61E43 4A8477A0 578D2772 549B11DD
        4E872764 B34385F8 B1C36ECC 3FB2411F F43BA64D 8C5628A7
        946CC6A7 918BF11E 5BB952E1 5A1000C2 C90AACAB 62334B3F
        4FEFD46E 0A3A1232 FB286FFC 9ADF93B9 5912965F 5DE46D54
        6CFE24F8 B7903FD2 EF6B123E 544E375C 3DCBA92A CDF9C93A
        ABC68D87 3D3CF3C0 41528D87 6065CC6F 4258BE06 06CB79F4
        C10F2CDC C126ADE1 462FED22 5192475F 7D91EF04 A3F39309
        10215A1D 5D08D6A0 575419C4 8B804E96 5860FC4B 701BCA2D

Z is
                                            26539E6A 05909271

A3A8DFBF A6C5C1CB EECB9B38 83CF2DA5 392955FD A44740A8
EBDCBFAA CF173787 8540DADF FBDC999C D08D32A2 CBD32350
5EECE030 B2947018 9EC79C04 3E1C26C6 15C61E43 4A8477A0
578D2772 549B11DD 4E872764 B34385F8 B1C36ECC 3FB2411F
F43BA64D 8C5628A7 946CC6A7 918BF11E 5BB952E1 5A1000C2
C90AACAB 62334B3F 4FEFD46E 0A3A1232 FB286FFC 9ADF93B9
5912965F 5DE46D54 6CFE24F8 B7903FD2 EF6B123E 544E375C
3DCBA92A CDF9C93A ABC68D87 3D3CF3C0 41528D87 6065CC6F
4258BE06 06CB79F4 C10F2CDC C126ADE1 462FED22 5192475F
7D91EF04 A3F39309 10215A1D 5D08D6A0 575419C4 8B804E96
5860FC4B 701BCA2D 552B5323 50CD2FC9 0263F1ED 74DA5C37
DCCBC3A1 7C8BA769 AEC10114 8DACB80C BAFED968 DA74FE33
9C037DE5 9C0F8404 910174B7 278929BD 8509D021 6CE06DCD
C1FBAEF4 A47B4CB8 AAD97448 98DA2080 92B5E591 BD17BFA0
86C1B134 5C8F8F01 FE809A24 8A1426DD 7CA849CE E343E614
2ADA16A8 46568ADF 98BE53CD C2BEA9F1 6B98612E 416FC9D4
E882DD0D 1480B83B DBC81E30 708A24EF F1C4FD98 AD4DC843
7F16739D 92E198CE 6702C083 ED75306E 56F3837F D9EE5A0F
65FA6EA2 DCFF547B DDA5B4BD 187695F4 026417D0 767DE59C
355211C9 754D1ED8 DBFAD415 449998EF 1C635F06 ED04E7B4
D3B677E8 092BFF0B 7E3A99A0 E068B7E7 536BFB62 368002ED

OtherInfo is
12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536

KDFval is
211E46BB CFF4502C
F719C952 6D37738B E1173440 5ECCBC0B 64166E3F FC228556
F3758678 BDF7823E 63C09375 04C922D0 D00CAB82 B39223C1
A2EAB529 EAC4C24E 274CF122 D9CFFBA1 BA744325 E71543C5

MacData is
4B435F31 5F56424F
42425941 4C494345 0AB497C2 CDE8456F 56922239 140BED9E
1D09B5AB CCB84341 63BD4CD3 559DEC35 2F3BDE1A B3C5DCD8
42B6BEB9 009679C6 DF6D3FB5 60188FB1 255AE1AB D7CC1894
DC4413BA 139831F4 68465C89 581A6995 B6FAC3FA E945FCC3
C8C3D555 A4E950C6 00EBB058 313E44F6 3463552E 1DCA28A5
7D36E5F4 694DC67B 8CCA855C AD6750D6 0F9DF426 84EB6B1A
A0E7962E 42217AF5 7A66AC2A 8A387341 2D3A9F24 01D91CC8
8CC0C935 56C7992B 9BCB3DB3 484B5C9E 56208519 116F4BE4
E88E90D3 50B4110E 0785445A 2A506F42 73DE95AB 035A637A
5526B711 85F7B67F 6F95A608 7FF8836B 998EF574 A53072C2

2CD97F17 D4F08F40 E639B674 251BA582 67F6985E 3B606295

MacKey is
211E46BB CFF4502C F719C952 6D37738B

Mtag is
A2EE5EF5 A8C38A74 1A28B4EE 2AD99554

KeyData is
E1173440 5ECCBC0B 64166E3F FC228556
F3758678 BDF7823E 63C09375 04C922D0 D00CAB82 B39223C1
A2EAB529 EAC4C24E 274CF122 D9CFFBA1 BA744325 E71543C5

Scheme Initiator, Key Confirmation Bilateral
NonceV is
08A04CED 97B00731
33B4DD87 3DBAD54C A5B7848C 09A13B66 F2408417 218B037A

Zs is
552B5323 50CD2FC9 0263F1ED 74DA5C37
DCCBC3A1 7C8BA769 AEC10114 8DACB80C BAFED968 DA74FE33
9C037DE5 9C0F8404 910174B7 278929BD 8509D021 6CE06DCD
C1FBAEF4 A47B4CB8 AAD97448 98DA2080 92B5E591 BD17BFA0
86C1B134 5C8F8F01 FE809A24 8A1426DD 7CA849CE E343E614
2ADA16A8 46568ADF 98BE53CD C2BEA9F1 6B98612E 416FC9D4
E882DD0D 1480B83B DBC81E30 708A24EF F1C4FD98 AD4DC843
7F16739D 92E198CE 6702C083 ED75306E 56F3837F D9EE5A0F
65FA6EA2 DCFF547B DDA5B4BD 187695F4 026417D0 767DE59C
355211C9 754D1ED8 DBFAD415 449998EF 1C635F06 ED04E7B4
D3B677E8 092BFF0B 7E3A99A0 E068B7E7 536BFB62 368002ED

Ze is
26539E6A 05909271 A3A8DFBF A6C5C1CB
EECB9B38 83CF2DA5 392955FD A44740A8 EBDCBFAA CF173787
8540DADF FBDC999C D08D32A2 CBD32350 5EECE030 B2947018
9EC79C04 3E1C26C6 15C61E43 4A8477A0 578D2772 549B11DD
4E872764 B34385F8 B1C36ECC 3FB2411F F43BA64D 8C5628A7

