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

FIPS 186-2 Appendix 3.1

    G(t,c) constructed from SHA-1

    Q =
                B5AFD2F9 3246B1EF CD1F3A7C 240C1E9E 21A3630B


    XKey =
                BD029BBE 7F51960B CF9EDB2B 61F06F0F EB5A38B6


    XSeed =
                00000000 00000000 00000000 00000000 00000000


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

XVal is
                BD029BBE 7F51960B CF9EDB2B 61F06F0F EB5A38B6


  G(t,c) using SHA-1
  --------------------------
    t is
                01234567 89ABCDEF FEDCBA98 76543210 F0E1D2C3


    c is
                BD029BBE 7F51960B CF9EDB2B 61F06F0F EB5A38B6


    G(t,c) is
                2070B322 3DBA372F DE1C0FFC 7B2E3B49 8B260614


  --------------------------
Updated XKey is
                DD734EE0 BD0BCD3B ADBAEB27 DD1EAA59 76803ECB


X is
                2070B322 3DBA372F DE1C0FFC 7B2E3B49 8B260614


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

FIPS 186-2 Appendix 3.1 using Change Notice 1

    G(t,c) constructed from SHA-1

    Q =
```

```
                B5AFD2F9 3246B1EF CD1F3A7C 240C1E9E 21A3630B


    XKey =
                BD029BBE 7F51960B CF9EDB2B 61F06F0F EB5A38B6


    XSeed =
                00000000 00000000 00000000 00000000 00000000

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

  i = 0
  XVal is
                BD029BBE 7F51960B CF9EDB2B 61F06F0F EB5A38B6


  G(t,c) using SHA-1
  --------------------------
    t is
                01234567 89ABCDEF FEDCBA98 76543210 F0E1D2C3


    c is
                BD029BBE 7F51960B CF9EDB2B 61F06F0F EB5A38B6


    G(t,c) is
                2070B322 3DBA372F DE1C0FFC 7B2E3B49 8B260614


  ---------------------------
  w is
                2070B322 3DBA372F DE1C0FFC 7B2E3B49 8B260614


  Updated XKey is
                DD734EE0 BD0BCD3B ADBAEB27 DD1EAA59 76803ECB


  **********************
  i = 1
  XVal is
                DD734EE0 BD0BCD3B ADBAEB27 DD1EAA59 76803ECB


  G(t,c) using SHA-1
  --------------------------
    t is
                01234567 89ABCDEF FEDCBA98 76543210 F0E1D2C3


    c is
```

```
                DD734EE0 BD0BCD3B ADBAEB27 DD1EAA59 76803ECB


    G(t,c) is
                3C6C18BA CB0F6C55 BABB1378 8E20D737 A3275116


  ---------------------------
  w is
                         2070B322 3DBA372F DE1C0FFC 7B2E3B49
        8B260614 3C6C18BA CB0F6C55 BABB1378 8E20D737 A3275116


  Updated XKey is
                19DF679B 881B3991 6875FEA0 6B3F8191 19A78FE2


  **********************
X is
                47C27EB6 16DBA413 91E5165B E9C5E397 7E39A15D


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

FIPS 186-2 Appendix 3.2

    G(t,c) constructed from SHA-1

    Q =
                B5AFD2F9 3246B1EF CD1F3A7C 240C1E9E 21A3630B


    KKey =
                687A66D9 0648F993 867E121F 4DDF9DDB 01205584


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

  G(t,c) using SHA-1
  ---------------------------
    t is
                89ABCDEF FEDCBA98 76543210 F0E1D2C3 01234567


    c is
                687A66D9 0648F993 867E121F 4DDF9DDB 01205584


    G(t,c) is
                FD00CEE3 87E139FD EA1DA3FD 07685FBA B979711E


  ---------------------------
Updated KKey is
```

```
                AFCB62C3 5BE381A1 A37C7BA0 313BDEF7 98F66398


K is
                4750FBEA 559A880E 1CFE6980 E35C411C 97D60E13


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

FIPS 186-2 Appendix 3.2 using Change Notice 1

    G(t,c) constructed from SHA-1

    Q =
                B5AFD2F9 3246B1EF CD1F3A7C 240C1E9E 21A3630B


    KKey =
                687A66D9 0648F993 867E121F 4DDF9DDB 01205584


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

  G(t,c) using SHA-1
  ---------------------------
    t is
                89ABCDEF FEDCBA98 76543210 F0E1D2C3 01234567


