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

  Keyed-Hash Message Authentication Code (HMAC)

    Hashlen = 512

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

Key length = 128

Tag length = 64

Input Date:
        "Sample message for keylen=blocklen"

Text is
                                        5361 6D706C65 206D6573
        73616765 20666F72 206B6579 6C656E3D 626C6F63 6B6C656E


Key is
                                                00010203 04050607
        08090A0B 0C0D0E0F 10111213 14151617 18191A1B 1C1D1E1F
        20212223 24252627 28292A2B 2C2D2E2F 30313233 34353637
        38393A3B 3C3D3E3F 40414243 44454647 48494A4B 4C4D4E4F
        50515253 54555657 58595A5B 5C5D5E5F 60616263 64656667
        68696A6B 6C6D6E6F 70717273 74757677 78797A7B 7C7D7E7F


----------------------------------------------------------------
K0 is
                                                00010203 04050607
        08090A0B 0C0D0E0F 10111213 14151617 18191A1B 1C1D1E1F
        20212223 24252627 28292A2B 2C2D2E2F 30313233 34353637
        38393A3B 3C3D3E3F 40414243 44454647 48494A4B 4C4D4E4F
        50515253 54555657 58595A5B 5C5D5E5F 60616263 64656667
        68696A6B 6C6D6E6F 70717273 74757677 78797A7B 7C7D7E7F


K0^ipad is
                                                36373435 32333031
        3E3F3C3D 3A3B3839 26272425 22232021 2E2F2C2D 2A2B2829
        16171415 12131011 1E1F1C1D 1A1B1819 06070405 02030001
        0E0F0C0D 0A0B0809 76777475 72737071 7E7F7C7D 7A7B7879
        66676465 62636061 6E6F6C6D 6A6B6869 56575455 52535051
        5E5F5C5D 5A5B5859 46474445 42434041 4E4F4C4D 4A4B4849
```

```
Hash((Key^ipad)||text) is
                          515C86E0 DD382747 A20BDD27 05AF56C1
        AB87AA1D A14F3EFD D99A5935 08EC520D 60C10643 A3841B1E
        CA7EEFF9 559F5D00 78F93479 58FCA632 1E58769D 15CF3A15


K0 xor opad is
                                             5C5D5E5F 58595A5B
        54555657 50515253 4C4D4E4F 48494A4B 44454647 40414243
        7C7D7E7F 78797A7B 74757677 70717273 6C6D6E6F 68696A6B
        64656667 60616263 1C1D1E1F 18191A1B 14151617 10111213
        0C0D0E0F 08090A0B 04050607 00010203 3C3D3E3F 38393A3B
        34353637 30313233 2C2D2E2F 28292A2B 24252627 20212223


Hash((K0^opad)||Hash((K0^ipad)||text)) is
                          FC25E240 658CA785 B7A811A8 D3F7B4CA
        48CFA26A 8A366BF2 CD1F836B 05FCB024 BD368530 81811D6C
        EA4216EB AD79DA1C FCB95EA4 586B8A0C E356596A 55FB1347


-----------------------------------------------------------------
mac is
                          FC25E240 658CA785 B7A811A8 D3F7B4CA
        48CFA26A 8A366BF2 CD1F836B 05FCB024 BD368530 81811D6C
        EA4216EB AD79DA1C FCB95EA4 586B8A0C E356596A 55FB1347


=================================================================
Key length = 64

Tag length = 64

Input Date:
        "Sample message for keylen<blocklen"

Text is
                                       5361 6D706C65 206D6573
        73616765 20666F72 206B6579 6C656E3C 626C6F63 6B6C656E


Key is
                          00010203 04050607 08090A0B 0C0D0E0F
        10111213 14151617 18191A1B 1C1D1E1F 20212223 24252627
```

```
        28292A2B 2C2D2E2F 30313233 34353637 38393A3B 3C3D3E3F


-----------------------------------------------------------
K0 is
                                            00010203 04050607
        08090A0B 0C0D0E0F 10111213 14151617 18191A1B 1C1D1E1F
        20212223 24252627 28292A2B 2C2D2E2F 30313233 34353637
        38393A3B 3C3D3E3F 00000000 00000000 00000000 00000000
        00000000 00000000 00000000 00000000 00000000 00000000
        00000000 00000000 00000000 00000000 00000000 00000000