946CC6A7 918BF11E 5BB952E1 5A1000C2 C90AACAB 62334B3F
4FEFD46E 0A3A1232 FB286FFC 9ADF93B9 5912965F 5DE46D54
6CFE24F8 B7903FD2 EF6B123E 544E375C 3DCBA92A CDF9C93A
ABC68D87 3D3CF3C0 41528D87 6065CC6F 4258BE06 06CB79F4
C10F2CDC C126ADE1 462FED22 5192475F 7D91EF04 A3F39309
10215A1D 5D08D6A0 575419C4 8B804E96 5860FC4B 701BCA2D

Z is
26539E6A 05909271
A3A8DFBF A6C5C1CB EECB9B38 83CF2DA5 392955FD A44740A8
EBDCBFAA CF173787 8540DADF FBDC999C D08D32A2 CBD32350
5EECE030 B2947018 9EC79C04 3E1C26C6 15C61E43 4A8477A0
578D2772 549B11DD 4E872764 B34385F8 B1C36ECC 3FB2411F
F43BA64D 8C5628A7 946CC6A7 918BF11E 5BB952E1 5A1000C2
C90AACAB 62334B3F 4FEFD46E 0A3A1232 FB286FFC 9ADF93B9
5912965F 5DE46D54 6CFE24F8 B7903FD2 EF6B123E 544E375C
3DCBA92A CDF9C93A ABC68D87 3D3CF3C0 41528D87 6065CC6F
4258BE06 06CB79F4 C10F2CDC C126ADE1 462FED22 5192475F
7D91EF04 A3F39309 10215A1D 5D08D6A0 575419C4 8B804E96
5860FC4B 701BCA2D 552B5323 50CD2FC9 0263F1ED 74DA5C37
DCCBC3A1 7C8BA769 AEC10114 8DACB80C BAFED968 DA74FE33
9C037DE5 9C0F8404 910174B7 278929BD 8509D021 6CE06DCD
C1FBAEF4 A47B4CB8 AAD97448 98DA2080 92B5E591 BD17BFA0
86C1B134 5C8F8F01 FE809A24 8A1426DD 7CA849CE E343E614
2ADA16A8 46568ADF 98BE53CD C2BEA9F1 6B98612E 416FC9D4
E882DD0D 1480B83B DBC81E30 708A24EF F1C4FD98 AD4DC843
7F16739D 92E198CE 6702C083 ED75306E 56F3837F D9EE5A0F
65FA6EA2 DCFF547B DDA5B4BD 187695F4 026417D0 767DE59C
355211C9 754D1ED8 DBFAD415 449998EF 1C635F06 ED04E7B4
D3B677E8 092BFF0B 7E3A99A0 E068B7E7 536BFB62 368002ED

OtherInfo is
12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536

KDFval is
211E46BB CFF4502C
F719C952 6D37738B E1173440 5ECCBC0B 64166E3F FC228556
F3758678 BDF7823E 63C09375 04C922D0 D00CAB82 B39223C1
A2EAB529 EAC4C24E 274CF122 D9CFFBA1 BA744325 E71543C5

U2V

MacData is
                        4B435F32 5F55414C 49434542 4F424259
        0AB497C2 CDE8456F 56922239 140BED9E 1D09B5AB CCB84341
        63BD4CD3 559DEC35 2F3BDE1A B3C5DCD8 42B6BEB9 009679C6
        DF6D3FB5 60188FB1 255AE1AB D7CC1894 DC4413BA 139831F4
        68465C89 581A6995 B6FAC3FA E945FCC3 C8C3D555 A4E950C6
        00EBB058 313E44F6 3463552E 1DCA28A5 7D36E5F4 694DC67B
        8CCA855C AD6750D6 0F9DF426 84EB6B1A A0E7962E 42217AF5
        7A66AC2A 8A387341 2D3A9F24 01D91CC8 8CC0C935 56C7992B
        9BCB3DB3 484B5C9E 56208519 116F4BE4 E88E90D3 50B4110E
        0785445A 2A506F42 73DE95AB 035A637A 5526B711 85F7B67F
        6F95A608 7FF8836B 998EF574 A53072C2 2CD97F17 D4F08F40
        E639B674 251BA582 67F6985E 3B606295 08A04CED 97B00731
        33B4DD87 3DBAD54C A5B7848C 09A13B66 F2408417 218B037A

MacKey is
                        211E46BB CFF4502C F719C952 6D37738B

Mtag is
                        45AF68B2 CB093A48 FD174892 7A58D406

V2U

MacData is
                        4B435F32 5F56424F 42425941 4C494345
        08A04CED 97B00731 33B4DD87 3DBAD54C A5B7848C 09A13B66
        F2408417 218B037A 0AB497C2 CDE8456F 56922239 140BED9E
        1D09B5AB CCB84341 63BD4CD3 559DEC35 2F3BDE1A B3C5DCD8
        42B6BEB9 009679C6 DF6D3FB5 60188FB1 255AE1AB D7CC1894
        DC4413BA 139831F4 68465C89 581A6995 B6FAC3FA E945FCC3
        C8C3D555 A4E950C6 00EBB058 313E44F6 3463552E 1DCA28A5
        7D36E5F4 694DC67B 8CCA855C AD6750D6 0F9DF426 84EB6B1A
        A0E7962E 42217AF5 7A66AC2A 8A387341 2D3A9F24 01D91CC8
        8CC0C935 56C7992B 9BCB3DB3 484B5C9E 56208519 116F4BE4
        E88E90D3 50B4110E 0785445A 2A506F42 73DE95AB 035A637A
        5526B711 85F7B67F 6F95A608 7FF8836B 998EF574 A53072C2
        2CD97F17 D4F08F40 E639B674 251BA582 67F6985E 3B606295

