## 20L1283-RameenAmir-35202-6708930-2

## Conversion to Binary

"2" = 00110010

"0" = 00110000

"L" = 01001100

"1" = 00110001

"2" = 00110010

"8" = 00111000

"3" = 00110011

"-" = 00101101

"R" = 01010010

"A" = 01000001

"M" = 01001101

"E" = 01000101

"E" = 01000101

"N" = 01001110

"A" = 01000001

"M" = 01001101

"I" = 01001001

"R" = 01010010

"-" = 00101101

"3" = 00110011

"5" = 00110101

"2" = 00110010

"0" = 00110000

"2" = 00110010

"-" = 00101101

"6" = 00110110

"7" = 00110111

"0" = 00110000

"8" = 00111000

"9" = 00111001

"3" = 00110011

"0" = 00110000

"-" = 00101101

"2" = 00110010

## Padding

**Input to hash function(1024 bits) = padded msg(896 bits) + msg length(128 bits)**

### Message

Message Length = 34 \* 8 = 272 bits

Length required ⩭ 896 mod 1024

272 mod 1024 = 896

(624 + 272) mod 1024 = 896

Padding 624 bits - 1 bit followed by 623 zeros bits

00110010001100000100110000110001001100100011100000110011001011010101001001000001010011010100010101000101010011100100000101001101010010010101001000101101001100110011010100110010001100000011001000101101001101100011011100110000001110000011100100110011001100000010110100110010100000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000 **(896 bits)**

### Message Length

* Binary representation of 272:

00000010 00000111 00000010

* Padding to make it 128 bits:

00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000

* Message length represented in 128 bits:

00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000100000011100000010 **(128 bits)**

## Expanding a 1024 bit block: Generating 16 Words(0-15) from 1024 bit block

* 1. **Message**

00110010 00110000 01001100 00110001

00110010 00111000 00110011 00101101

01010010 01000001 01001101 01000101

01000101 01001110 01000001 01001101

01001001 01010010 00101101 00110011

00110101 00110010 00110000 00110010

00101101 00110110 00110111 00110000

00111000 00111001 00110011 00110000

00101101 00110010 00000000 00000000

00000000 00000000 00000000 00000000

In hex Without Padding :

32 30 4C 31 32 38 33 2D

52 41 4D 45 45 4E 41 4D

49 52 2D 33 35 32 30 32

2D 36 37 30 38 39 33 30

2D 32

* 1. **Key**

00000000 00000000 00000000 00000000

00000000 00000000 00000000 00000000

00000000 00000000 00000000 00000000

00000000 00000010 00000111 00000010

In hex Without Padding:

20702

**16 words**

W0: 32304C313238332D

W1: 52414D45454E414D

W2: 49522D3335323032

W3: 2D36373038393330

W4: 2D32000000000000

W5: 0000000000000000

W6: 0000000000000000

W7: 0000000000000000

W8: 0000000000000000

W9: 0000000000000000

W10: 0000000000000000

W11: 0000000000000000

W12: 0000000000000000

W13: 0000000000000000

W14: 0000000000000000

W15: 0000000000020702

## Compression Function

Initial Hash Constants:

H0 = 6a09e667f3bcc908

H1 = bb67ae8584caa73b

H2 = 3c6ef372fe94f82b

H3 = a54ff53a5f1d36f1

H4 = 510e527fade682d1

H5 = 9b05688c2b3e6c1f

H6 = 1f83d9abfb41bd6b

H7 = 5be0cd19137e2179

There will be 16 rounds.

