# SHA-512

# Plain Text

Your Roll No-Your Name-Your CNIC No.

**20L-1377-Maida Shahid-35202-7166376-8**

2 0 L -

1 3 7 7

- M A I

D A S

H a h i

d - 3 5

2 0 2 -

7 1 6 6

3 7 6 -

8

# Convert it into Binary

00000010 00000000 01001100 00101101

00000001 00000011 00000111 00000111

00101101 01001101 01100001 01101001

01100100 01100001 00100000 00100000

01010011 01101000 01100001 01101001

01100100 00101101 00000011 00000101

00000010 00000000 00000010 00101101

00000111 00000001 00000110 00000110

00000011 00000111 00000110 00101101

00001000

Total bits =**296 bits**

Msg length= **896 mod 1024**

**296+600 mod 1024=896**

600 bits are to be padded starting with **1** and **599** zeros.

# 

# Step 1 Append padding bits.

02004C2D01030707

2D4D5A6564612020

53696169642D0305

0200022D07010606

0307062D08800000

0000000000000000

0000000000000000

0000000000000000

0000000000000000

0000000000000000

0000000000000000

0000000000000000

0000000000000000

0000000000000000

# Step 2 Append length.

296 in hex=128

Added 128 bits.

02004C2D01030707

2D4D5A6564612020

53696169642D0305

0200022D07010606

0307062D08800000

0000000000000000

0000000000000000

0000000000000000

0000000000000000

0000000000000000

0000000000000000

0000000000000000

0000000000000000

0000000000000000

0000000000000000

0000000000000128

This block is assigned to the words W0, . . . , W15 of the message schedule,

which appears as follows.

W0 = 02004C2D01030707 W8 = 0000000000000000

W1 = 2D4D5A6564612020 W9 = 0000000000000000

W2 = 53696169642D0305 W10 = 0000000000000000

W3 = 0200022D07010606 W11 = 0000000000000000

W4 = 0307062D08800000 W12 = 0000000000000000

W5 = 0000000000000000 W13 = 0000000000000000

W6 = 0000000000000000 W14 = 0000000000000000

W7 = 0000000000000000 W15 = 0000000000000128

# Step 3 Initialize hash buffer.

# Initialize hash values

H = [

a= 0x6a09e667f3bcc908,

b=0xbb67ae8584caa73b,

c= 0x3c6ef372fe94f82b,

d=0xa54ff53a5f1d36f1,

e=0x510e527fade682d1,

f=0x9b05688c2b3e6c1f,

g=0x1f83d9abfb41bd6b,

h=0x5be0cd19137e2179

]

# Step 4 Process message in 1024-bit (128-byte) blocks.

Now we do the computation:

**1st Round**

h=0x5be0cd19137e2179

e=0x510e527fade682d1

f=0x9b05688c2b3e6c1f

g=0x1f83d9abfb41bd6b

Ch(e,f,g)=(e∧f)⊕(¬e∧g)

e∧f=0x5006488c2ac68201

-e= 0xaef1ad8a5021972e

(¬e∧g)=0xae1f017d50b2044a

Now Xor

(e∧f)⊕(¬e∧g)= 0xfe1e4ff15adac86b

e after circular shift

14,18,41

e= 0x9c1a1a1c4d7b0a4f

W0 = 02004C2D01030707

k0=0x428a2f98d728ae22

Now T1 = (h + Ch(e, f, g) + s1(e) + W[t] + K[t]) % (2\*\*64)

Adding all values and taking mod with 2^64

T1=5300053968767794506

Now T2

T2 = (s0(a) + Maj(a, b, c)) % (2\*\*64)

s0(a)=This term involves the circular right shift function

s0(a), which is defined as a bitwise rotation of a by 1 bit, followed by a rotation by 8 bits, and then another rotation by 7 bits.

Original value: 0x6a09e667f3bcc908 in binary is 01101010000010011110011001100111111110001101100111000 1001001000111101111100001011001001000.

