

Name: Adwait Purao

UID: 2021300101

BE-COMPS B

CSS - Batch - V

PAGE NO.:



Exp - 5a - Report writeup

Steps:

1) Select Plaintext:

m : 10101100 10001101 10100001
00101110

here $m(\text{length}) = 32$ $l(\text{block length}) = 8$

2) Generate Initialization Vector:

IV: 11010011

3) Fix spad & opad values

IV: 11010011

4) Divide plaintext into chunks

$m_1 = 10101100$

$m_2 = 11001101$

$m_3 = 10100001$

$m_4 = 00101110$

5) Compute $z_0 = \text{IV} \parallel k \text{ XOR } \text{spad}$

for chunk 1

$m_1 = 10101100$

$\text{spad} = 00110110$

$\therefore k \text{ XOR} = 10011010$

6) Concatenate with IV: $z_1 = z_0 || m_1$

$$\therefore z_1 = 1101\ 0011\ 1001\ 1010 || 10101100$$

7) Compute $z_2 = 1101\ 0010\ 1001\ 10 || 11001101$

8) Repeat for remaining chunks

$$z_3 = z_2 || m_3$$

$$z_4 = z_3 || m_4$$

9) Compute $z_{k+1} = z_k || l$

here $l = 32$ bits, $\therefore l = 0010\ 000$

10) Compute $P = IV || (k \text{ XOR opad})$

for the 1st chunk:

$$m_1 = 1010\ 1100$$

$$\text{opad} = 0101\ 1100$$

$$k \text{ XOR opad} = 1111\ 0000$$

Concatenate with IV

$$P = IV || (k \text{ XOR opad})$$

$$\therefore P = 1101\ 0011\ 1111\ 0000$$

11) Compute $r = q || z_{k+1}$

$$r = 0000\ 1000\ 1001\ 0111$$

12) Final HMAC tag (t) :-

t = 0010 1110

$z_0 =$ 1100 1100 1101 1001

$z_1 =$ 0000 0111 1100 0000

$z_2 =$ 0010 0000 0011 1100

$z_3 =$ 0100 0000 0101 0100

$z_4 =$ 1000 1110 0000 1011

p = 1100 1100 1011 0011

q = 0000 1000

r = 0000 1000 1001 0111

t = 0010 1110