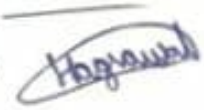
Declaration and statement of authorship

I, bearing Registration Number 106118036, agree and acknowledge that:

1. The assessment was answered by me as per the instructions applicable to each assessment, and that I have not resorted to any unfair means to deliberately improve my performance.

2. I have neither impersonated anyone, nor have I been impersonated by any person for the purpose of assessments.

Signature of the Student : 

Full Name : Harshit Agrawal

Roll No. : 106118036

Sub Code : CSPC 35

Mobile No. : 7016004637

10/5/21

CSPC36 - POC

106118036

1) Fermat's theorem $\Rightarrow$ $a^{p-1} \bmod p = 1 \bmod p$

↓

Prime number.

2) Now, given $X = 9794 \bmod 73$

and we need to find 'a' for $a \equiv 0..72$

$\therefore 9794 \,\%\, 73 = \underline{12}$

$\therefore \boxed{a = 12}$ $\Rightarrow$ Ans

3) GCD (400, 60) : Extended Euclidean Theorem.

a b

So, we write the following table to calculate the GCD.

q	r_1	r_2	r	s_1	s_2	s	t_1	t_2	t
6	400	60	40	1	0	1	0	1	-6
1	60	40	20	0	1	-1	1	-6	7
2	40	(20)	0	1	(-1)	3	-6	(7)	-20

$\therefore$ GCD = 20
s = -1
t = 7
} Answer

Verification :> $400 \times -1 + 60 \times 7 = \underline{20}$ ✓

c) CRT → Chinese Remainder Theorem.

→ The CRT states that if one knows the remainders of the Euclidean division of an integer 'n' by several integers, then one can determine uniquely the remainder of the division of 'n' by the product of these integers, under the condition that the divisors are pairwise coprime.

→ Mathematically,
Let $m_1, \ldots, m_n$ be pairwise coprime (that is $\gcd(m_i, m_j) = 1$). Then the system of 'n' equations

$$x = a_1 \pmod{m_1}$$
$$\vdots$$
$$x = a_n \pmod{m_n}$$

has a unique sol" for 'x' modulo M, where
$M = m_1 * m_2 * \ldots * m_n$.

Proof:-
Let $b_i = M/m_i$ & $b_i' = b_i^{-1} \pmod{m_i}$
then,

$$x = \sum_{i=1}^{n} a_i b_i b_i' \pmod{M}$$

→ Applications:
- FFT (fast fourier transform)
- Encryption (RSA)
- Rabin Crypto System to find $P_1 P_2 P_3 P_4$.

2) Cipher → Vigenere
Key → Random(0, 26)

i)

P → s e n d m o re m o n e y
K → 9 0 1 7 23 15 21 14 11 11 2 8 9

C → b e o k j d m s x z p m h

Answer

ii) Now, using 'C' from (i), we need to find key 'K' such that P becomes as follows

P → c a s h not needed

C → b e o k j d m s x z p m h

Now, $K_i = (C_i - P_i + 26) \% 26$

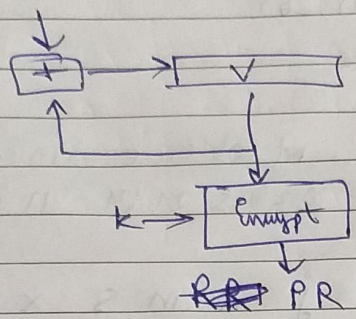
∴

K → 25, 4, 22, 3, 22, 15, 19, 5, 19, 21, 24, 8, 4

Answer

b) PRNG mechanisms based on block ciphers.

(i) CTR mode (Counter Mode)

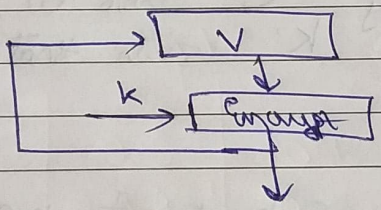


→ Recommended in SP800-90.

→ The value of 'V' is incremented by 1 after each encryption.

→ Strong security compared to OFB.

ii) OFB mode.



→ Recommended in RFS 4086

→ Value of 'V' is updated to equal the value of preceding PRNG.