Right rotation by 1 bit:

rotated\_1: 100110100000010011110011001100111111000110110011100010010010001111101111100001011001001000

Right rotation by 8 bits:

rotated\_8: 110110011111000011011011111111100001100100011100000101110011100001111110000001011001001000

Right rotation by 7 bits:

rotated\_7: 010111001111100001110111111111110000110010001110000010111001110000111111000000101100100100

Combine the results:

result\_s0: 11000001111011011111010000111011001111011001110000111000111110001100111000110111100001110011100

s0(a)=0xc1edf43b3b398c7c

Maj(a,b,c)

Bitwise AND of a and b

a∧b: 0110101000001001111001100110011111111000110110011100010100101101101101101001110101011101000010010000010010110101001001010110001000010100111101000110

Bitwise AND of a and c:

a∧c: 01101010000010011110011001100111111110001101100111000000001001110011100101111111101001000101010001000111011111100001001000110010111111000

Bitwise AND of b and c

b∧c: 001101100110011110101110100001010000001001000000110111110110111111010100010110010001100111000101101100011010111101111100000010011110000

Combine the results using XOR:

Maj(a,b,c): 0110101000001001111001100110011111111000110110011100010100101101101101101001110101011101000010010000010010110101001001010110001000010100111101000110

=0x6a09e667f3bcc908

Combining all values and

T2=8658961387745676042

h = g

h=0x1f83d9abfb41bd6b

g = f

g=0x9b05688c2b3e6c1f

f = e

f=0x510e527fade682d1

e = (d + T1) % (2\*\*64)

d+T1= 0x7619e6080f30ad58

e= 0x7619e6080f30ad58

d = c

d=0x3c6ef372fe94f82b

c = b

c=0xbb67ae8584caa73b

b = a

b=0x6a09e667f3bcc908

a = (T1 + T2) % (2\*\*64)

