

PT = 1100000000111100101010

m1 = 11000000

m2 = 00111100

m3 = 10101000

IV = 11001100

k = 10000101

ipad = 01011100

opad = 00110110

z0 = 1100110011011001

z1 = 0000011111000000

z2 = 0010000000111100

z3 = 0100000010101000

z4 = 1000111000010110

p = 1100110010110011

q = 00001000

r = 0000100010010111

t = 00101110

HMAC construction

Plaintext:

Next Plaintext

length of Initialization Vector (IV), 1,

IV:

Next IV

Key, k:

Next Key

ipad: 0x5C (01011100)

opad: 0x36 (00110110)

Put your text of size 21 to get the corresponding value of hash of size 1.

Your text:

get hash

Hashed value:

Final Output:

Check Answer!

CORRECT!!