→ It is weak security wise compared to CTR Mode.

3.
a)

b)

3) a) The round key generator creates 16, 48-bit keys out of a 56-bit cipher key. However, the cipher key is normally given as a 64-bit key in which 8 extra bits are the parity bits.

→ To remove the parity bits and create a 56-bit cipher key, a parity drop permutation is required. This done before key expansion in a compression-transposition step.

→ It not only drops the parity bits, but also permutes the rest of the bits, thereby adding another layer of permutation to it to increase the encryption.

b) For GF(x) to be a valid Galois Field, 'x' needs to be a power of the prime.

$$x = p^n \quad ; \quad p \Rightarrow \text{prime}.$$

Now, GF(17), $x = 17$

where, $17 = 17^1$, where 17 is a prime number.

Hence, valid GF.

3.)

a) i) Writing a 4x4 matrix,

00	04	08	0C
01	05	09	0D
02	06	0A	0E
03	07	0B	0F

ii) After the initial AddRoundKey here, each byte of the state is combined with a byte of the round key using bitwise XOR.

Hence, we get

01	05	09	0D
00	04	08	0C
03	07	0B	0F
02	06	0A	0E

iii) After the SubBytes procedure, therefore we get

7C	6B	01	D7
63	F2	30	FE
7B	C5	2B	76
77	6F	67	AB

iv) After performing the ShiftRows operation, we get

7C	6B	01	D7
F2	30	FF	63
2B	76	7B	C5
AB	77	6F	67

v) After performing MixColumns, we get

75	87	0F	A2
55	E6	04	22
3E	2E	B8	BC
10	15	58	0A

4)

a) A trapdoor one-way function is a one-way function with an additional requirement. Informally, a one-way function might be described as a function for which evaluation in one-direction is straightforward, while computation in the reverse direction is a far more difficult job.

→ Informally, a function $f: \{0,1\}^{f(n)} \times \{0,1\}^{n} \to \{0,1\}^{m(n)}$ is a trapdoor one-way function if:-

- It is a one-way function.

- For a fixed public key, $y \in \{0,1\}^{s(n)}$ $f(x,y)$ is viewed as a function $f_y(x)$ of x that map n bits to $m(n)$ bits. Then there is an efficient algorithm that, on input $\{y, f_y(x), z\}$ produces x' such that $f_y(x') = f_y(x)$ for some trapdoor key $z \in \{0,1\}^{k(n)}$

b) Given details, we have

$e = 31$, $n = 3599$

Now, $n = p \times q = 3599 = 59 * 61$

$\phi(n) = 58 * 60$

$\boxed{\phi(n) = 3480}$

Now, $e = 31$

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

$= (31)^{-1} \bmod (3480) = \underline{3031}$

$\therefore$ $\boxed{\text{Private key } (d) = 3031}$ Ans

c) Given,

$q = 2579$ (p)

$\alpha = 2$ (e_1)

$x_B = 7$ (d)

$M = 1299$ (m)

$k = 853$ (K)

Now, $e_2 = e_1^d \bmod q = 2^7 \bmod 2579 = 128$

Now,

$$C_1 = e_1^{*K} \bmod q$$

$$= 2^{853} \bmod 2579 = \boxed{435}$$

$$C_2 = (m * e_2^K) \bmod q$$

$$= (1299 * (128)^{853}) \bmod q$$

$$\boxed{C_2 = 696}$$

Hence, Encrypted $[C_1, C_2] = [435, 696]$

Now, in decryption,

$$M = [C_2 * (C_1^d)^{-1}] \bmod q$$

$$= \{696 * [(435)^7]^{-1}\} \bmod 2579$$

$$\boxed{M = 1299}$$

5.)

a)

HMAC	CMAC
• Hash based message authentication code.	• Block ciphers based authentication code algorithm.
• Resistant towards cryptanalysis attacks since hashing is used twice	• Provides authenticity and integrity of data.
• Faster than CMAC because hash functions are faster.	• Slower than HMAC as block ciphers are slower.

b) Hash functions:-

- Digital data is mapped to a fixed data size using hashing functions.
- Slight differences in the input data produce large differences in the hashed data (Avalanche effect).
- Principles involved in hashing.
  - Sequence of n-bit blocks is used for analysis
  - at a time, one input block is processed at a time to produce an n-bit hash function.
  - Example of a simple hash is XOR.