MacKey is
                        211E46BB CFF4502C F719C952 6D37738B

```
Mtag is
                        8E35A256 0E539E6C 58745F42 674E415C


KeyData is
                        E1173440 5ECCBC0B 64166E3F FC228556
        F3758678 BDF7823E 63C09375 04C922D0 D00CAB82 B39223C1
        A2EAB529 EAC4C24E 274CF122 D9CFFBA1 BA744325 E71543C5


================================================================


MQV1(256)
----------------------------------------------------------
xU is
                                                26DC8BED 912F1348
        AAFBE989 657253AC B35A59D1 B20605BE B7282179 8B18F384


yU is
                        596A5667 612A3993 9B4A702B C43D8A26
        2E870EAC 656049BD BBA26825 EBBA837D E7AC76CA 449A8FEC
        52E4473F 9095F3F2 B3AF4AE1 0DECF8B1 DF2CB72C 42E5165B
        C82F0A43 47FD2FC8 E051BC3B 892A07A8 660AD8FC 280FB3CA
        5B0DB43D 70431981 BEA414DC ACF5B1F7 067812FB A99A30C4
        C98EB4F0 EA8A61B8 4FE98734 4150E3F4 6A9F0937 25D02440
        5F79B6E7 859BB633 6171FF06 E26C68E3 8A9F4D70 250CDDFD
        906CD0C1 F63C8DCC 35661830 99EFB28A 62259BD4 67A027C9
        C9640E31 545964A9 1C6B1A8D 8E441CB3 4139F2C8 78412613
        8284646D D23FFB7B 4336B533 AD32655F 657C320A F3669B11
        B947D648 9B5E412F F0C2107F E7477CA8 73260504 CDB33CBD


xV is
                                                2135EB4C 18326E44
        8977EE83 6FCACE6C 4504C536 FE8BFADE 6B7D1C12 762D84CF


yV is
                        85CDAF25 EACF7F2D 2DD51B86 1E6D9567
        3B033DE6 F7159FB3 DC69E037 188A8C24 7E8CB8D4 2639CE97
        64F0081C 54036D7D BDAEC329 7CDDD640 7150D907 55B5D5F7
        FE491C6B AE60E917 0E1CCE19 D525017D BE845801 2BBE7F9E
        30B87579 FB6AEACA FA6B7A7B 03F34D28 4135556C ADBEB3D6
        8DF84797 B72D5681 7D008952 08694A7E D935C796 34B9F92F
```

B5156FF5 A8DB725F 919D8FB0 CD07E1F9 5BC8FFD9 484F9E42
BD35335B 5614CB64 063B74CE 3B6BFFF5 5596171C EBC52630
0ADB8E18 B0662CBD AC318925 AD3DBE47 A4DBAD60 A9660745
C1A73B1C 27A2CF73 8BB56046 CE433E5A 30DC0E84 AF576E97
19F14CCB 988B9986 A7410240 45AFFDE4 26D63F0B CC04F1F7

rU is
20B7946C 867E65DD
D808FB43 86483B21 63679173 73D92D88 4737FFE9 8FCB04B6

tU is
58EA5EA6 75A27704 2C2E842C 05061136
B6B53163 20233F49 D5338C38 48C71852 738F6E1E 39371F50
C84A7910 2C76DA3B C1BFD15C 83CAA8D2 378D9C32 8C6E5CB0
8F669763 6BB13CC7 77A38855 9237858F 05606E0A 8014194E
9487DB1F F14E9903 E84EAB89 13EC38BC 439F2F38 5F2D1E34
DB4A538C AA6161BF 552AD467 62C4C404 75880763 D69AFA49
34DBEBD0 EB5388F4 CA3FE8FD B08948B3 1CDC1A5B 7814BD34
5C0F0EFD E4418C1A F6197C7E 8A02B3DB 78C28F67 EAF85130
F5E04A65 5AFC1673 29E13B3E 709B6255 97DE7A65 B15EB7A4
92154007 7CD43D24 5C060D5C 14F98AFE EC9B039B E1460A59
4A46CD16 7DA70237 27259822 91932C86 947B4D53 8B4B180D

---

no Key Confirmation
Z is
51DC2E96 72AA6621 4D32485E 17344B26
5C622A7F 2B7F2B8A E1B2EEA5 091C4DCC 0E3A7A7F B1610014
12BC7FB7 E923ABE0 CE876543 C6AF4A15 7ACB4E5F 3041B2EB
9CE411F5 A8BE3AD4 B1E45BA9 867EE3B9 C117C2F1 A813BD49
743AF2BE 3BE7093C 1E42D1BE DE2CF8D0 85A2FF6F 1A79DAC2
F2222D5C 80B26BAE F1153714 A778BA0C 7A4B4CB3 352B4A0A
D9B78B0E 92B78354 640927FF A3CB433E 3A11A2D8 FB5D2179
8033530B 95C02F67 B1734AA2 DD8DEEE4 9AEC1332 DFBF62A9
717C3F8F 1410D0EE A86D5CC7 2729BE13 33709895 06E9F228
75D593F3 9CB65C91 D7987A6E EECAFC18 C10AE7D1 93E54445
E41D0959 65705737 38A31262 40E75989 5681AD0C 86EA8364

OtherInfo is
12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536

KDFval is
                        979CA810 0BCF89EC 6DC9DA5F 62729DFA
        068AED5D 2BB085A4 B046D5EC 89CFE0DC CFC5D126 0B1CF955
        EEDB7D9C F5254DFD 99CF5B8C 39CABACE D2F3DD2A 53E8DEEA

KeyData is
                        979CA810 0BCF89EC 6DC9DA5F 62729DFA
        068AED5D 2BB085A4 B046D5EC 89CFE0DC CFC5D126 0B1CF955
        EEDB7D9C F5254DFD 99CF5B8C 39CABACE D2F3DD2A 53E8DEEA

Scheme Initiator, Key Confirmation Provider: U to V
NonceV is
                                            19B7D0AA 84E65DDA
        DEC2401C B8035C91 D15F2EA7 7E39B4A4 39FE0E6C 7B22BFC6

Z is
                        51DC2E96 72AA6621 4D32485E 17344B26
        5C622A7F 2B7F2B8A E1B2EEA5 091C4DCC 0E3A7A7F B1610014
        12BC7FB7 E923ABE0 CE876543 C6AF4A15 7ACB4E5F 3041B2EB
        9CE411F5 A8BE3AD4 B1E45BA9 867EE3B9 C117C2F1 A813BD49
        743AF2BE 3BE7093C 1E42D1BE DE2CF8D0 85A2FF6F 1A79DAC2
        F2222D5C 80B26BAE F1153714 A778BA0C 7A4B4CB3 352B4A0A
        D9B78B0E 92B78354 640927FF A3CB433E 3A11A2D8 FB5D2179
        8033530B 95C02F67 B1734AA2 DD8DEEE4 9AEC1332 DFBF62A9
        717C3F8F 1410D0EE A86D5CC7 2729BE13 33709895 06E9F228
        75D593F3 9CB65C91 D7987A6E EECAFC18 C10AE7D1 93E54445
        E41D0959 65705737 38A31262 40E75989 5681AD0C 86EA8364

OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536

KDFval is
                                            979CA810 0BCF89EC
        6DC9DA5F 62729DFA 068AED5D 2BB085A4 B046D5EC 89CFE0DC
        CFC5D126 0B1CF955 EEDB7D9C F5254DFD 99CF5B8C 39CABACE
        D2F3DD2A 53E8DEEA 7EEE7CF9 7B9B0511 3CF4B6D2 27B9D681

MacData is
                        4B435F31 5F55414C 49434542 4F424259
        58EA5EA6 75A27704 2C2E842C 05061136 B6B53163 20233F49
        D5338C38 48C71852 738F6E1E 39371F50 C84A7910 2C76DA3B
        C1BFD15C 83CAA8D2 378D9C32 8C6E5CB0 8F669763 6BB13CC7
        77A38855 9237858F 05606E0A 8014194E 9487DB1F F14E9903
        E84EAB89 13EC38BC 439F2F38 5F2D1E34 DB4A538C AA6161BF
        552AD467 62C4C404 75880763 D69AFA49 34DBEBD0 EB5388F4
        CA3FE8FD B08948B3 1CDC1A5B 7814BD34 5C0F0EFD E4418C1A
        F6197C7E 8A02B3DB 78C28F67 EAF85130 F5E04A65 5AFC1673
        29E13B3E 709B6255 97DE7A65 B15EB7A4 92154007 7CD43D24
        5C060D5C 14F98AFE EC9B039B E1460A59 4A46CD16 7DA70237
        27259822 91932C86 947B4D53 8B4B180D 19B7D0AA 84E65DDA
        DEC2401C B8035C91 D15F2EA7 7E39B4A4 39FE0E6C 7B22BFC6

MacKey is
                        979CA810 0BCF89EC 6DC9DA5F 62729DFA

Mtag is
                        BB5A371C 1AE76B0E E752822A 51D203FD

KeyData is
                        068AED5D 2BB085A4 B046D5EC 89CFE0DC
        CFC5D126 0B1CF955 EEDB7D9C F5254DFD 99CF5B8C 39CABACE
        D2F3DD2A 53E8DEEA 7EEE7CF9 7B9B0511 3CF4B6D2 27B9D681

Scheme Responder, Key Confirmation Provider: V to U
NonceU is
                                            19B7D0AA 84E65DDA
        DEC2401C B8035C91 D15F2EA7 7E39B4A4 39FE0E6C 7B22BFC6

Z is
                        51DC2E96 72AA6621 4D32485E 17344B26
        5C622A7F 2B7F2B8A E1B2EEA5 091C4DCC 0E3A7A7F B1610014
        12BC7FB7 E923ABE0 CE876543 C6AF4A15 7ACB4E5F 3041B2EB
        9CE411F5 A8BE3AD4 B1E45BA9 867EE3B9 C117C2F1 A813BD49

743AF2BE 3BE7093C 1E42D1BE DE2CF8D0 85A2FF6F 1A79DAC2
F2222D5C 80B26BAE F1153714 A778BA0C 7A4B4CB3 352B4A0A
D9B78B0E 92B78354 640927FF A3CB433E 3A11A2D8 FB5D2179
8033530B 95C02F67 B1734AA2 DD8DEEE4 9AEC1332 DFBF62A9
717C3F8F 1410D0EE A86D5CC7 2729BE13 33709895 06E9F228
75D593F3 9CB65C91 D7987A6E EECAFC18 C10AE7D1 93E54445
E41D0959 65705737 38A31262 40E75989 5681AD0C 86EA8364

OtherInfo is
12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536

KDFval is
979CA810 0BCF89EC
6DC9DA5F 62729DFA 068AED5D 2BB085A4 B046D5EC 89CFE0DC
CFC5D126 0B1CF955 EEDB7D9C F5254DFD 99CF5B8C 39CABACE
D2F3DD2A 53E8DEEA 7EEE7CF9 7B9B0511 3CF4B6D2 27B9D681

MacData is
4B435F31 5F56424F
42425941 4C494345 58EA5EA6 75A27704 2C2E842C 05061136
B6B53163 20233F49 D5338C38 48C71852 738F6E1E 39371F50
C84A7910 2C76DA3B C1BFD15C 83CAA8D2 378D9C32 8C6E5CB0
8F669763 6BB13CC7 77A38855 9237858F 05606E0A 8014194E
9487DB1F F14E9903 E84EAB89 13EC38BC 439F2F38 5F2D1E34
DB4A538C AA6161BF 552AD467 62C4C404 75880763 D69AFA49
34DBEBD0 EB5388F4 CA3FE8FD B08948B3 1CDC1A5B 7814BD34
5C0F0EFD E4418C1A F6197C7E 8A02B3DB 78C28F67 EAF85130
F5E04A65 5AFC1673 29E13B3E 709B6255 97DE7A65 B15EB7A4
92154007 7CD43D24 5C060D5C 14F98AFE EC9B039B E1460A59
4A46CD16 7DA70237 27259822 91932C86 947B4D53 8B4B180D

MacKey is
979CA810 0BCF89EC 6DC9DA5F 62729DFA

Mtag is
EA86BE00 C8783454 FE3BB6FF B42CA0FF

KeyData is
068AED5D 2BB085A4 B046D5EC 89CFE0DC
CFC5D126 0B1CF955 EEDB7D9C F5254DFD 99CF5B8C 39CABACE

D2F3DD2A 53E8DEEA 7EEE7CF9 7B9B0511 3CF4B6D2 27B9D681

Scheme Initiator, Key Confirmation Bilateral
NonceV is
19B7D0AA 84E65DDA
DEC2401C B8035C91 D15F2EA7 7E39B4A4 39FE0E6C 7B22BFC6