a=0xb3da4af260bf22ea

**Now Round 2**

T1 4243844985367047122

T2 2362384768941999370

a 6606229754309046492

b 13959015356513470548

c 7640891576956012808

d 13503953896175478587

e 8598530550303892477

f 17212063139238704187

g 5840696475078001361

h 11170449401992604703

**Round 3**

T1 4505895742819145214

T2 4387731227661102555

a 8893626970480247769

b 6606229754309046492

c 13959015356513470548

d 7640891576956012808

e 18009849638994623801

f 8598530550303892477

g 17212063139238704187

h 5840696475078001361

**Round 4**

T1 13800916329445355762

T2 13828293165178720708

a 9182465420914524854

b 8893626970480247769

c 6606229754309046492

d 13959015356513470548

e 2995063832691816954

f 18009849638994623801

g 8598530550303892477

h 17212063139238704187

**Round 5**

T1 9677649281238225408

T2 334797887427624760

a 10012447168665850168

b 9182465420914524854

c 8893626970480247769

d 6606229754309046492

e 5189920564042144340

f 2995063832691816954

g 18009849638994623801

h 8598530550303892477

**Round 6**

T1 10198336203731093083

T2 17894283350991969767

a 9645875481013511234

b 10012447168665850168

c 9182465420914524854

d 8893626970480247769

e 16804565958040139575

f 5189920564042144340

g 2995063832691816954

h 18009849638994623801

**Round 7**

T1 17410931822963360128

T2 10475353982908951615

a 9439541732162760127

b 9645875481013511234

c 10012447168665850168

d 9182465420914524854

e 7857814719734056281

f 16804565958040139575

g 5189920564042144340

h 2995063832691816954

**Round 8**

T1 1670659869993368563

T2 214018034904502947

a 1884677904897871510

b 9439541732162760127

c 9645875481013511234

d 10012447168665850168

e 10853125290907893417

f 7857814719734056281

g 16804565958040139575

h 5189920564042144340

**Round 9**

T1 16625831964692942482

T2 2179017861362715374

a 358105752346106240

b 1884677904897871510

c 9439541732162760127

d 9645875481013511234

e 8191535059649241034

f 10853125290907893417

g 7857814719734056281

h 16804565958040139575

**Round 10**

T1 5158416014672267755

T2 9615419363861215616

a 14773835378533483371

b 358105752346106240

c 1884677904897871510

d 9439541732162760127

e 14804291495685778989

f 8191535059649241034

g 10853125290907893417

h 7857814719734056281

**Round 11**

T1 8815642315374447760

T2 11023634173931726578

a 1392532415596622722

b 14773835378533483371

c 358105752346106240

d 1884677904897871510

e 18255184047537207887

f 14804291495685778989

g 8191535059649241034

h 10853125290907893417

**Round 12**

T1 553135322471621220

T2 10443720993798990551

a 10996856316270611771

b 1392532415596622722

c 14773835378533483371

d 358105752346106240

e 2437813227369492730

f 18255184047537207887

g 14804291495685778989

h 8191535059649241034

**Round 13**

T1 3612663990095943769

T2 10376037626376696757

a 13988701616472640526

b 10996856316270611771

c 1392532415596622722

d 14773835378533483371

e 3970769742442050009

f 2437813227369492730

g 18255184047537207887

h 14804291495685778989

**Round 14**

T1 16565902492287898022

T2 29376720633171037

a 16595279212921069059

b 13988701616472640526

c 10996856316270611771

d 1392532415596622722

e 12892993797111829777

f 3970769742442050009

g 2437813227369492730

**Round 15**

T1 12343988719312767835

T2 12905838849466170798

a 6803083495069387017

b 16595279212921069059

c 13988701616472640526

d 10996856316270611771

e 13736521134909390557

f 12892993797111829777

g 3970769742442050009

h 2437813227369492730

Now add the first values and values after calculation

The hash value is then calculated as

H1,0 = 6a09e667f3bcc908 + 73a54f399fa4b1b2 = C8B613604CA311D1

H1,1 = bb67ae8584caa73b + 10d9c4c4295599f6 = A1FD8C08B84D4F3E

H1,2 = 3c6ef372fe94f82b + d67806db8b148677 = 0026D636CCB5FF59

H1,3 = a54ff53a5f1d36f1 + 654ef9abec389ca9 = 3EABD65C899C31C4

H1,4 = 510e527fade682d1 + d08446aa79693ed7 = 0F9B51DFD5E7FDE6

H1,5 = 9b05688c2b3e6c1f + 9bb4d39778c07f9e = 4E5A1050E6B0D000

H1,6 = 1f83d9abfb41bd6b + 25c96a7768fb2aa3 = 56F740C3F59D00A4

H1,7 = 5be0cd19137e2179 + ceb9fc3691ce8326 = 7E334BA1B91C9F23

H[0]= 14443975072025399825

H[1]= 11652489035386996030

H[2]= 18343387181409485881

H[3]= 4462121413031969836

H[4]= 1130473536277840302

H[5]= 5616699125394882864

H[6]= 6241667712244936516

H[7]= 9058330187189031539

# Step 5 Output.

The resulting 512-bit message digest is

c8734eccf0abd211 a1b5f50a4760453e fe90cd743d5dc439 3deca3c8a86f442c

0fb03fb115d201ae 4df286189368c130 569edbb6ea626f44 7db5a74fe9999273

# 

# HMAC

# Plain Text

Your Roll No-Your Name-Your CNIC No.

**20L-1377-Maida Shahid-35202-7166376-8**

2 0 L -

1 3 7 7

- M A I

D A S

hahi

d - 3 5

2 0 2 -

7 1 6 6

3 7 6 -

8

# Convert it into Binary

00000010 00000000 01001100 00101101

00000001 00000011 00000111 00000111

00101101 01001101 01100001 01101001

01100100 01100001 00100000 00100000

01010011 01101000 01100001 01101001

01100100 00101101 00000011 00000101

00000010 00000000 00000010 00101101

00000111 00000001 00000110 00000110

00000011 00000111 00000110 00101101

00001000

Total bits =**296 bits**

Msg length= **896 mod 1024**

**296+600 mod 1024=896**

600 bits are to be padded starting with **1** and **599** zeros.

# Step 1 Append padding bits.

02004C2D01030707

2D4D5A6564612020

53696169642D0305

0200022D07010606

0307062D08800000

0000000000000000

0000000000000000

0000000000000000

0000000000000000

0000000000000000

0000000000000000

0000000000000000

0000000000000000

0000000000000000

## 1. Append zeros to the left end of K to create a b-bit string K+

key=1 5 0 9 2 0 0 0

00000001 00000101 00000000 00001001 00000010 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000

00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000

00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000

00000000 00000000

01 05 00 09 02 00 00 00

64 bits

Now add 960 bits

The IV = 01010101 is repeated over b/16 times.

