Assignment-2

Submitted By:-
Om Prakash
19103077

(1.) keywords $w_0 = \begin{bmatrix} 0 & 0 \\ 0 & 0 \\ 0 & 0 \\ 0 & 0 \end{bmatrix}$, $w_1 = \begin{bmatrix} 0 & 0 \\ 0 & 0 \\ 0 & 0 \\ 0 & 0 \end{bmatrix}$, $w_2 = \begin{bmatrix} 0 & 0 \\ 0 & 0 \\ 0 & 0 \\ 0 & 0 \end{bmatrix}$

$w_3 = \begin{bmatrix} 0 & 0 \\ 0 & 0 \\ 0 & 0 \\ 0 & 0 \end{bmatrix}$

for first round key

Rot Word

$w_3 = \begin{bmatrix} 0 & 0 \\ 0 & 0 \\ 0 & 0 \\ 0 & 0 \end{bmatrix} \xrightarrow{\text{RotWord}} \begin{bmatrix} 0 & 0 \\ 0 & 0 \\ 0 & 0 \\ 0 & 0 \end{bmatrix}$

(2) SB (SubByte)

$t = \begin{bmatrix} 0 & 0 \\ 0 & 0 \\ 0 & 0 \\ 0 & 0 \end{bmatrix} \xrightarrow{\text{SubWord}} \begin{bmatrix} 6 & 3 \\ 6 & 3 \\ 6 & 3 \\ 6 & 3 \end{bmatrix}$

→ Applying Rcon for first round.

$$\begin{bmatrix} 6 & 3 \\ 6 & 3 \\ 6 & 3 \\ 6 & 3 \end{bmatrix} \oplus \begin{bmatrix} 0 & 1 \\ 0 & 0 \\ 0 & 0 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 6 & 2 \\ 6 & 3 \\ 6 & 3 \\ 6 & 3 \end{bmatrix}$$

$6\ 3 = 01100011$ bit2, $0\ 1 = 0000\ 0001$ (bitwise)

$63 \oplus 01 = 01100010$ (bitwise) $= 62$ (Hexadecimal)

and $63 \oplus 00 = 63$

so finally $t = \begin{bmatrix} 6 & 2 \\ 6 & 3 \\ 6 & 3 \\ 6 & 3 \end{bmatrix}$

First Round by words are

$$w_4 = t \oplus w_0 = \begin{bmatrix} 6 & 2 \\ 6 & 3 \\ 6 & 3 \\ 6 & 3 \end{bmatrix} \oplus \begin{bmatrix} 0 & 0 \\ 0 & 0 \\ 0 & 0 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 6 & 2 \\ 6 & 3 \\ 6 & 3 \\ 6 & 3 \end{bmatrix}$$

$\left\{ \because\ x \oplus 0 = x \right.$

$\left. \because\ 62 \oplus 00 = 62 \right\}$

$$w_5 = w_0 \oplus w_1 = \begin{bmatrix} 62 \\ 63 \\ 63 \\ 63 \end{bmatrix} \oplus \begin{bmatrix} 00 \\ 00 \\ 00 \\ 00 \end{bmatrix} = \begin{bmatrix} 62 \\ 63 \\ 63 \\ 63 \end{bmatrix}$$

$$w_6 = w_5 \oplus w_4 = \begin{bmatrix} 63 \\ 63 \\ 63 \\ 63 \end{bmatrix} \oplus \begin{bmatrix} 00 \\ 00 \\ 00 \\ 00 \end{bmatrix} = \begin{bmatrix} 62 \\ 63 \\ 63 \\ 63 \end{bmatrix}$$

$$w_7 = w_6 \oplus w_3 = \begin{bmatrix} 62 \\ 63 \\ 63 \\ 63 \end{bmatrix} \oplus \begin{bmatrix} 00 \\ 00 \\ 00 \\ 00 \end{bmatrix} = \begin{bmatrix} 62 \\ 63 \\ 63 \\ 63 \end{bmatrix}$$

So first and key words are

$$w_0 = \begin{bmatrix} 62 \\ 63 \\ 63 \\ 63 \end{bmatrix}, w_5 = \begin{bmatrix} 62 \\ 63 \\ 63 \\ 63 \end{bmatrix}, w_6 = \begin{bmatrix} 62 \\ 63 \\ 63 \\ 63 \end{bmatrix}, w_7 = \begin{bmatrix} 62 \\ 63 \\ 63 \\ 63 \end{bmatrix}$$

