

#####

ANSI X9.62-1998 Annex A.4

G(t,c) constructed from SHA-1

N =

FFFFFFF 0000000
FFFFFFF FFFFFFF BCE6FAAD A7179E84 F3B9CAC2 FC632551

XKey =

BD029BBE 7F51960B CF9EDB2B 61F06F0F EB5A38B6

XSeed =

00000000 00000000 00000000 00000000 00000000

#####

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

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

X is

1BD6472C 1D0350F7
93A6B0A4 5C49C328 967C7131 6EA87CC2 A15BF578 AC2A3D77

#####

ANSI X9.62-1998 Annex A.4

G(t,c) constructed from DES

N =
FFFFFFFFFF 00000000
FFFFFFFFFF BCE6FAAD A7179E84 F3B9CAC2 FC632551

XKey =
BD029BBE 7F51960B CF9EDB2B 61F06F0F EB5A38B6

XSeed =
00000000 00000000 00000000 00000000 00000000

#####

G(t,c) using DES

t is
67452301 EFCDAB89 98BADC9E 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

G(t,c) using DES

t is

67452301 EFCDAB89 98BADCCE 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

x is
E1E80EC8 1C63E21E
4EBFDCE4 0B5E3EC5 391C3523 D30D61F6 07207AD7 EAF3B7A9