Z is
51DC2E96 72AA6621 4D32485E 17344B26
5C622A7F 2B7F2B8A E1B2EEA5 091C4DCC 0E3A7A7F B1610014
12BC7FB7 E923ABE0 CE876543 C6AF4A15 7ACB4E5F 3041B2EB
9CE411F5 A8BE3AD4 B1E45BA9 867EE3B9 C117C2F1 A813BD49
743AF2BE 3BE7093C 1E42D1BE DE2CF8D0 85A2FF6F 1A79DAC2
F2222D5C 80B26BAE F1153714 A778BA0C 7A4B4CB3 352B4A0A
D9B78B0E 92B78354 640927FF A3CB433E 3A11A2D8 FB5D2179
8033530B 95C02F67 B1734AA2 DD8DEEE4 9AEC1332 DFBF62A9
717C3F8F 1410D0EE A86D5CC7 2729BE13 33709895 06E9F228
75D593F3 9CB65C91 D7987A6E EECAFC18 C10AE7D1 93E54445
E41D0959 65705737 38A31262 40E75989 5681AD0C 86EA8364

OtherInfo is
12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536

KDFval is
979CA810 0BCF89EC
6DC9DA5F 62729DFA 068AED5D 2BB085A4 B046D5EC 89CFE0DC
CFC5D126 0B1CF955 EEDB7D9C F5254DFD 99CF5B8C 39CABACE
D2F3DD2A 53E8DEEA 7EEE7CF9 7B9B0511 3CF4B6D2 27B9D681

U2V

MacData is
4B435F32 5F55414C 49434542 4F424259
58EA5EA6 75A27704 2C2E842C 05061136 B6B53163 20233F49
D5338C38 48C71852 738F6E1E 39371F50 C84A7910 2C76DA3B
C1BFD15C 83CAA8D2 378D9C32 8C6E5CB0 8F669763 6BB13CC7
77A38855 9237858F 05606E0A 8014194E 9487DB1F F14E9903
E84EAB89 13EC38BC 439F2F38 5F2D1E34 DB4A538C AA6161BF

552AD467 62C4C404 75880763 D69AFA49 34DBEBD0 EB5388F4
CA3FE8FD B08948B3 1CDC1A5B 7814BD34 5C0F0EFD E4418C1A
F6197C7E 8A02B3DB 78C28F67 EAF85130 F5E04A65 5AFC1673
29E13B3E 709B6255 97DE7A65 B15EB7A4 92154007 7CD43D24
5C060D5C 14F98AFE EC9B039B E1460A59 4A46CD16 7DA70237
27259822 91932C86 947B4D53 8B4B180D 19B7D0AA 84E65DDA
DEC2401C B8035C91 D15F2EA7 7E39B4A4 39FE0E6C 7B22BFC6

MacKey is
979CA810 0BCF89EC 6DC9DA5F 62729DFA

Mtag is
BDC52F83 335115A8 F882B1F2 6909E62C

V2U

MacData is
4B435F32 5F56424F 42425941 4C494345
19B7D0AA 84E65DDA DEC2401C B8035C91 D15F2EA7 7E39B4A4
39FE0E6C 7B22BFC6 58EA5EA6 75A27704 2C2E842C 05061136
B6B53163 20233F49 D5338C38 48C71852 738F6E1E 39371F50
C84A7910 2C76DA3B C1BFD15C 83CAA8D2 378D9C32 8C6E5CB0
8F669763 6BB13CC7 77A38855 9237858F 05606E0A 8014194E
9487DB1F F14E9903 E84EAB89 13EC38BC 439F2F38 5F2D1E34
DB4A538C AA6161BF 552AD467 62C4C404 75880763 D69AFA49
34DBEBD0 EB5388F4 CA3FE8FD B08948B3 1CDC1A5B 7814BD34
5C0F0EFD E4418C1A F6197C7E 8A02B3DB 78C28F67 EAF85130
F5E04A65 5AFC1673 29E13B3E 709B6255 97DE7A65 B15EB7A4
92154007 7CD43D24 5C060D5C 14F98AFE EC9B039B E1460A59
4A46CD16 7DA70237 27259822 91932C86 947B4D53 8B4B180D