For first round $w_8 = w_{10}$ & $w_3 = w_{11}$ firstly calculate for Round 2 by these steps

1.) Rotword

$$t = w_7 = \begin{bmatrix} 62 \\ 63 \\ 63 \\ 63 \end{bmatrix} \xrightarrow{\text{Rotword}} \begin{bmatrix} 63 \\ 63 \\ 63 \\ 62 \end{bmatrix}$$

2) SubWord

$$t = \begin{bmatrix} 63 \\ 63 \\ 63 \\ 62 \end{bmatrix} \xrightarrow{\text{SubWord}} \begin{bmatrix} FB \\ FB \\ FB \\ AA \end{bmatrix}$$

3) Applying RCON for second Round

$$\begin{bmatrix} FB \\ FB \\ FB \\ AB \end{bmatrix} \oplus \begin{bmatrix} 02 \\ 00 \\ 00 \\ 00 \end{bmatrix} = \begin{bmatrix} F9 \\ FB \\ FB \\ AB \end{bmatrix}$$

$\Rightarrow$ $FB \oplus 02 \Rightarrow 1111\ 1011 \oplus 0000\ 0010$

$\Rightarrow 1111\ 1010$

$\Rightarrow F9$

and $x \oplus 00 = k$

So $t_{z_{10}} = \begin{bmatrix} F9 \\ FB \\ FB \\ AB \end{bmatrix}$

words for Rand 2

$$w_8 = t_{2/8} \oplus w_4 = \begin{bmatrix} F9 \\ FB \\ FB \\ FB \end{bmatrix} \oplus \begin{bmatrix} 62 \\ 63 \\ 63 \\ 63 \end{bmatrix} = \begin{bmatrix} 9B \\ 98 \\ 98 \\ C9 \end{bmatrix}$$

$\Rightarrow$ F9 $\oplus$ 62 = 9B, 11111001 $\oplus$ 01100010 = 10011011 = 9B

$\Rightarrow$ FB $\oplus$ 63 = 98, 11111011 $\oplus$ 01100011 = 10011000 = 9B

$\Rightarrow$ FA $\oplus$ 63 = C9, 11101010 $\oplus$ 01100011 = 11001001 = C9

$$w_9 = w_8 \oplus w_5 = \begin{bmatrix} 9B \\ 98 \\ 98 \\ C9 \end{bmatrix} \oplus \begin{bmatrix} 62 \\ 63 \\ 63 \\ 63 \end{bmatrix} = \begin{bmatrix} F9 \\ FB \\ FB \\ FA \end{bmatrix}$$

if $a \oplus b = x$

then $x \oplus b = a$

as seen w_0 & w_5 are equal

do $t_{2(8)} \oplus w_0 \oplus w_5 = t_{2(8)}$

and

$$w_{10} = w_9 \oplus w_6 = \begin{bmatrix} F9 \\ FB \\ FB \\ FA \end{bmatrix} \oplus \begin{bmatrix} 62 \\ 63 \\ 63 \\ 63 \end{bmatrix} = \begin{bmatrix} 9B \\ 98 \\ 98 \\ C9 \end{bmatrix}$$

same as in w_{10}

and

$$w_{11} = w_{10} \oplus w_7 = \begin{bmatrix} 9B \\ 98 \\ 98 \\ C9 \end{bmatrix} \oplus \begin{bmatrix} 62 \\ 63 \\ 63 \\ 63 \end{bmatrix} = \begin{bmatrix} F9 \\ FB \\ FB \\ FB \end{bmatrix}$$

so $w_8 = w_{10}$ & $w_9 = w_{11}$ because of property of a xOR.