Round Constant = 01010101

**64 bit binary:**

01010101 01010101 01010101 01010101 01010101 01010101 01010101 01010101

**16 bit hex** = 55 55 55 55 55 55 55 55

### **Round 0:**

#### Variables:

a = 6a09e667f3bcc908

b = bb67ae8584caa73b

c = 3c6ef372fe94f82b

d = a54ff53a5f1d36f1

e = 510e527fade682d1

f = 9b05688c2b3e6c1f

g = 1f83d9abfb41bd6b

h = 5be0cd19137e2179

W0: 32304C313238332D

#### Round operations:

T1 = h + Σ1(e) + Ch(e, f, g) + K[0] + W[0]

= 5be0cd19137e2179 + Σ1(510e527fade682d1) + Ch(510e527fade682d1,9b05688c2b3e6c1f, 1f83d9abfb41bd6b) + 5555555555555555 + 32304C313238332D

= 5be0cd19137e2179 + (e right-rotate 14) ^ (e right-rotate 18) ^ (e right-shift 3) + ((e & f) ^ (~e & g)) + 5555555555555555 + 32304C313238332D

= 5be0cd19137e2179 + 35d08c401fb05b2f + 8B300000420410B + 5555555555555555 + 32304C313238332D

**T1 = 86320A2D95DBD03A**

T2 = Σ0(a) + Maj(a, b, c)

= ((a right-rotate 28) ^ (a right-rotate 34) ^ (a right-shift 39)) + ((a & b) ^ (a & c) ^ (b & c))

= 6f60d84f0b78850d + 3A64260440800000

**T2 = A002FC5305F8850D**

* Variables Calculation:

h = g = 1f83d9abfb41bd6b

g = f = 9b05688c2b3e6c1f

f = e = 510e527fade682d1

e = d + T1 = a54ff53a5f1d36f1 + 86320A2D95DBD03A = 8B785F89F4F8E3FB

d = c = 3c6ef372fe94f82b

c = b = bb67ae8584caa73b

b = a = 6a09e667f3bcc908

a = T1 + T2 = 86320A2D95DBD03A + A002FC5305F8850D = 12352E78FB3A58647

* Update hash values:

H0 = H0 + a = 6a09e667f3bcc908 + 12352e78fb3a58647

= 7f8634f893e82f4f

H1 = H1 + b = bb67ae8584caa73b + 6a09e667f3bcc908

= dbe0d4ed785f6e43

H2 = H2 + c = 3c6ef372fe94f82b + bb67ae8584caa73b

= f83dc24b836f6b66

H3 = H3 + d = a54ff53a5f1d36f1 + 3c6ef372fe94f82b

= d9bfe8acd40c1efc

H4 = H4 + e = 510e527fade682d1 + 8b785f89f4f8e3fb

= db8e1163f8e051dc

H5 = H5 + f = 9b05688c2b3e6c1f + 510e527fade682d1

= ec0ecafd5f1c2e40

H6 = H6 + g = 1f83d9abfb41bd6b + 9b05688c2b3e6c1f

= ba8bb02dc36f0d8a

H7 = H7 + h = 5be0cd19137e2179 + 1f83d9abfb41bd6b

= 7ae4a4ba2ebfe8e4

### **Round 1:**

T1 = h + Σ1(e) + Ch(e, f, g) + K[1] + W[1]

= 1F83D9ABFB41BD6B + Σ1(8B785F89F4F8E3FB) + Ch(8B785F89F4F8E3FB, 510E527FADE682D1, 9B05688C2B3E6C1F) + 5555555555555555 + 52414D45454E414D

**T1 = 7E1A38F29C15567E**

T2 = Σ0(a) + Maj(a, b, c)

Σ0(a) = (a right-rotate 1) ^ (a right-rotate 8) ^ (a right-shift 7)

= D29A6385F95C5713

Maj(a, b, c) = (a & b) ^ (a & c) ^ (b & c)

= 68E0A68132B8400B

T2 = D29A6385F95C5713 + 68E0A68132B8400B

**T2 = F96D0A0762F1CD71E**

h = g = 9b05688c2b3e6c1f

g = f = 510e527fade682d1

f = e = 8B785F89F4F8E3FB

e = d + T1 = 3c6ef372fe94f82b + 7E1A38F29C15567E = B01A2CB5FBAA1AA9

d = c = bb67ae8584caa73b

c = 6a09e667f3bcc908

b = a = 12352E78FB3A58647

a = T1 + T2 = 7E1A38F29C15567E + F96D0A0762F1CD71E = 177E42F9C8D722FC

**Updated hash values:**

H0 = F7E88E284C43AC04

H1 = F6EEF97E0B0F1A77

H2 = A72ED33AC38EA133

H3 = E1BB4EAC0E1246DC

H4 = 065E5800E68C432A

H5 = AB21454E46EC875E

H6 = D8A2C681B0F62A34

H7 = F103350E4EBB8006

### **Round 2:**

W2: 49522D3335323032

T1 = 56170C03CB98242E + Σ1(1A2267DFA0A42A8CD) + Ch(1A2267DFA0A42A8CD, 38F42A68A75426A8, 2F55AAAAA3F8BCB2) + 5555555555555555 + 49522D3335323032