MacKey is
979CA810 0BCF89EC 6DC9DA5F 62729DFA

Mtag is
6106CBC5 730CF460 F9626599 61F9C07B

KeyData is
068AED5D 2BB085A4 B046D5EC 89CFE0DC
CFC5D126 0B1CF955 EEDB7D9C F5254DFD 99CF5B8C 39CABACE

```
        D2F3DD2A 53E8DEEA 7EEE7CF9 7B9B0511 3CF4B6D2 27B9D681


================================================================


dhOneFlow(256)
----------------------------------------------------------
xV is
                                                3D37042D FD8441A4
        3D5A4EA9 3A4DBEEC 0D71E3B5 3719CC52 F894C3D5 3A830B3A


yV is
                        15C08EFE 47F2418B 1275137F BC028A9E
        62016029 DF8444F1 4327E37E D68FAECA 11400570 B914D149
        AC076F29 C6ED1E3F E0A96EBF 973378F6 0590858F EAF85A3C
        CF9265D2 37B93697 95BB5A2F 88876EC3 82BF68DE 3A0C252A
        0518BAED 9707088F E87CC2DC 399CA046 EAE4015C 5D4D2851
        1509C43A 8D1F04C9 6C714ABF 27B5B6C8 7C2227FF F021C7CF
        82216668 49020644 E3C6E905 A115242A D01B9428 021EB450
        501C64BB 8FF095EE 61B2FAEF 5F20F169 28FCDF46 1F65B5DE
        783C2A4D 0DD5A9BA 7602DBB6 90184267 586B1222 68167AC5
        064478AE 0204B17E B8E59B5E 4475767C 695FAE00 78360263
        E7220FE7 ECE8BB91 3ED0AB88 197C5FCF 06513975 5097542C


rU is
                                                04B7AF95 7BF80E5E
        93CE6EAE 1E67165D C04E4391 A61A56C5 A5E02E10 AB4E6939


tU is
                        6A99740F E11FF1E3 DFCEB45C 8C5124C2
        8C1715E1 D35194EB 2531E781 C25C13E0 97A36400 84DD83CB
        889ECD7D 8FCA033E A1C8C265 A3981E0E 7F186E92 0CC18622
        BE0F74DE 2621108B 4074EADF 75D7D8FF DC431C27 2EF7FFBC
        8D7AB16C 75EBD292 3060930B 2E59D80C 01FAC985 9E34915E
        A122642E CE081F29 D6715B25 2B16E884 BE75589C B9A2111C
        3443199A 238018D9 BF4BA49D 9ADAF3FF 60BBC5EB B4A9F7AE
        E2823CB0 F195148D 307F893C 954A0DE3 6E9CFA1A FF6B02F4
        87DC5A99 978362FD AF65F4CD 86BFE9CA 32CB7A5F 48DFC235
        8087F7CD 858AE877 A97D7408 15F830FD C32D8CFD E09831BB
        686F02A0 5F2C0F16 939D4758 8742EA8A C04C960D 1393C1CE
```

```
------------------------------------------------------------
no Key Confirmation
Z is
                          2CCCF4BF A6286776 0C662AA3 59D9822E
        48F4431A 60C42451 EB4F7568 F737A880 B36C6186 B431F8E7
        91693C1A DD39A06E 38A4C28A 455F0A31 80D5368F 401FDC6F
        86FB72F6 A293EEB0 0F9A81D1 ACF202C7 38AF497F BAD8AB4C
        A691C3FA 3F004BE8 C07F6140 90858BD4 74E0B2CF 4029EF6B
        3E332E1E 619827D9 049A9A0C 232A92F0 3BAE0880 F868BB0A
        38B3D9CD 42D70B14 30645534 D251C2C5 3FAD8CD9 88CD3C6E
        8D736CA0 37A7F58E 1DE1C74A B184D37D B8CF82B9 A5355706
        0C05D3D6 9B5A048A 5D4212C4 DD67669B 6CE480C4 3293ADDB
        5E576F5C A9E99BB0 8DFB5532 807D77A1 4A9B1D5D 93D9F409
        33092D1F D5D18726 20D8D453 FD8E76CA 01DEEF38 F8F60245


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


KDFval is
                          4EE8467B 0AE068F6 C1848CCE 805A8222
        A1DAF8AE 88B54777 51A7A625 8BAA19B9 29DE8380 C694F277
        9CDD3DC3 64D79845 F75B3B18 18459649 617986C2 B6F0967E


KeyData is
                          4EE8467B 0AE068F6 C1848CCE 805A8222
        A1DAF8AE 88B54777 51A7A625 8BAA19B9 29DE8380 C694F277
        9CDD3DC3 64D79845 F75B3B18 18459649 617986C2 B6F0967E




------------------------------------------------------------
Scheme Responder, Key Confirmation Provider: V to U
Z is
                          2CCCF4BF A6286776 0C662AA3 59D9822E
        48F4431A 60C42451 EB4F7568 F737A880 B36C6186 B431F8E7
        91693C1A DD39A06E 38A4C28A 455F0A31 80D5368F 401FDC6F
        86FB72F6 A293EEB0 0F9A81D1 ACF202C7 38AF497F BAD8AB4C
        A691C3FA 3F004BE8 C07F6140 90858BD4 74E0B2CF 4029EF6B
        3E332E1E 619827D9 049A9A0C 232A92F0 3BAE0880 F868BB0A
        38B3D9CD 42D70B14 30645534 D251C2C5 3FAD8CD9 88CD3C6E
```

```
        8D736CA0 37A7F58E 1DE1C74A B184D37D B8CF82B9 A5355706
        0C05D3D6 9B5A048A 5D4212C4 DD67669B 6CE480C4 3293ADDB
        5E576F5C A9E99BB0 8DFB5532 807D77A1 4A9B1D5D 93D9F409
        33092D1F D5D18726 20D8D453 FD8E76CA 01DEEF38 F8F60245


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


KDFval is
                                            4EE8467B 0AE068F6
        C1848CCE 805A8222 A1DAF8AE 88B54777 51A7A625 8BAA19B9
        29DE8380 C694F277 9CDD3DC3 64D79845 F75B3B18 18459649
        617986C2 B6F0967E BBA3533D 06752A1F 625607E1 B60448A9


MacData is
                                            4B435F31 5F56424F
        42425941 4C494345 6A99740F E11FF1E3 DFCEB45C 8C5124C2
        8C1715E1 D35194EB 2531E781 C25C13E0 97A36400 84DD83CB
        889ECD7D 8FCA033E A1C8C265 A3981E0E 7F186E92 0CC18622
        BE0F74DE 2621108B 4074EADF 75D7D8FF DC431C27 2EF7FFBC
        8D7AB16C 75EBD292 3060930B 2E59D80C 01FAC985 9E34915E
        A122642E CE081F29 D6715B25 2B16E884 BE75589C B9A2111C
        3443199A 238018D9 BF4BA49D 9ADAF3FF 60BBC5EB B4A9F7AE
        E2823CB0 F195148D 307F893C 954A0DE3 6E9CFA1A FF6B02F4
        87DC5A99 978362FD AF65F4CD 86BFE9CA 32CB7A5F 48DFC235
        8087F7CD 858AE877 A97D7408 15F830FD C32D8CFD E09831BB
        686F02A0 5F2C0F16 939D4758 8742EA8A C04C960D 1393C1CE


MacKey is
                        4EE8467B 0AE068F6 C1848CCE 805A8222


Mtag is
                        0FC1F505 73B09265 D719CAAE 42EE2151


KeyData is
                        A1DAF8AE 88B54777 51A7A625 8BAA19B9
        29DE8380 C694F277 9CDD3DC3 64D79845 F75B3B18 18459649
        617986C2 B6F0967E BBA3533D 06752A1F 625607E1 B60448A9
```

==========

dhStatic(256)
---
xU is
                                                484850F2 2E54702A
        97F54702 46F9AF25 3BEE47ED A5B9A713 6F43F834 E3F4AA4C

yU is
                         120CE9E1 C7F69749 26B5D2FC 157022D8
        CDDD23B1 048E98F9 34B39D2D EB6BABEE 454F358C 1D54FB41
        72267273 9AB2541C 9DDD53B7 8299AC32 90F5DC68 49ADF3F3
        C7F99076 E53F9CE5 49C8687A BDB4DD1E E9FF36C4 A3A2942A
        F516A104 4F833CAC 466E388E 6C8BCB83 4CAB0AF8 CD5B99B9
        06A720AA BA969293 2DC77995 926D9B91 05B45809 6E8907B8
        22DF0BB9 B3DEAF2E ABE20C17 6BDFF0B5 A0085DEA 2109294A
        787A6FDC 177AFB88 F43D6697 E8A2CC68 DFE6D8E4 7FB4F3C2
        7DF7C53A 8784FEC8 8E31D36C 54BF614F 628C36EE FC74B2D9
        420DCD31 0DE19536 9D9D3AE4 F61C026E 1239876A 2C207B47
        5FD7149B 354E2D34 308A5767 847495F1 939B8EDD 4C23BCC7