K0^ipad is
                                            36373435 32333031
        3E3F3C3D 3A3B3839 26272425 22232021 2E2F2C2D 2A2B2829
        16171415 12131011 1E1F1C1D 1A1B1819 06070405 02030001
        0E0F0C0D 0A0B0809 36363636 36363636 36363636 36363636
        36363636 36363636 36363636 36363636 36363636 36363636
        36363636 36363636 36363636 36363636 36363636 36363636


Hash((Key^ipad)||text) is
                        DDCB7529 40EDC533 D61AD7A9 0F907AED
        49827F68 FD6514DA 45688AAA 083E03E3 C961D63E 7BAC1B23
        1EA3F78D 63C5A97B 96156202 6C895EF0 51C0F750 679591A9


K0 xor opad is
                                            5C5D5E5F 58595A5B
        54555657 50515253 4C4D4E4F 48494A4B 44454647 40414243
        7C7D7E7F 78797A7B 74757677 70717273 6C6D6E6F 68696A6B
        64656667 60616263 5C5C5C5C 5C5C5C5C 5C5C5C5C 5C5C5C5C
        5C5C5C5C 5C5C5C5C 5C5C5C5C 5C5C5C5C 5C5C5C5C 5C5C5C5C
        5C5C5C5C 5C5C5C5C 5C5C5C5C 5C5C5C5C 5C5C5C5C 5C5C5C5C


Hash((K0^opad)||Hash((K0^ipad)||text)) is
                        FD44C18B DA0BB0A6 CE0E82B0 31BF2818
        F6539BD5 6EC00BDC 10A8A2D7 30B3634D E2545D63 9B0F2CF7
        10D0692C 72A1896F 1F211C2B 922D1A96 C392E07E 7EA9FEDC


-----------------------------------------------------------
mac is
                        FD44C18B DA0BB0A6 CE0E82B0 31BF2818
```

F6539BD5 6EC00BDC 10A8A2D7 30B3634D E2545D63 9B0F2CF7
10D0692C 72A1896F 1F211C2B 922D1A96 C392E07E 7EA9FEDC

==========

Key length = 200

Tag length = 64

Input Date:
"Sample message for keylen=blocklen"

Text is
5361 6D706C65 206D6573
73616765 20666F72 206B6579 6C656E3D 626C6F63 6B6C656E

Key is
00010203 04050607
08090A0B 0C0D0E0F 10111213 14151617 18191A1B 1C1D1E1F
20212223 24252627 28292A2B 2C2D2E2F 30313233 34353637
38393A3B 3C3D3E3F 40414243 44454647 48494A4B 4C4D4E4F
50515253 54555657 58595A5B 5C5D5E5F 60616263 64656667
68696A6B 6C6D6E6F 70717273 74757677 78797A7B 7C7D7E7F
80818283 84858687 88898A8B 8C8D8E8F 90919293 94959697
98999A9B 9C9D9E9F A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF
B0B1B2B3 B4B5B6B7 B8B9BABB BCBDBEBF C0C1C2C3 C4C5C6C7

K0 is
986058E9 895E2C2A
B8F9E8CB DF801DB1 2A44842A 56A91D5A 4E87B1FC 98B29372
2C466414 2E42C3C5 51FF8986 46268CD9 2B84ED23 0B8C94BE
D7798D4F 27CD7465 00000000 00000000 00000000 00000000
00000000 00000000 00000000 00000000 00000000 00000000
00000000 00000000 00000000 00000000 00000000 00000000

K0^ipad is
AE566EDF BF681A1C
8ECFDEFD E9B62B87 1C72B21C 609F2B6C 78B187CA AE84A544
1A705222 1874F5F3 67C9BFB0 7010BAEF 1DB2DB15 3DBAA288
E14FBB79 11FB4253 36363636 36363636 36363636 36363636
36363636 36363636 36363636 36363636 36363636 36363636
36363636 36363636 36363636 36363636 36363636 36363636

```
Hash((Key^ipad)||text) is
                          6DF26817 41D1FE25 F78ED617 188F35C4
        142351B8 A07090AE 7FC7E123 1E5F67A0 D1F14F15 436DD01D
        EECC3E4E 59F9B10A 15DBE69A 6EBF5921 A9428A37 0BA2618D