    c is
                687A66D9 0648F993 867E121F 4DDF9DDB 01205584


    G(t,c) is
                FD00CEE3 87E139FD EA1DA3FD 07685FBA B979711E


  ---------------------------
  i = 0
  w is
                FD00CEE3 87E139FD EA1DA3FD 07685FBA B979711E


  Updated KKey is
                657B35BC 8E2A3391 709BB61C 5547FD95 BA99C6A3


  G(t,c) using SHA-1
  ---------------------------
    t is
                89ABCDEF FEDCBA98 76543210 F0E1D2C3 01234567


    c is
```

```
                657B35BC 8E2A3391 709BB61C 5547FD95 BA99C6A3


    G(t,c) is
                BFB1C43B A8C9326C 16D8A3AA A3E35B30 B4349B31


  ---------------------------
  i = 1
  w is
                          FD00CEE3 87E139FD EA1DA3FD 07685FBA
        B979711E BFB1C43B A8C9326C 16D8A3AA A3E35B30 B4349B31


  Updated KKey is
                252CF9F8 36F365FD 877459C6 F92B58C6 6ECE61D5


K is
                952127C8 C4B38B8B FFB0DEFA 5FF6AF91 A2A81296


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

FIPS 186-2 Appendix 3.1

    G(t,c) constructed from DES

    Q =
                B5AFD2F9 3246B1EF CD1F3A7C 240C1E9E 21A3630B


    XKey =
                BD029BBE 7F51960B CF9EDB2B 61F06F0F EB5A38B6


    XSeed =
                00000000 00000000 00000000 00000000 00000000


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

XVal is
                BD029BBE 7F51960B CF9EDB2B 61F06F0F EB5A38B6


  G(t,c) using DES
  ---------------------------
    t is
                67452301 EFCDAB89 98BADCFE 10325476 C3D2E1F0


    c is
                BD029BBE 7F51960B CF9EDB2B 61F06F0F EB5A38B6
```

```
    x is
                DA47B8BF 909C3D82 572407D5 71C23B79 2888D946

    ------------

    i = 1

    b1 is
                                                        EB5A38B6

    b2 is
                                                        61F06F0F

    a1 is
                                                        DA47B8BF

    a2 is
                                                        B814E4C4

Block #1
Blockin   DA47B8BF B814E4C4
Blockout  5389735A D85D0E68

    y is
                                            5389735A D85D0E68

    ------------

    i = 2

    b1 is
                                                        BD029BBE

    b2 is
                                                        EB5A38B6

    a1 is
                                                        909C3D82

    a2 is
                                                        8D63BF6A
```

```
Block #1
Blockin   909C3D82 8D63BF6A
Blockout  F195BFD3 B536006D

    y is
                                        5389735A D85D0E68


    ------------

    i = 3

    b1 is
                                                  7F51960B


    b2 is
                                                  BD029BBE


    a1 is
                                                  572407D5


    a2 is
                                                  E15E06FB


Block #1
Blockin   572407D5 E15E06FB
Blockout  E252CB93 6E53217B

    y is
                                        5389735A D85D0E68


    ------------

    i = 4

    b1 is
                                                  CF9EDB2B


    b2 is
                                                  7F51960B


    a1 is
                                                  71C23B79


    a2 is
                                                  7FACDE93
```

```
Block #1
Blockin   71C23B79 7FACDE93
Blockout  D7CB8744 401A5A38

    y is
                                          5389735A D85D0E68


    ------------

    i = 5

    b1 is
                                                    61F06F0F


    b2 is
                                                    CF9EDB2B


    a1 is
                                                    2888D946


    a2 is
                                                    AB8583C6


Block #1
Blockin   2888D946 AB8583C6
Blockout  46029A90 5B813784

    y is
                                          5389735A D85D0E68


    G(t,c) is
                EA11D565 F78D7F7B EA5A8F4D FE0336FF 1166516E


  ---------------------------
Updated XKey is
                F1649E2B 44986397 ECDA2FFD 3BE78770 DB1D271A