K+=

0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000001050902000000

IPAD=

3636363636363636363636363636363636363636363636363636363636363636363636363636363636363636363636363636363636363636363636363636363636363636363633636363636363636363636363636363636363636363636363636363636363636336363636363636363636363636363636363636363636363636

## 2. XOR (bitwise exclusive-OR) K+ with ipad to produce the b-bit block Si

K+ XOR IPAD=S

3636363636363636363636363636363636363636363636363636363636363636363636363636363636363636363636363636363636363636363636363636363636363636363633636363636363636363636363636363636363636363636363636363636363636336363636363636363636363636363636363637333f34363636

## 3. Append M to Si

Append S+M

3636363636363636

3636363636363636

3636363636363636

3636363636363636

3636363636363636

3636363636363636

3636363636363636

3636363636363636

3636363636363363

6363636363636363

6363636363636363

6363636363636363

6363636363636336

3636363636363636

3636363636363636

3637333f34363636

02004C2D01030707

2D4D5A6564612020

53696169642D0305

0200022D07010606

0307062D08800000

0000000000000000

0000000000000000

0000000000000000

0000000000000000

0000000000000000

0000000000000000

0000000000000000

0000000000000000

0000000000000000

0000000000000000

0000000000000128

## 4. Apply H to the stream

After Hash Value:

9e0ac827abc52ff2

6d3974cdeea28899

9f6bc443cb7a26b5

6355fd4ecfa1f84e

55c05cb3c111ead2

5Aec7b5df1727efe

fE1c6025add19203

F5a894b935fef30a

## 5. XOR K+ with opad to produce the b-bit block So.

OPAD

01011100 01011100 01011100 01011100 01011100 01011100 01011100 01011100

01011100 01011100 01011100 01011100 01011100 01011100 01011100 01011100

01011100 01011100 01011100 01011100 01011100 01011100 01011100 01011100

01011100 01011100 01011100 01011100 01011100 01011100 01011100 01011100

01011100 01011100 01011100 01011100 01011100 01011100 01011100 01011100

01011100 01011100 01011100 01011100 01011100 01011100 01011100 01011100

01011100 01011100 01011100 01011100 01011100 01011100 01011100 01011100

01011100 01011100 01011100 01011100 01011100 01011100 01011100 01011100

5C5C5C5C 5C5C5C5C 5C5C5C5C 5C5C5C5C 5C5C5C5C 5C5C5C5C 5C5C5C5C 5C5C5C5C

5C5C5C5C 5C5C5C5C 5C5C5C5C 5C5C5C5C 5C5C5C5C 5C5C5C5C 5C5C5C5C 5C5C5C5C

5C5C5C5C 5C5C5C5C 5C5C5C5C 5C5C5C5C 5C5C5C5C 5C5C5C5C 5C5C5C5C 5C5C5C5C

5C5C5C5C 5C5C5C5C 5C5C5C5C 5C5C5C5C 5C5C5C5C 5C5C5C5C 5C5C5C5C

5C5C5C5C

K+XOR OPAD=S0

5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5c5d59555e5c5c5c

Append bits to make 1024 bits

9e0ac827abc52ff2 6d3974cdeea28899 9f6bc443cb7a26b5 6355fd4ecfa1f84e

55c05cb3c111ead2 5aec7b5df1727efe fe1c6025add19203 f5a894b935fef30a

0000000000000000 0000000000000000 0000000000000000 0000000000000000

0000000000000000 0000000000000000 0000000000000000 0000000000000000

## 6. Append the hash result from step 4 to So.

Append S0 and M

5c5c5c5c5c5c5c5c

5c5c5c5c5c5c5c5c

5c5c5c5c5c5c5c5c

5c5c5c5c5c5c5c5c

5c5c5c5c5c5c5c5c

5c5c5c5c5c5c5c5c

5c5c5c5c5c5c5c5c

5c5c5c5c5c5c5c5c

5c5c5c5c5c5c5c5c

5c5c5c5c5c5c5c5c

5c5c5c5c5c5c5c5c

5c5c5c5c5c5c5c5c

5c5c5c5c5c5c5c5c

5c5c5c5c5c5c5c5c

5c5c5c5c5c5c5c5c

5c5d59555e5c5c5c

9e0ac827abc52ff2

6d3974cdeea28899

9f6bc443cb7a26b5

6355fd4ecfa1f84e

55c05cb3c111ead2

5aec7b5df1727efe

Fe1c6025add19203

f5a894b935fef30a

0000000000000000

0000000000000000

0000000000000000

0000000000000000

0000000000000000

0000000000000000

0000000000000000

0000000000000000

## 7. Apply H to the stream generated in step 6 and output the result.

Hash value

166f342bf9b22533 839957bd2e1b520a bb54d45d37a72cd1 86d21d1a5407613d 9bf98b548412fd1c d94641630a74f326 6ed39649ef4fc29b b5e1bd8861514791