xV is
                                                4105E2A1 14F13D63
        42CD1382 095AAAF7 1CAAB3C3 0BB7BDEB 77E138B9 BB837E9F

yV is
                         135C398E 5E9F767C 7C95B7E0 C6FB172A
        D45D805E 3BC2E6C3 80A41CF2 46927EF8 10B21797 7A18B387
        F6698677 97EB7047 19D998AA EA4F21D1 B4E24DBC 0E242FC0
        5540CB76 0FBB6A8C CFAF008E 0A664706 8FAA0B77 0CEF04A2
        5A230393 131FCD77 8ACD2EB6 B11B026A 8D49C11D F80BA6B7
        C088CFA3 38BE53B5 D936C679 C894C55D 9B219FC6 12079FA3
        56B4888D 92E54C39 A3582308 D596C9EF EBF76731 BE5FACC9
        FC7C2F05 1624733F C3AF7175 7D3CB16D B49D8044 061AC2A9
        A1EDE377 33FD4ED3 1F2179A3 142FA8FE 8FCA3786 664D476D
        DB5B3A69 B1AE229D 6F0F5487 3C4B862C 0497284F 1A8ED3C0
        247E2737 6E2FC936 03743B0F 37C3FFC9 3D01B05B ECCDECC4

```
no Key Confirmation
NonceU is
                                                  021DDABB 1C8326DA
        EACC8E35 7607DECB 56DC8640 30BBEA24 94352DEB 6791F02F


Z is
                         40B63CDD B7129BE7 AD46DF54 FC20474C
        94B78D2D 9A2B13D6 CA8C431D 16752E90 59B41E22 FD2F7678
        13FB572A AAEFFE72 A588F710 58C59EF9 1DE12450 F3CCD515
        45E76401 09AD05AC 9CAC9FC1 AB8FBCF3 13E73AED A41C8FF9
        22640604 68FAA6E2 AB9F8683 D6838F67 9C9D76EF 42CE37BC
        DE5D0C09 2139782D 019659EF 938ABE10 9795BFDD B0043312
        5DAF3F6B BE888251 B3F0A154 1BB59581 3B852451 FDB2F7AB
        2974C5E1 429D2CAB 19EAD1D0 99CD3CDE 9322B6B1 72058E6D
        F901D97B 71875AE3 D367BC72 501DB04D ED6E7208 7EBB7837
        D6FBB222 97883F6D 3662331B 49A49F72 7B2BF08F 3FAE3BC6
        EFBE81E3 8101B09B 9AA86090 41AA1669 0718316F 0220F07F


OtherInfo is
                                       1234 56789ABC DEF0414C
        49434531 32330020 021DDABB 1C8326DA EACC8E35 7607DECB
        56DC8640 30BBEA24 94352DEB 6791F02F 424F4242 59343536


KDFval is
                         0D2C9360 4243E8B6 D8087A8F BC8E8BC7
        E362047F 47056583 95D7FAE5 8E33D7A8 E10039E3 0730EA8E
        BA5F43F6 B4B9D239 8587E77A 58505925 0D2A6ED8 4F18C2DD


KeyData is
                         0D2C9360 4243E8B6 D8087A8F BC8E8BC7
        E362047F 47056583 95D7FAE5 8E33D7A8 E10039E3 0730EA8E
        BA5F43F6 B4B9D239 8587E77A 58505925 0D2A6ED8 4F18C2DD




------------------------------------------------------------
Scheme Initiator, Key Confirmation Provider: U to V
NonceU is
                                                  021DDABB 1C8326DA
        EACC8E35 7607DECB 56DC8640 30BBEA24 94352DEB 6791F02F
```

NonceV is
                                        10033DD1 41ED4A76
        F3D0D3E5 2983222B 2AD10743 AD163E5C 007F3EF3 B9891062

Z is
                        40B63CDD B7129BE7 AD46DF54 FC20474C
        94B78D2D 9A2B13D6 CA8C431D 16752E90 59B41E22 FD2F7678
        13FB572A AAEFFE72 A588F710 58C59EF9 1DE12450 F3CCD515
        45E76401 09AD05AC 9CAC9FC1 AB8FBCF3 13E73AED A41C8FF9
        22640604 68FAA6E2 AB9F8683 D6838F67 9C9D76EF 42CE37BC
        DE5D0C09 2139782D 019659EF 938ABE10 9795BFDD B0043312
        5DAF3F6B BE888251 B3F0A154 1BB59581 3B852451 FDB2F7AB
        2974C5E1 429D2CAB 19EAD1D0 99CD3CDE 9322B6B1 72058E6D
        F901D97B 71875AE3 D367BC72 501DB04D ED6E7208 7EBB7837
        D6FBB222 97883F6D 3662331B 49A49F72 7B2BF08F 3FAE3BC6
        EFBE81E3 8101B09B 9AA86090 41AA1669 0718316F 0220F07F

OtherInfo is
                                    1234 56789ABC DEF0414C
        49434531 32330020 021DDABB 1C8326DA EACC8E35 7607DECB
        56DC8640 30BBEA24 94352DEB 6791F02F 424F4242 59343536

KDFval is
                                        0D2C9360 4243E8B6
        D8087A8F BC8E8BC7 E362047F 47056583 95D7FAE5 8E33D7A8
        E10039E3 0730EA8E BA5F43F6 B4B9D239 8587E77A 58505925
        0D2A6ED8 4F18C2DD 48425B69 81A348E1 9FC4116D 39ABFAB4

MacData is
                                        4B435F31 5F55414C
        49434542 4F424259 021DDABB 1C8326DA EACC8E35 7607DECB
        56DC8640 30BBEA24 94352DEB 6791F02F 10033DD1 41ED4A76
        F3D0D3E5 2983222B 2AD10743 AD163E5C 007F3EF3 B9891062

MacKey is
                        0D2C9360 4243E8B6 D8087A8F BC8E8BC7

Mtag is
                        FB913109 BF588555 B2DE5B08 06B0CDA0

KeyData is
                        E362047F 47056583 95D7FAE5 8E33D7A8
        E10039E3 0730EA8E BA5F43F6 B4B9D239 8587E77A 58505925
        0D2A6ED8 4F18C2DD 48425B69 81A348E1 9FC4116D 39ABFAB4