K0 xor opad is
                                                 C43C04B5 D5027076
        E4A5B497 83DC41ED 7618D876 0AF54106 12DBEDA0 C4EECF2E
        701A3848 721E9F99 0DA3D5DA 1A7AD085 77D8B17F 57D0C8E2
        8B25D113 7B912839 5C5C5C5C 5C5C5C5C 5C5C5C5C 5C5C5C5C
        5C5C5C5C 5C5C5C5C 5C5C5C5C 5C5C5C5C 5C5C5C5C 5C5C5C5C
        5C5C5C5C 5C5C5C5C 5C5C5C5C 5C5C5C5C 5C5C5C5C 5C5C5C5C


Hash((K0^opad)||Hash((K0^ipad)||text)) is
                          D93EC8D2 DE1AD2A9 957CB9B8 3F14E76A
        D6B5E0CC E285079A 127D3B14 BCCB7AA7 286D4AC0 D4CE6421
        5F2BC9E6 870B33D9 7438BE4A AA20CDA5 C5A912B4 8B8E27F3


---------------------------------------------------------------
mac is
                          D93EC8D2 DE1AD2A9 957CB9B8 3F14E76A
        D6B5E0CC E285079A 127D3B14 BCCB7AA7 286D4AC0 D4CE6421
        5F2BC9E6 870B33D9 7438BE4A AA20CDA5 C5A912B4 8B8E27F3


===============================================================
Key length = 49

Tag length = 32

Input Date:
        "Sample message for keylen<blocklen, with truncated tag"

Text is
                                                    5361 6D706C65
        206D6573 73616765 20666F72 206B6579 6C656E3C 626C6F63
        6B6C656E 2C207769 74682074 72756E63 61746564 20746167


Key is
                                                               00
```

```
        01020304 05060708 090A0B0C 0D0E0F10 11121314 15161718
        191A1B1C 1D1E1F20 21222324 25262728 292A2B2C 2D2E2F30


-------------------------------------------------------------
K0 is
                                            00010203 04050607
        08090A0B 0C0D0E0F 10111213 14151617 18191A1B 1C1D1E1F
        20212223 24252627 28292A2B 2C2D2E2F 30000000 00000000
        00000000 00000000 00000000 00000000 00000000 00000000
        00000000 00000000 00000000 00000000 00000000 00000000
        00000000 00000000 00000000 00000000 00000000 00000000


K0^ipad is
                                            36373435 32333031
        3E3F3C3D 3A3B3839 26272425 22232021 2E2F2C2D 2A2B2829
        16171415 12131011 1E1F1C1D 1A1B1819 06363636 36363636
        36363636 36363636 36363636 36363636 36363636 36363636
        36363636 36363636 36363636 36363636 36363636 36363636
        36363636 36363636 36363636 36363636 36363636 36363636


Hash((Key^ipad)||text) is
                          0F70BAB7 04356437 72518C8A 803CB42D
        D3CAEB69 F96C6712 FFB4461A 90FF4900 B3BE2863 AABCCD84
        61D7FD95 3452691B 5F7ACAF1 51A6BC38 5DBFDD3D 97B49C20


K0 xor opad is
                                            5C5D5E5F 58595A5B
        54555657 50515253 4C4D4E4F 48494A4B 44454647 40414243
        7C7D7E7F 78797A7B 74757677 70717273 6C5C5C5C 5C5C5C5C
        5C5C5C5C 5C5C5C5C 5C5C5C5C 5C5C5C5C 5C5C5C5C 5C5C5C5C
        5C5C5C5C 5C5C5C5C 5C5C5C5C 5C5C5C5C 5C5C5C5C 5C5C5C5C
        5C5C5C5C 5C5C5C5C 5C5C5C5C 5C5C5C5C 5C5C5C5C 5C5C5C5C


Hash((K0^opad)||Hash((K0^ipad)||text)) is
                          00F3E9A7 7BB0F06D E15F1606 03E42B50
        28758808 596664C0 3E1AB8FB 2B076778 0563AEDC 644960D4
        F0C0C5D2 39F67A2A 61B141E8 C871F3D4 0DB2C605 588DAB92


-------------------------------------------------------------
mac is
```

00F3E9A7 7BB0F06D
E15F1606 03E42B50 28758808 596664C0 3E1AB8FB 2B076778