

PT = 11011001000001011101

M1 = 11011001

M2 = 00000101

M3 = 11010000

IV = 01011010

K = 00001111

Ipad = 01011100

Opad = 00110110

Z0 = 0101101001010011

Z1 = 1111110011011001

Z2 = 0000011100000101

Z3 = 0010001111010000

Z4 = 0100010000010100

P = 0101101000111001

Q = 1111001110100110

T = 00001111

## HMAC construction

Plaintext:

Next Plaintext

length of Initialization Vector (IV),  $l$ ,

IV:

Next IV

Key,  $k$ :

Next Key

ipad: 0x5C (01011100)

opad: 0x36 (00110110)

Put your text of size  $2l$  to get the corresponding value of hash of size  $l$ .

Your text:

get hash

Hashed value:

Final Output:

Check Answer!

CORRECT!!