In Rand 1 all the words are same

$$w_0 = w_5 = w_6 = w_7$$

and

$w_8 = t \oplus w_4$ — (1)

$w_9 = w_8 \oplus w_5 = t \oplus w_0 \oplus w_5 = w_7$ [$\because w_0 = w_5$ & by xOR property $x \oplus b \oplus b = b$]

$w_{10} = w_9 \oplus w_6 = t \oplus w_4$ ($\because w_6 = w_4$) — (3)

$w_{11} = w_{10} \oplus w_7 = t \oplus w_0 \oplus w_7$

$= t$ ($\because w_0 = w_4$) — (4)

By equation ① & ③

$$w_8 = w_{10}$$

and by equation ② & ④

Ques2 Show that $SB(x_1 \oplus x_2) \neq SB(x_1) \oplus SB(x_2)$. If $x_1 = (57)$ and $x_2 = (A2)$. (6)

Ans $x_1 = 57 = 01010111$ (bitwise), $x_2 = A2 = 10100010$ (bitwise)

$x_1 \oplus x_2 = 11110101 = F5$

$LHS = SB(x_1 \oplus x_2) = SB(F5) = E6$

$RHS = SB(52) \oplus SB(A2) = 00 \oplus 3A = 3A$

$L.H.S \neq R.H.S$

$$SB(x_1 \oplus x_2) \neq SB(x_1) \oplus SB(x_2)$$

Ques3 Alice chooses AES-128 for encrypt the plain text using key $k = [11\ldots1]$ now determine the first key words & justify why w_8 = Compliment of w_{10} & w_9 = Compliment of w_{11}

Ans keys word

$$w_0 = \begin{bmatrix} FF \\ FF \\ FF \\ FF \end{bmatrix}, \quad w_1 = \begin{bmatrix} FF \\ FF \\ FF \\ FF \end{bmatrix}, \quad w_2 = \begin{bmatrix} FF \\ FF \\ FF \\ FF \end{bmatrix}, \quad w_3 = \begin{bmatrix} FF \\ FF \\ FF \\ FF \end{bmatrix}$$

1. Firstly calculate $t_{(10)}$ for first Round.

Rotword

$$t_{(10)} = w_3 = \begin{bmatrix} FF \\ FF \\ FF \\ FF \end{bmatrix} \xrightarrow{\text{RotWord}} \begin{bmatrix} FF \\ FF \\ FF \\ FF \end{bmatrix}$$

2. Sub Byte

$$t_{(10)} = \begin{bmatrix} FF \\ FF \\ FF \\ FF \end{bmatrix} \xrightarrow{\text{SubByte}} \begin{bmatrix} 16 \\ 16 \\ 16 \\ 16 \end{bmatrix}$$

3. Applying RCON for first Round

$$t_{(10)} = \begin{bmatrix} 16 \\ 16 \\ 16 \\ 16 \end{bmatrix} \oplus \begin{bmatrix} 01 \\ 00 \\ 00 \\ 00 \end{bmatrix} = \begin{bmatrix} 17 \\ 16 \\ 16 \\ 16 \end{bmatrix} \quad \because x \oplus 0 = x \text{ and } 16 \oplus 00 = 16$$

$16 \oplus 01 = 00010111 = 17$

finally $t(10) = \begin{bmatrix} 17 \\ 16 \\ 16 \\ 16 \end{bmatrix}$

first Round words are

$w_4 = t(10) \oplus w_0 = \begin{bmatrix} 17 \\ 16 \\ 16 \\ 16 \end{bmatrix} \oplus \begin{bmatrix} FF \\ FF \\ FF \\ FF \end{bmatrix} = \begin{bmatrix} E8 \\ E9 \\ E9 \\ E9 \end{bmatrix}$

$\because x \oplus FF = \bar{x}$

$\therefore 17 \oplus FF = \overline{17} = \overline{00010111} = 11101000 = E8$

$16 \oplus FF = \overline{16} = 00010110 = 11101001 = E9$

$w_5 = w_4 \oplus w_1 = t_1(4) \oplus w_0 \oplus w_1$ ($\because w_0 = w_1$, $\therefore x \oplus b \oplus b = x$)

$= f_1(4) = \begin{bmatrix} 17 \\ 16 \\ 16 \\ 16 \end{bmatrix}$

$w_6 = w_5 \oplus w_2 = t_1(4) \oplus w_2 = \begin{bmatrix} 17 \\ 16 \\ 16 \\ 16 \end{bmatrix} \oplus \begin{bmatrix} FF \\ FF \\ FF \\ FF \end{bmatrix} = \begin{bmatrix} E8 \\ E9 \\ E9 \\ E8 \end{bmatrix}$

$w_7 = w_6 \oplus w_3 = t_1(4) \oplus w_2 \oplus w_5$ ($\because w_2 = w_3$)