**T1 = 9B96A7435F3C9E24**

T2 = (1F83D9ABFB41BD6B right-rotate 1) ^ (1F83D9ABFB41BD6B right-rotate 8) ^ (1F83D9ABFB41BD6B right-shift 7) + ((1F83D9ABFB41BD6B & 129F6BA98034ED06) ^ (1F83D9ABFB41BD6B & C9F92170F5672ED9) ^ (129F6BA98034ED06 & C9F92170F5672ED9))

**T2 = 3E0C4B8219681B98**

Variables:

h = g = 1A2267DFA0A42A8CD

g = f = 38F42A68A75426A8

f = e = 2F55AAAAA3F8BCB2

e = d + T1 = 8883725DCEBBE5DB + 9B96A7435F3C9E24

d = c = C9F92170F5672ED9

c = b = 1F83D9ABFB41BD6B

b = a = 129F6BA98034ED06

a = T1 + T2 = 9B96A7435F3C9E24 + 3E0C4B8219681B98

Updated hash values after Round 2:

H0 = 67D50E7D98E00334

H1 = 3AB91933C839FBA0

H2 = 1DAAB7C6640D0A32

H3 = E78E9D53E7818759

H4 = 0D0DDA89D55AC994

H5 = 6AA8F8558FA9F271

H6 = 2D97235E98D1716E

H7 = F96138E2D2B7D54B

### **Round 3:**

W3: 2D36373038393330

T1 = 3C6B2CB406C4B769

T2 = E8A6A1B47A7F3091

**Updated variables:**

h = g = 3E0C4B8219681B98

g = f = 38F42A68A75426A8

f = e = 1A2267DFA0A42A8CD

e = d + T1 = C9F92170F5672ED9 + 3C6B2CB406C4B769

d = c = 8883725DCEBBE5DB

c = b = 129F6BA98034ED06

b = a = 1F83D9ABFB41BD6B

a = T1 + T2 = 3C6B2CB406C4B769 + E8A6A1B47A7F3091

**Updated hash values for Round 3:**

H0 = CAA2EDE078748C9D

H1 = E2B1B2E4FCC18FCA

H2 = F83F97F5D44F36D7

H3 = 6CB01175B34F648A

H4 = 8DA02F20455C18F4

H5 = D0E9EC2D70EAE05F

H6 = F82C585C5A93B1F2

H7 = D152AAB81F9E7D3E

### **Round 4:**

W4: 2D32000000000000

T1 = 3D5FDF9426E1AAAB

T2 = 8DA6A1D4B2D1D5CE

**Updated variables:**

h = g = E8A6A1B47A7F3091

g = f = 38F42A68A75426A8

f = e = 3E0C4B8219681B98

e = d + T1 = 8883725DCEBBE5DB + 3D5FDF9426E1AAAB = 38F42A68A75426A8

d = c = E8A6A1B47A7F3091

c = b = 1F83D9ABFB41BD6B

b = a = E8A6A1D4B2D1D5CE

a = 3D5FDF9426E1AAAB + 8DA6A1D4B2D1D5CE = 8ECC3726A22F4881

**Updated hash values for Round 4:**

H0 = C5B151B171EDCEAE

H1 = A76B9B3A23F5B7E1

H2 = 4F41EC14D3E39BDA

H3 = 063FCDEA9DAB89B0

H4 = C318EEA8D405F987

H5 = 42A5726E5C5D4E64

H6 = 95ABF6E60C0B4EC2

H7 = E8E07C5906A469CC

### **Round 5:**

W5: 0000000000000000

T1 = D3AC8F69AF3B4859

T2 = 8ECC3726A22F4881

**Updated variables:**

h = g = E8A07C5906A469CC

g = f = 42A5726E5C5D4E64

f = e = 38F42A68A75426A8

e = d + T1 = A76B9B3A23F5B7E1 + D3AC8F69AF3B4859

d = c = 42A5726E5C5D4E64

c = b = E8A07C5906A469CC

b = a = 8ECC3726A22F4881

a = D3AC8F69AF3B4859 + 8ECC3726A22F4881 = 8468B6E571B1A3E5

**Updated hash values for Round 5:**

H0 = 04F390754872169A