X is
                3462026C C546CD8C 1D3B54D1 D9F71860 EFC2EE63


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

FIPS 186-2 Appendix 3.1 using Change Notice 1
```

```
    G(t,c) constructed from DES

    Q =
                B5AFD2F9 3246B1EF CD1F3A7C 240C1E9E 21A3630B


    XKey =
                BD029BBE 7F51960B CF9EDB2B 61F06F0F EB5A38B6


    XSeed =
                00000000 00000000 00000000 00000000 00000000


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

  i = 0
  XVal is
                BD029BBE 7F51960B CF9EDB2B 61F06F0F EB5A38B6


  G(t,c) using DES
  ---------------------------
    t is
                67452301 EFCDAB89 98BADCFE 10325476 C3D2E1F0


    c is
                BD029BBE 7F51960B CF9EDB2B 61F06F0F EB5A38B6


    x is
                DA47B8BF 909C3D82 572407D5 71C23B79 2888D946


    ------------

    i = 1

    b1 is
                                                    EB5A38B6


    b2 is
                                                    61F06F0F


    a1 is
                                                    DA47B8BF


    a2 is
                                                    B814E4C4
```

```
Block #1
Blockin   DA47B8BF B814E4C4
Blockout  5389735A D85D0E68

    y is
                                          5389735A D85D0E68


    ------------

    i = 2

    b1 is
                                                   BD029BBE


    b2 is
                                                   EB5A38B6


    a1 is
                                                   909C3D82


    a2 is
                                                   8D63BF6A


Block #1
Blockin   909C3D82 8D63BF6A
Blockout  F195BFD3 B536006D

    y is
                                          5389735A D85D0E68


    ------------

    i = 3

    b1 is
                                                   7F51960B


    b2 is
                                                   BD029BBE


    a1 is
                                                   572407D5
```

```
    a2 is
                                                    E15E06FB


Block #1
Blockin   572407D5 E15E06FB
Blockout  E252CB93 6E53217B

    y is
                                          5389735A D85D0E68


    ------------

    i = 4

    b1 is
                                                    CF9EDB2B


    b2 is
                                                    7F51960B


    a1 is
                                                    71C23B79


    a2 is
                                                    7FACDE93


Block #1
Blockin   71C23B79 7FACDE93
Blockout  D7CB8744 401A5A38

    y is
                                          5389735A D85D0E68


    ------------

    i = 5

    b1 is
                                                    61F06F0F


    b2 is
                                                    CF9EDB2B


    a1 is
                                                    2888D946
```

```
    a2 is
                                                        AB8583C6


Block #1
Blockin   2888D946 AB8583C6
Blockout  46029A90 5B813784

    y is
                                            5389735A D85D0E68


    G(t,c) is
                EA11D565 F78D7F7B EA5A8F4D FE0336FF 1166516E


  ---------------------------
  w is
                EA11D565 F78D7F7B EA5A8F4D FE0336FF 1166516E


  Updated XKey is
                A7147124 76DF1587 B9F96A79 5FF3A60E FCC08A25


  **********************
  i = 1
  XVal is
                A7147124 76DF1587 B9F96A79 5FF3A60E FCC08A25


  G(t,c) using DES
  ---------------------------
    t is
                67452301 EFCDAB89 98BADCFE 10325476 C3D2E1F0


    c is
                A7147124 76DF1587 B9F96A79 5FF3A60E FCC08A25


    x is
                C0515225 9912BE0E 2143B687 4FC1F278 3F126BD5


    ------------

    i = 1

    b1 is
                                                        FCC08A25
```

```
    b2 is
                                                    5FF3A60E

    a1 is
                                                    C0515225

    a2 is
                                                    A600D5DB


Block #1
Blockin   C0515225 A600D5DB
Blockout  EB20EACD 2B873150

    y is
                                          EB20EACD 2B873150

    ------------

    i = 2

    b1 is
                                                    A7147124

    b2 is
                                                    FCC08A25

    a1 is
                                                    9912BE0E

    a2 is
                                                    E112E4A2


Block #1
Blockin   9912BE0E E112E4A2
Blockout  4C56BF15 94DBEAA5

    y is
                                          EB20EACD 2B873150

    ------------

    i = 3

    b1 is
```

76DF1587

b2 is

A7147124

a1 is

2143B687

a2 is

D6D34C76

Block #1
Blockin 2143B687 D6D34C76
Blockout A77FC099 05551033

y is

EB20EACD 2B873150

---

i = 4

b1 is

B9F96A79

b2 is

76DF1587

a1 is

4FC1F278

a2 is

1E51DD52

Block #1
Blockin 4FC1F278 1E51DD52
Blockout 4D6C7002 1F0880D4

y is

EB20EACD 2B873150

---

i = 5