$\therefore x \oplus 6 \oplus 6 = x$

$= t_1(4)$

$= \begin{bmatrix} 17 \\ 16 \\ 16 \\ 16 \end{bmatrix}$

so find kword words are

$w_4 = \begin{bmatrix} E8 \\ E9 \\ E9 \\ E9 \end{bmatrix}$, $w_5 = \begin{bmatrix} 17 \\ 16 \\ 16 \\ 16 \end{bmatrix}$, $w_6 = \begin{bmatrix} E8 \\ E9 \\ E9 \\ E9 \end{bmatrix}$, $w_7 = \begin{bmatrix} 17 \\ 16 \\ 16 \\ 16 \end{bmatrix}$

Now let $t_2(8)$ is the first IV for second round so

$w_8 = t_2(8) \oplus w_4$ — (1)

$w_9 = w_8 \oplus w_5 = t_2(18) \oplus w_4 \oplus w_5$ — (2)

$$w_{10} = w_9 \oplus w_6 \quad -(3)$$

$$w_{11} = w_{10} \oplus w_7 \quad -(4)$$

and

$$w_8 \oplus w_5 = \begin{bmatrix} E8 \\ E9 \\ E9 \\ E9 \end{bmatrix} \oplus \begin{bmatrix} 17 \\ 16 \\ 16 \\ 16 \end{bmatrix} = \begin{bmatrix} FF \\ FF \\ FF \\ FF \end{bmatrix} \quad -(5)$$

$$w_6 \oplus w_7 = \begin{bmatrix} E8 \\ E9 \\ E9 \\ E9 \end{bmatrix} \oplus \begin{bmatrix} 17 \\ 16 \\ 16 \\ 16 \end{bmatrix} = \begin{bmatrix} FF \\ FF \\ FF \\ FF \end{bmatrix} \quad -(6)$$

$$w_4 = w_6 \text{ and } w_5 = w_7 \quad -(7)$$

By equator (2) & (5)

$$w_9 = t_2(8) \oplus \begin{bmatrix} FF \\ FF \\ FF \\ FF \end{bmatrix} = \overline{t_2(18)} \quad -(8)$$

$(\because x \oplus FF = \bar{x})$

By equator (3), (8) and (7)

$$w_{10} = \overline{t_2 18} \oplus w_6$$

$$\Rightarrow w_{10} = \overline{t_2(18)} \oplus w_4 \quad (\text{by equator (1)}) \quad -(9)$$

By equator (4), (7) & (9)

$$w_{11} = \overline{t_2(8)} \oplus w_4 \oplus w_7$$

$$\therefore w_4 \oplus w_7 = \begin{bmatrix} FF \\ FF \\ FF \\ FF \end{bmatrix}$$

$$\therefore w_{11} = \overline{t_2(18)} \oplus \begin{bmatrix} FF \\ FF \\ FF \\ FF \end{bmatrix} = t_2(8) \quad -(10)$$

By equation (1) & (9)

w_8 = Complement of w_{10}

By equation (8) & (10)

$$w_9 = \overline{w_{11}}$$

w_9 = Complement of w_{11}

Ques ④ Let the group $G = \{1, 2, 3, 4, 5, 6\}$ and check G is cyclic under multiplication modulo 7 with generator 3.

Ans Cyclic group are those group in which at least one exist such that the all subgroup of generate

But generator represent the whole group so

$G = [1, 2, 5, 0, 5, 6]$

i) G is a cyclic group with generator 3 then 3 must represent the entire group,

subgroup of g is:

$\langle 3 \rangle = \{3, 6, 2, 5, 1, 4, 0\}$

∴ generator 3 represent the entire group so G is a cyclic group

	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6
1	1	2	3	4	5	6	0
2	2	3	4	5	6	0	1
3	3	4	5	6	0	1	2
4	4	5	6	0	1	2	3
5	5	6	0	1	2	3	4
6	6	0	1	2	3	4	5

Q-5 If Alice always uses the same IV instead of different IVs for all communication with Bob. Which mode of operation (CBC Vs CTR) in block cipher is more secure against same IV and why?

Ans If Alice sends a message with IV two times (maybe more) by both CBC and CTR. so in IV same case these point describe reason.