H1 = B0B5E4D7E7AC50A9

H2 = 44E7FBC1D5AC8B5C

H3 = 6D92E40BCF7E13A0

H4 = 3A4B57FAB2A80C38

H5 = 9CB1484116ECCFE4

H6 = 7AC8CC61E1B39083

H7 = 3D750A7E8E05921A

### **Round 6:**

W6: 0000000000000000

T1 = 6A09BCE459348F21

T2 = 8468B6E571B1A3E5

**Updated variables:**

h = g = E8CC3726A22F4881

g = f = 9CB1484116ECCFE4

f = e = 38F42A68A75426A8

e = d + T1 = 42A5726E5C5D4E64 + 6A09BCE459348F21d = 9CB1484116ECCFE4

c = b = E8CC3726A22F4881

b = a = 8468B6E571B1A3E5

a = EFC6D889E0E1E939

**Updated hash values for Round 6:**

H0 = 8A1C14754F6DD663

H1 = 8EB11D00A500CD69

H2 = E0E22C6B3FD4507F

H3 = 2012053FA8D3F378

H4 = 5ED0F3B4D8B82D7E

H5 = DBC23E1A88F1343B

H6 = 0C7C8A051AA8A0AB

H7 = 66D2859EE203A512

### **Round 7:**

W7: 0000000000000000

T1 = D0B732E59BEB1F27

T2 = EFC6D889E0E1E939

**Updated variables:**

h = g = E87C8A051AA8A0AB

g = f = DBC23E1A88F1343B

f = e = 38F42A68A75426A8

e = d + T1 = 9CB1484116ECCFE4 + D0B732E59BEB1F27

d = c = DBC23E1A88F1343B

c = b = E87C8A051AA8A0AB

b = a = EFC6D889E0E1E939

a = C48361B50103F882

**Updated hash values for Round 7:**

H0 = ECE449AE144CE209

H1 = 875789BB808B50A9

H2 = C2093B151BE153AE

H3 = 3B1587347A0F3B23

H4 = 4FAF097B02AB2289

H5 = 1007EBFA490E6253

H6 = 2F7CEAFA0AA12B3E

H7 = 9A43C1643900366D

### **Round 8:**

W8: 0000000000000000

T1 = 993EDBC20A057DD3

T2 = C48361B50103F882

**Updated variables:**

h = g = EFC6D889E0E1E939

g = f = 1007EBFA490E6253

f = e = 38F42A68A75426A8

e = d + T1 = DBC23E1A88F1343B + 993EDBC20A057DD3

d = c = 1007EBFA490E6253

c = b = EFC6D889E0E1E939

b = a = C48361B50103F882

a = 2B71F019CF84011E

**Updated hash values for Round 8:**

H0 = A558401FBFDC19B7

H1 = E6A9DA55549B4F49

H2 = 89C86DDA5E18F7E2

H3 = D4A07521A03C29E9

H4 = 83A9C07FB765E399

H5 = F7D97538E01D20A9

H6 = D1D8E068C2761F20

H7 = 1259A3605C284E59

### **Round 9:**

W9: 0000000000000000

T1 = FCC982B3E6BCDF5E

T2 = 2B71F019CF84011E

**Updated variables:**

h = g = C48361B50103F882

g = f = F7D97538E01D20A9

f = e = 38F42A68A75426A8

e = d + T1 = 1007EBFA490E6253 + FCC982B3E6BCDF5E

d = c = F7D97538E01D20A9

c = b = C48361B50103F882

b = a = 2B71F019CF84011E

a =

**Updated hash values for Round 9:**

H0 = D8F5E12D193D7B00

H1 = 671D702B8C59A212

H2 = 0B411BF2162871EC

H3 = 8B0D0A8E51AC9541

H4 = 96DD6FD98E4C0D89

H5 = 0B83CCE8B5E1F3BF

H6 = D3DFC33B2DE6CE0B

H7 = 17D3061B3D126C41