```
    b1 is
                                                        5FF3A60E

    b2 is
                                                        B9F96A79

    a1 is
                                                        3F126BD5

    a2 is
                                                        8F90A05D


Block #1
Blockin   3F126BD5 8F90A05D
Blockout  F0A1E8C4 6CA24297

    y is
                                            EB20EACD 2B873150

    G(t,c) is
                A3198AFC A3FFD705 20FD68C3 2ABDFE47 C305C2F8


  ----------------------------
  w is
                          EA11D565 F78D7F7B EA5A8F4D FE0336FF
        1166516E A3198AFC A3FFD705 20FD68C3 2ABDFE47 C305C2F8


  Updated XKey is
                A4A2DFC21 1ADEEC8C DAF6D33C 8AB1A456 BFC64D1E


  **********************
X is
                2E108577 08B9FDE1 2AF830D1 2A028FF6 DF7C5C8F


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

FIPS 186-2 Appendix 3.2

    G(t,c) constructed from DES

    Q =
                B5AFD2F9 3246B1EF CD1F3A7C 240C1E9E 21A3630B
```

```
    KKey =
                687A66D9 0648F993 867E121F 4DDF9DDB 01205584


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

  G(t,c) using DES
  ---------------------------
    t is
                EFCDAB89 98BADCFE 10325476 C3D2E1F0 67452301


    c is
                687A66D9 0648F993 867E121F 4DDF9DDB 01205584


    x is
                87B7CD50 9EF2256D 964C4669 8E0D7C2B 66657685


    ------------

    i = 1

    b1 is
                                                    01205584


    b2 is
                                                    4DDF9DDB


    a1 is
                                                    87B7CD50


    a2 is
                                                    F89753E8


Block #1
Blockin   87B7CD50 F89753E8
Blockout  A48A13ED 32096663

    y is
                                            A48A13ED 32096663


    ------------

    i = 2

    b1 is
                                                    687A66D9
```

```
    b2 is
                                                        01205584

    a1 is
                                                        9EF2256D

    a2 is
                                                        11FB8B39


Block #1
Blockin   9EF2256D 11FB8B39
Blockout  4DEBC1C7 E8CFDF11

    y is
                                            A48A13ED 32096663

    ------------

    i = 3

    b1 is
                                                        0648F993

    b2 is
                                                        687A66D9

    a1 is
                                                        964C4669

    a2 is
                                                        10FF5946


Block #1
Blockin   964C4669 10FF5946
Blockout  E9A38B42 4C3E7665

    y is
                                            A48A13ED 32096663

    ------------

    i = 4
```

b1 is
867E121F

b2 is
0648F993

a1 is
8E0D7C2B

a2 is
F02930EC

Block #1
Blockin 8E0D7C2B F02930EC
Blockout A0E66966 F629FF98

y is
A48A13ED 32096663

---

i = 5

b1 is
4DDF9DDB

b2 is
867E121F

a1 is
66657685

a2 is
09BAB17B

Block #1
Blockin 66657685 09BAB17B
Blockout 39D9FD01 51EC3440

y is
A48A13ED 32096663

G(t,c) is
48520CEE 821BC35E 1CC5ACEF DF04CEC2 38B5A952

```
  ---------------------------
Updated KKey is
                B0CC73C7 8864BCF1 A343BF0F 2CE46C9D 39D5FED7


K is
                48520CEE 821BC35E 1CC5ACEF DF04CEC2 38B5A952


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

FIPS 186-2 Appendix 3.2 using Change Notice 1

    G(t,c) constructed from DES

    Q =
                B5AFD2F9 3246B1EF CD1F3A7C 240C1E9E 21A3630B


    KKey =
                687A66D9 0648F993 867E121F 4DDF9DDB 01205584


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

  G(t,c) using DES
  ---------------------------
    t is
                EFCDAB89 98BADCFE 10325476 C3D2E1F0 67452301


