

HASH-1)

$$\text{aesenc}(M_1, IV) = C$$

$$\text{aesenc}(M_2, C) = \text{hash}$$

Therefore

$$\text{aesdec}(C, IV) = M_1$$

$$\text{aesdec}(\text{hash}, C) = M_2$$

$$\text{set } C = 10101010 \ 1010 \ 1010$$

$$M_1 = 101011101000001$$

$$M_2 = 1110 \ 0000 \ 0010 \ 0000$$

$$\text{aesenc}(M_1, IV) = 101010101010 \ 1010 = C$$

$$\text{aesenc}(M_2, C) = 1111 \ 1111 \ 1111 \ 1111 = \text{hash}$$

MAC-1)

$$\text{macker} = 0100 \ 1100 \ 1000 \ 0011$$

$$\text{me} = 0110 \ 1101 \ 0110 \ 0101$$

$$\text{mo} = 0110 \ 1101 \ 0110 \ 1111$$

$$\text{ry} = 0111 \ 0010 \ 0111 \ 1001$$

$$x = \text{aesenc}(\text{me}, \text{macker})$$

$$y = \text{aesenc}(\text{mo}, x)$$

$$z = \text{aesenc}(\text{ry}, y) = 1011 \ 0110 \ 1110 \ 0110$$