### **Round 10:**

W10: 0000000000000000

T1 = 0A0E2C8BCEDE2992

T2 = B6C932EBC5AE9D42

**Updated variables:**

h = g = 2B71F019CF84011E

g = f = 0B83CCE8B5E1F3BF

f = e = 38F42A68A75426A8

e = d + T1 = F7D97538E01D20A9 + 0A0E2C8BCEDE2992

d = c = 0B83CCE8B5E1F3BF

c = b = 2B71F019CF84011E

b = a = B6C932EBC5AE9D42

**Updated hash values for Round 10:**

H0 = 2DCC23E51A956B40

H1 = 3EFA719A892B8F5F

H2 = E12CC3A45D157CB2

H3 = E9A889AC5E28B78D

H4 = CDD634601AE87EFA

H5 = 3A62B3F4E54584A4

H6 = 0A08466EF44A1135

H7 = 9B3ED9A0E0475C06

### **Round 11:**

W11: 0000000000000000

T1 = 62CC225067BF1FF2

T2 = 03EB9A8BFC04BBF2

**Update variables:**

h = g = B6C932EBC5AE9D42

g = f = 3A62B3F4E54584A4

f = e = 38F42A68A75426A8

e = d + T1 = 0B83CCE8B5E1F3BF + 62CC225067BF1FF2

d = c = 3A62B3F4E54584A4

c = b = B6C932EBC5AE9D42

b = a = 03EB9A8BFC04BBF2

**Updated hash values for Round 11:**

H0 = DBDD9B1E1AC06BE2

H1 = B5703D58534B3E2F

H2 = D50C9C2F49EF3CC9

H3 = D8122E3FD556D0C3

H4 = 1510F2D15C465BA2

H5 = 6F4B01EED59CFA70

H6 = F9C04E198C3C877D

H7 = A0A11E6190A9C79E

### **Round 12:**

W12: 0000000000000000

T1 = 5A2F75C885689D92

T2 = D6A56B5B19D1A15E

**Update variables:**

h = g = 03EB9A8BFC04BBF2

g = f = 6F4B01EED59CFA70

f = e = 38F42A68A75426A8

e = d + T1 = 3A62B3F4E54584A4 + 5A2F75C885689D92

d = c = 6F4B01EED59CFA70

c = b = 03EB9A8BFC04BBF2

b = a = D6A56B5B19D1A15E

**Updated hash values for Round 12:**

H0 = 6F6E49CC25A7041B

H1 = 6B7E7B0E85C8AB31

H2 = D1E7E36A21E0806D

H3 = 3C9139806A7D8B92

H4 = 3F4511E6BB68E072

H5 = F72CBAADE0A9DC53

H6 = 3A88B74007AA49A4

H7 = 7D440038DC5BC24F

### **Round 13:**

W13: 0000000000000000

T1 = F7E2042A16C58BB4

T2 = D9A7E02B44C21C87

**Update variables:**

h = g = D6A56B5B19D1A15E

g = f = F72CBAADE0A9DC53

f = e = 3A62B3F4E54584A4

e = d + T1 = 03EB9A8BFC04BBF2 + F7E2042A16C58BB4

d = c = F72CBAADE0A9DC53

c = b = D6A56B5B19D1A15E

b = a = D9A7E02B44C21C87

**Updated hash values for Round 13:**

H0 = ECEB9E8274A0BAA6

H1 = 8537A8F94C4B9562

H2 = B7F80EF5A5F7ED3C

H3 = 4DF0B52A4526747D

H4 = C7A9AC35A987F9D5

H5 = E1D7F1A0B26E6957

H6 = 157720E5CDAF5C52

H7 = 0E362D10FAE6B802

### **Round 14:**

W14: 0000000000000000

T1 = F38D5EFCB047E2BC

T2 = D52AE8253B09E1F6

**Update variables:**

h = g = D9A7E02B44C21C87

g = f = E1D7F1A0B26E6957

f = e = 3A62B3F4E54584A4

e = d + T1 = D6A56B5B19D1A15E + F38D5EFCB047E2BC

d = c = E1D7F1A0B26E6957