1. If IV same then in CTR bitsream $(C_1, C_2 \ldots C_n)$ are same It does not depend on the planetext but in CBC the bitsream is depend on planetext. Hence for each plaintext CBC has different bit sheen.

(2) If Eve knows the plaintext and ~~ciphertext~~ ciphertext so in CTR it can easily find bitstream(c_1, p_1, p_n) by exoring both cipher and plaintext. Because bitstream is same (due to IV same) In all future plaintext Eve can easily find the plain text by exoring ciphertext with bitstream. But in case of CBC if Eve knows plaintext and ciphertext then it cannot determine key for finding future plaintext.

So by above points it clean find CTR is more secure than CBC.

Ques6 Let's consider the stream cipher RC4, but instead of the full 256 bytes, we will use state vector S is 8x3-bits. Encrypt a 3 bit plaintext P = [15 32] if we use a 4x3-bit key of K = [20 13]. Also show the process of key stream generator.

Ans RC4 is a byte oriented cipher. RC4 has several steps before cipher ~~encrypt~~ (initization, intial permutation, key generation process). As in question state is return of 8-bit. then

S = [0 1 2 3 4 5 6 7]

After this generate a vector T by seperated key bytes until T's get full. T has also key equal to state.

T = [2013 2013]

After this Initial permutation of state do by help of T.

Also of initial permutation is

Iterate i=0 t=0 to 8

j = (T + S[i] + [i])

Swap (S[i], S[j])

(a) First iteration i=0, j=0

j = (0+0+2) %8 = 2

Swap [S[0], S[2]) (state is = [2 1 0 3 4 5 6 7]

(c) Third iteration i=2, j=3

$i = (3 + 0 + 1) \% 8 = 4$

swap(s[2], s[4]) = (23410567)

(d) fourth iteration i=3, j=4

$j = (4 + 1 + 3) \% 8 = 0$

swap (s[3], s[0]) (state [13420567])

(e) fifth iteration i=4, j=0

$j = (0 + 0 + 2) \% 8 = 2$

swap (s[4], s[2]) (state is [13024567]

(f) sixth iteration i=5, j=2

$j = (2 + 5 + 0) \% 8 = 7$

swap (s[5], s[7]) (state is [13024765])

(e) seventh iteration i=6, j=7

$j = (7 + 6 + 1) \% 8 = 6$

swap (s[6], s[6]) (state is [13024765])

(h) Eight iteration $j = (6 + 5 + 3) \% 8 = 6$

swap (s[7], s[6]) (state [13024756])

After this key seed generation → start Algo of generation process

Our final state

S = [13024756]

Now generate key

(a) final iteration i=0, j=0

$i = (0 + 1) \% 8 = 1$

$j = (0 + 3) \% 8 = 3$

swap [s[1], s[3])

Iterate on the length of plaintext.

$i = (i + 1) \% 8$

$j = (i + S[i]) \% 8$

swap (s[i], s[j]).

$t = [s[i] + [s[j]] \% 8$

$k = s[t]$

(state is [12034756])

t = (2+3)%8 = 5

k = S[5] = 7 (k = [7])

(b) Second iteration i=1, j=3

i = (1+1)%8 = 2

j = (3+0)%8 = 3

Swap (S[2], S[3])

t = [3+0]%8 = 3 (state [12304756])

k = S[3] = 0 (k = [7, 0])

(c) Third iteration i=2, j=3

i = (2+1)%8 = 3

j = (3+0)%8 = 3

swap (S[3], S[3]) (state [12304756])

t = (0+0)%8 = 0

k = S[0] = 01 (k = [7, ⊕, ϕ])

(d) fourth iteration i=3, j=3

i = (3+1)%8 = 4

j = (3+4)%8 = 7

swap (S[4], S[7])

t = (6+4)%8 = 2 (state is [12306750])

k = S[2] = 3 (R = [7, 0, ϕ, 3])

So for length key = [7013]

After key generation encryption starts

plaintext = [1 5 32]

key = [7 0 1 3]

Cipher = Plaintext ⊕ key

C = [1⊕7, 5⊕0, 3⊕1, 2⊕3]

= [16, 5, 2, 1]