Scheme Responder, Key Confirmation Provider: V to U
NonceV is
                                            10033DD1 41ED4A76
        F3D0D3E5 2983222B 2AD10743 AD163E5C 007F3EF3 B9891062

NonceU is
                                            021DDABB 1C8326DA
        EACC8E35 7607DECB 56DC8640 30BBEA24 94352DEB 6791F02F

Z is
                        40B63CDD B7129BE7 AD46DF54 FC20474C
        94B78D2D 9A2B13D6 CA8C431D 16752E90 59B41E22 FD2F7678
        13FB572A AAEFFE72 A588F710 58C59EF9 1DE12450 F3CCD515
        45E76401 09AD05AC 9CAC9FC1 AB8FBCF3 13E73AED A41C8FF9
        22640604 68FAA6E2 AB9F8683 D6838F67 9C9D76EF 42CE37BC
        DE5D0C09 2139782D 019659EF 938ABE10 9795BFDD B0043312
        5DAF3F6B BE888251 B3F0A154 1BB59581 3B852451 FDB2F7AB
        2974C5E1 429D2CAB 19EAD1D0 99CD3CDE 9322B6B1 72058E6D
        F901D97B 71875AE3 D367BC72 501DB04D ED6E7208 7EBB7837
        D6FBB222 97883F6D 3662331B 49A49F72 7B2BF08F 3FAE3BC6
        EFBE81E3 8101B09B 9AA86090 41AA1669 0718316F 0220F07F

OtherInfo is
                                       1234 56789ABC DEF0414C
        49434531 32330020 021DDABB 1C8326DA EACC8E35 7607DECB
        56DC8640 30BBEA24 94352DEB 6791F02F 424F4242 59343536

KDFval is
                                            0D2C9360 4243E8B6
        D8087A8F BC8E8BC7 E362047F 47056583 95D7FAE5 8E33D7A8
        E10039E3 0730EA8E BA5F43F6 B4B9D239 8587E77A 58505925

```
        0D2A6ED8 4F18C2DD 48425B69 81A348E1 9FC4116D 39ABFAB4


MacData is
        4B435F31 5F56424F 42425941 4C494345 021DDABB 1C8326DA
        EACC8E35 7607DECB 56DC8640 30BBEA24 94352DEB 6791F02F


MacKey is
                         0D2C9360 4243E8B6 D8087A8F BC8E8BC7


Mtag is
                         47929517 E24E9C31 386C3A40 C435B2DB


KeyData is
                         E362047F 47056583 95D7FAE5 8E33D7A8
        E10039E3 0730EA8E BA5F43F6 B4B9D239 8587E77A 58505925
        0D2A6ED8 4F18C2DD 48425B69 81A348E1 9FC4116D 39ABFAB4




------------------------------------------------------------
Scheme Initiator, Key Confirmation Bilateral
NonceU is
                                           021DDABB 1C8326DA
        EACC8E35 7607DECB 56DC8640 30BBEA24 94352DEB 6791F02F


NonceV is
                                           10033DD1 41ED4A76
        F3D0D3E5 2983222B 2AD10743 AD163E5C 007F3EF3 B9891062


Z is
                         40B63CDD B7129BE7 AD46DF54 FC20474C
        94B78D2D 9A2B13D6 CA8C431D 16752E90 59B41E22 FD2F7678
        13FB572A AAEFFE72 A588F710 58C59EF9 1DE12450 F3CCD515
        45E76401 09AD05AC 9CAC9FC1 AB8FBCF3 13E73AED A41C8FF9
        22640604 68FAA6E2 AB9F8683 D6838F67 9C9D76EF 42CE37BC
        DE5D0C09 2139782D 019659EF 938ABE10 9795BFDD B0043312
        5DAF3F6B BE888251 B3F0A154 1BB59581 3B852451 FDB2F7AB
        2974C5E1 429D2CAB 19EAD1D0 99CD3CDE 9322B6B1 72058E6D
        F901D97B 71875AE3 D367BC72 501DB04D ED6E7208 7EBB7837
```

```
        D6FBB222 97883F6D 3662331B 49A49F72 7B2BF08F 3FAE3BC6
        EFBE81E3 8101B09B 9AA86090 41AA1669 0718316F 0220F07F


OtherInfo is
                                        1234 56789ABC DEF0414C
        49434531 32330020 021DDABB 1C8326DA EACC8E35 7607DECB
        56DC8640 30BBEA24 94352DEB 6791F02F 424F4242 59343536


KDFval is
                                             0D2C9360 4243E8B6
        D8087A8F BC8E8BC7 E362047F 47056583 95D7FAE5 8E33D7A8
        E10039E3 0730EA8E BA5F43F6 B4B9D239 8587E77A 58505925
        0D2A6ED8 4F18C2DD 48425B69 81A348E1 9FC4116D 39ABFAB4


U2V
----------------
MacData is
                                             4B435F32 5F55414C
        49434542 4F424259 021DDABB 1C8326DA EACC8E35 7607DECB
        56DC8640 30BBEA24 94352DEB 6791F02F 10033DD1 41ED4A76
        F3D0D3E5 2983222B 2AD10743 AD163E5C 007F3EF3 B9891062


MacKey is
                          0D2C9360 4243E8B6 D8087A8F BC8E8BC7


Mtag is
                          76D1CC43 32FFEA0B 69AE3F96 305AD064


V2U
----------------
MacData is
                                             4B435F32 5F56424F
        42425941 4C494345 10033DD1 41ED4A76 F3D0D3E5 2983222B
        2AD10743 AD163E5C 007F3EF3 B9891062 021DDABB 1C8326DA
        EACC8E35 7607DECB 56DC8640 30BBEA24 94352DEB 6791F02F


MacKey is
                          0D2C9360 4243E8B6 D8087A8F BC8E8BC7
```

Mtag is

361303C6 316FB7C2 EE7D6403 F5FB02AD

KeyData is

E362047F 47056583 95D7FAE5 8E33D7A8
E10039E3 0730EA8E BA5F43F6 B4B9D239 8587E77A 58505925
0D2A6ED8 4F18C2DD 48425B69 81A348E1 9FC4116D 39ABFAB4