c = b = D9A7E02B44C21C87

b = a = D52AE8253B09E1F6

**Updated hash values for Round 14:**

H0 = E819F51132AB53A9

H1 = 00B1C13FEBF048AC

H2 = 6964D641A8E6A2EF

H3 = FBE04CEA8E67FAE1

H4 = F3C7A153E76D99F2

H5 = 64A5938E6F3D3D3A

H6 = 1A64E73FD0E92009

H7 = B670E732F008E04C

### **Round 15:**

W15: 0000000000020702

T1 = 0DA0BBE561BDA54A

T2 = 46E8C9BFD9DA7005

**Update variables:**

h = g = D52AE8253B09E1F6

g = f = 64A5938E6F3D3D3A

f = e = 3A62B3F4E54584A4

e = d + T1 = D9A7E02B44C21C87 + 0DA0BBE561BDA54A

d = c = 64A5938E6F3D3D3A

c = b = D52AE8253B09E1F6

b = a = 46E8C9BFD9DA7005

**Updated hash values for Round 15:**

H0 = A8A4F350E69C5353

H1 = 90DEB64DBCB6063B

H2 = 9DA0D482E6D0A980

H3 = 232E5A1B7544C7E5

H4 = BDD45474C64F97C1

H5 = 22CFFEB5F036CCF5

H6 = 68EF154B2488B8D9

H7 = 7DCDF9C53E50B827

### **Final Answer:**

H0 = (A8A4F350E69C5353 + 5555555555555555) % (2^64)

H0 = FCFA47A65C91A908

H1 = (90DEB64DBCB6063B + 5555555555555555) % (2^64)

H1 = E62D9C99B2116C90

H2 = (9DA0D482E6D0A980 + 5555555555555555) % (2^64)

H2 = F30829D89425A4D5

H3 = (232E5A1B7544C7E5 + 5555555555555555) % (2^64)

H3 = 77E3AFFCCB99CDEA

H4 = (BDD45474C64F97C1 + 5555555555555555) % (2^64)

H4 = 0B29AA7A1C44F4BC

H5 = (22CFFEB5F036CCF5 + 5555555555555555) % (2^64)

H5 = 783E5E11636A21EA

H6 = (68EF154B2488B8D9 + 5555555555555555) % (2^64)

H6 = B437DAA3D9E410D2

H7 = (7DCDF9C53E50B827 + 5555555555555555) % (2^64)

H7 = D328AC9B939DCD7C

## **Digest:**

A8A4F350E69C535390DEB64DBCB6063B9DA0D482E6D0A980232E5A1B7544C7E5BDD45474C64F97C122CFFEB5F036CCF568EF154B2488B8D97DCDF9C53E50B827

It's a 128 bits hexadecimal digest.

128 \* 4 = 512 binary bits digest

:: each group of 4 bits gives a hex digit.

# Question 2:

## 20L1283-RameenAmir-35202-6708930-2

**Key:** 08022003

**In binary:**  
00110000 00111000 00110000 00110010 00110010 00110000 00110000 00110011 (64 bits)

Padding 960 zeros to make 1024 bits

000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000 00110000 00111000 00110000 00110010 00110010 00110000 00110000 00110011

**In hexadecimal:**  
3038303232303033

With padding:

0000000000000000 0000000000000000 0000000000000000 0000000000000000

0000000000000000 0000000000000000 0000000000000000 0000000000000000

0000000000000000 0000000000000000 0000000000000000 0000000000000000 0000000000000000 0000000000000000 0000000000000000 3038303232303033

(128 bit hex / 1024 bit binary)