Ques 7. Find the value of x using Fermat's theorem when

$x^{85} = 6 \pmod{29}$

Ans

$x^{85} \equiv 6 \bmod (29)$

$(x^{28} \times x^{28} \times x^{29}) \bmod 29 \equiv 6 \bmod 29$

$(x^{28} \bmod 29) \times (x^{28} \bmod 29) \times (x^{29} \bmod 29) \equiv 6 \bmod 29$ — (1)

[By module multiplication law]

$a^{p-1} \bmod p \equiv 1 \bmod p$

and $a^p \bmod p = a \bmod p$ { by fermat's theorem }

∴ In equation (1)

$(1 \bmod 29) \times (1 \bmod 29) \times (x \bmod 29) \equiv 6 \bmod 29$

$\Rightarrow x \bmod 29 \equiv 6 \bmod 29$

By Comparing $x = 6$

so at $x = 6$ $x^{85} \equiv 6 \bmod (29)$

Q8) An integer gives remainders 3, 3, 0 on division by 7, 13, and 5 respectively. Find the integer value using Chinese remainder theorem.

Ans

$3 = x \bmod 7$

$0 = x \bmod 5$ $(m_1 = 7, m_2 = 13, m_3 = 5$ and $a_1 = 3, a_2 = 3, a_3 = 0)$

In chinese Remainder Theorem these are four steps

1. Calculate M

$M = m_1 \times m_2 \times m_3$

$M = 7 \times 13 \times 5 = 455$

$x = 3 \bmod 7$

$x = 3 \bmod 13$

$x = 0 \bmod 5$

$x \equiv a_i \bmod (m_i)$

$a_1 = 3$ $\quad m_1 = 7$

$a_2 = 3$ $\quad m_2 = 13$

$a_3 = 0$ $\quad m_3 = 5$

since 5, 7 & 13 all are prime to one another we can find x.

i.e. $\gcd(5,7) = \gcd(7,13) = \gcd(5,13) = 1$

$M = m_1 \times m_2 \times m_3 = 5 \times 7 \times 13 = 455$

$\boxed{M = 455}$

$M_1 = m_2 m_3 = 65$

$M_2 = m_1 m_3 = 35$

$M_3 = m_1 m_2 = 91$

Now we call x_i value

$M_1 x_1 \equiv 1 \pmod{m_1}$ i.e. $M_1 x_1 \pmod{m_1} = 1$

$65\ x_1 \pmod 7 = 1$

$2\ x_1 \pmod 7 = 1$

$\therefore \boxed{x_1 = 4}$

similarity $M_2 x_2 = 1 \pmod{m_2}$

$35\ x_2 \pmod{13} = 1$

$9\ x_2 \pmod{13} = 1$

$\therefore \boxed{x_2 = 3}$

III rd $M_3 x_3 = 0 \pmod{m_3}$

$91\ x_3 \bmod 5 = 0$

$1\ x_2 \bmod 5 = 0$

$\boxed{\therefore x_2 = 5}$

$a_1 = 3$ $a_2 = 3$ $a_3 = 0$

$m_1 = 7$ $m_2 = 13$ $m_3 = 5$

$X_1 = 4$ $X_2 = 3$ $X_3 = 5$

$M_1 = 65$ $M_2 = 35$ $M_3 = 91$

$M = 455$

$x = (m_1 X_1 a_1 + m_2 X_2 a_2 + m_3 X_3 a_3) \bmod M$

$= (65(4)(3) + (35 \times 3 \times 3) + (91 \times 5 \times 0)) \bmod M$

$= (780 + 315 + 0) \bmod 455$

$= 1095 \bmod 455$

$x = 185$

To verify

$185 \bmod 7 = 3$

$185 \bmod 13 = 3$

$185 \bmod 5 = 0$

Hence verified $x = 185$

(10) Cipher text = 10

Public key $= \{e, n\} = \{5, 35\}$

Encrypt $= C = m^e \bmod n$

Decrypt $= M = C^d \bmod n$

To find d

$d = e^{-1} \bmod \phi(n)$

$ed \bmod \phi(n) = 1$

$5 \times d \bmod \phi(35) = 1$

$\phi(35) = \phi(7) \times \phi(5) = 6 \times 4 = 24$

$5 \times d \bmod 24 = 1$

$\therefore d = 5$

In decryption

$$M = C^d \bmod n$$

$$M = 10^5 \bmod 35$$

$$M = 10^5 \bmod 35$$

$$\therefore M = 5$$