    c is
                687A66D9 0648F993 867E121F 4DDF9DDB 01205584


    x is
                87B7CD50 9EF2256D 964C4669 8E0D7C2B 66657685


    ------------

    i = 1

    b1 is
                                                    01205584


    b2 is
                                                    4DDF9DDB


    a1 is
```

87B7CD50

a2 is

F89753E8

Block #1
Blockin 87B7CD50 F89753E8
Blockout A48A13ED 32096663

y is

A48A13ED 32096663

---

i = 2

b1 is

687A66D9

b2 is

01205584

a1 is

9EF2256D

a2 is

11FB8B39

Block #1
Blockin 9EF2256D 11FB8B39
Blockout 4DEBC1C7 E8CFDF11

y is

A48A13ED 32096663

---

i = 3

b1 is

0648F993

b2 is

687A66D9

```
    a1 is
                                                    964C4669


    a2 is
                                                    10FF5946


Block #1
Blockin   964C4669 10FF5946
Blockout  E9A38B42 4C3E7665

    y is
                                          A48A13ED 32096663


    ------------

    i = 4

    b1 is
                                                    867E121F


    b2 is
                                                    0648F993


    a1 is
                                                    8E0D7C2B


    a2 is
                                                    F02930EC


Block #1
Blockin   8E0D7C2B F02930EC
Blockout  A0E66966 F629FF98

    y is
                                          A48A13ED 32096663


    ------------

    i = 5

    b1 is
                                                    4DDF9DDB


    b2 is
```

867E121F

a1 is
66657685

a2 is
09BAB17B

Block #1
Blockin   66657685 09BAB17B
Blockout 39D9FD01 51EC3440

y is
A48A13ED 32096663

G(t,c) is
48520CEE 821BC35E 1CC5ACEF DF04CEC2 38B5A952

---
i = 0
w is
48520CEE 821BC35E 1CC5ACEF DF04CEC2 38B5A952

Updated KKey is
B0CC73C7 8864BCF1 A343BF0F 2CE46C9D 39D5FED7

G(t,c) using DES
---
t is
EFCDAB89 98BADCFE 10325476 C3D2E1F0 67452301

c is
B0CC73C7 8864BCF1 A343BF0F 2CE46C9D 39D5FED7

x is
5F01D84E 10DE600F B371EB79 EF368D6D 5E90DDD6

---

i = 1

b1 is
39D5FED7

```
    b2 is
                                                        2CE46C9D

    a1 is
                                                        5F01D84E

    a2 is
                                                        4E4EBDD9


Block #1
Blockin   5F01D84E 4E4EBDD9
Blockout  44667CD3 59DC370E

    y is
                                            44667CD3 59DC370E

    ------------

    i = 2

    b1 is
                                                        B0CC73C7

    b2 is
                                                        39D5FED7

    a1 is
                                                        10DE600F

    a2 is
                                                        EC703337


Block #1
Blockin   10DE600F EC703337
Blockout  D65109CE 56D45411

    y is
                                            44667CD3 59DC370E

    ------------

    i = 3

    b1 is
```

8864BCF1

b2 is

B0CC73C7

a1 is

B371EB79

a2 is

FFE8ED62

Block #1
Blockin B371EB79 FFE8ED62
Blockout 198A2B58 201B8B4B

y is

44667CD3 59DC370E

---

i = 4

b1 is

A343BF0F

b2 is

8864BCF1

a1 is

EF368D6D

a2 is

EDE136AF

Block #1
Blockin EF368D6D EDE136AF
Blockout 669F8462 60DAD099

y is

44667CD3 59DC370E

---

i = 5

```
    b1 is
                                                        2CE46C9D

    b2 is
                                                        A343BF0F

    a1 is
                                                        5E90DDD6

    a2 is
                                                        B0375523


Block #1
Blockin   5E90DDD6 B0375523
Blockout  AF18C564 0B7505E2

    y is
                                            44667CD3 59DC370E

    G(t,c) is
                02E273FA 19931C33 56995269 E912BAA2 E046BA2D


  ----------------------------
  i = 1
  w is
                          48520CEE 821BC35E 1CC5ACEF DF04CEC2
         38B5A952 02E273FA 19931C33 56995269 E912BAA2 E046BA2D


  Updated KKey is
                B3AEE7C1 A1F7D924 F9DD1179 15F72740 1A1CB905


K is
                AB2AB897 CE90C05A 343CC115 4AFA19A5 0170D7EF
```