**Ipad:**  
3636363636363636 3636363636363636 3636363636363636 3636363636363636

3636363636363636 3636363636363636 3636363636363636 3636363636363636

3636363636363636 3636363636363636 3636363636363636 3636363636363636

3636363636363636 3636363636363636 3636363636363636 3636363636363636

**XOR with Ipad:**

363636363636363636363636363636363636363636363636363636363636363636363636363636363636363636363636363636363636363636363636363636363636363636363636363636363636363636363636363636363636363636363636363636363636363636363636363636363636363636363636060e060404060605

**Input to SHA:**  
363636363636363636363636363636363636363636363636363636363636363636363636363636363636363636363636363636363636363636363636363636363636363636363636363636363636363636363636363636363636363636363636363636363636363636363636363636363636363636363636060e060404060605

32304C313238332D52414D45454E414D49522D33353230322D363730383933302D3200000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000020702

2 blocks 1024 bit binary/ 256 bit hex

**SHA-512 digest: 11ee93922237d51d10697fb9422510b60f2a4aa8486963573973663ccefec5978db749be228db9c354367f76153a11639c5817e1c5538dc7a9060f0f1f2a6c81**

**Padding to make it 1024:**

00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000**11ee93922237d51d10697fb9422510b60f2a4aa8486963573973663ccefec5978db749be228db9c354367f76153a11639c5817e1c5538dc7a9060f0f1f2a6c81**

**Key XOR with Opad:**

**Opad:**

5C5C5C5C5C5C5C5C 5C5C5C5C5C5C5C5C 5C5C5C5C5C5C5C5C 5C5C5C5C5C5C5C5C

5C5C5C5C5C5C5C5C 5C5C5C5C5C5C5C5C 5C5C5C5C5C5C5C5C 5C5C5C5C5C5C5C5C

5C5C5C5C5C5C5C5C 5C5C5C5C5C5C5C5C 5C5C5C5C5C5C5C5C 5C5C5C5C5C5C5C5C

5C5C5C5C5C5C5C5C 5C5C5C5C5C5C5C5C 5C5C5C5C5C5C5C5C 5C5C5C5C5C5C5C5C

**Key:**

0000000000000000 0000000000000000 0000000000000000 0000000000000000

0000000000000000 0000000000000000 0000000000000000 0000000000000000

0000000000000000 0000000000000000 0000000000000000 0000000000000000 0000000000000000 0000000000000000 0000000000000000 3038303232303033

**XOR:**  
5C5C5C5C5C5C5C5C 5C5C5C5C5C5C5C5C 5C5C5C5C5C5C5C5C 5C5C5C5C5C5C5C5C

5C5C5C5C5C5C5C5C 5C5C5C5C5C5C5C5C 5C5C5C5C5C5C5C5C 5C5C5C5C5C5C5C5C

5C5C5C5C5C5C5C5C 5C5C5C5C5C5C5C5C 5C5C5C5C5C5C5C5C 5C5C5C5C5C5C5C5C

5C5C5C5C5C5C5C5C 5C5C5C5C5C5C5C5C 5C5C5C5C5C5C5C5C 6C646C6E6E6C6C6F

**Appending with padded 1024 bit Digest:**

5C5C5C5C5C5C5C5C5C5C5C5C5C5C5C5C5C5C5C5C5C5C5C5C5C5C5C5C5C5C5C5C5C5C5C5C5C5C5C5C5C5C5C5C5C5C5C5C5C5C5C5C5C5C5C5C5C5C5C5C5C5C5C5C5C5C5C5C5C5C5C5C5C5C5C5C5C5C5C5C5C5C5C5C5C5C5C5C5C5C5C5C5C5C5C5C5C5C5C5C5C5C5C5C5C5C5C5C5C5C5C5C5C5C5C5C5C5C5C5C6C646C6E6E6C6C6F

00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000**11ee93922237d51d10697fb9422510b60f2a4aa8486963573973663ccefec5978db749be228db9c354367f76153a11639c5817e1c5538dc7a9060f0f1f2a6c81**

### **Final Hash Digest:**

**648764308c3f9c5fe3e395e9b37ff0c75eb53af65c4238f98f318a92ae761ad63e3e6180c39f2afdfaeab402b87d241ee23b62f71d005b34ca6f9063bdcaed0c**