Name - Shubham Solanki
UID - 20223010 15.

1. Select plain text
m = 10101100 10001101 10100001
00101110.

Here. m (length) = 32, l = 8 (block length).

2. Generate initialization vector.
IV = 11010011

3. Fix ipad and opad values (constants).
ipad = 00110110
opad = 01011100

4. Divide plaintext into chunks.
m1 = 10101100
m2 = 11001101
m3 = 10100001
m4 = 00101110

5. Compute z0 = IV || (x XOR ipad)
for chunk1
m1 = 10101100
ipad = 00110110.
x XOR ipad = 10011010

Concatenate with IV z1 = z0 || m1.

z1 = 11010011 00110110 || 10101100

8. Compute $z_2 = z_1 || m_2$
$z_2 = 1101001110011 0 \ldots \ldots || 1100101101$

9. Repeat for remaining chunks.
$z_3 = z_2 || m_3$
$z_4 = z_3 || m_4 \ldots$

10. Compute $z_{(k+3)} = z_k || z$
here $l = 32$ bits.
$\therefore L = 00100000$

11. Compute $r = IV || (K \text{ XOR } opad)$
for first chunk m_1,
$m_1 = 10101100$
$opad = 01011100$
$K \text{ XOR } opad = 11110000$

Concatenate with IV
$r \rightarrow IV || (K \text{ XOR } opad)$
$= 1101001111110000$

12. Compute $v = S_1 || z_{(10+4)}$
$S = 0000100010010010111$

15. The final HMAC tag (t)
$t = 00101110$