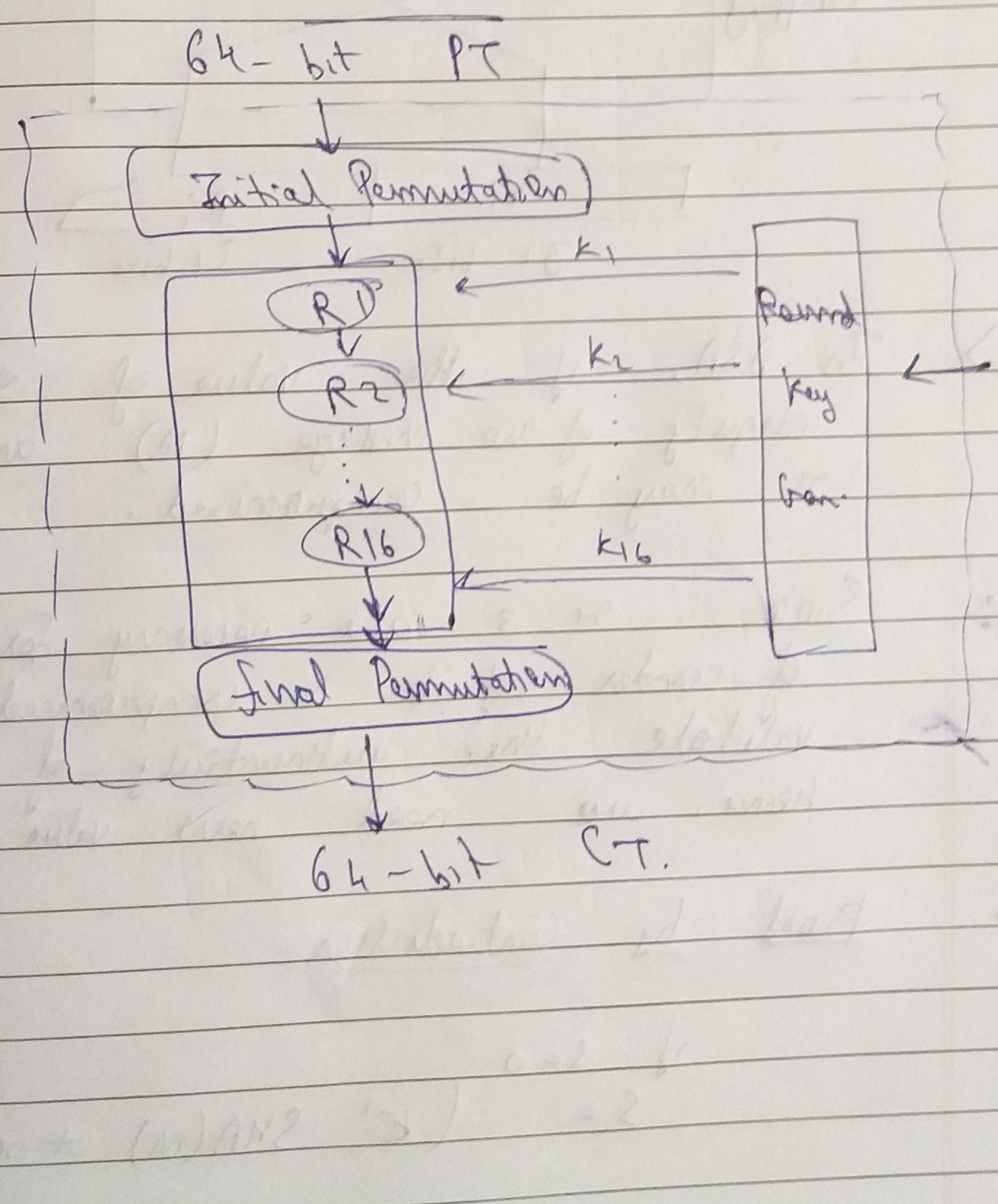
→ Using hash functions to construct block ciphers.

- One round of DES can be described as

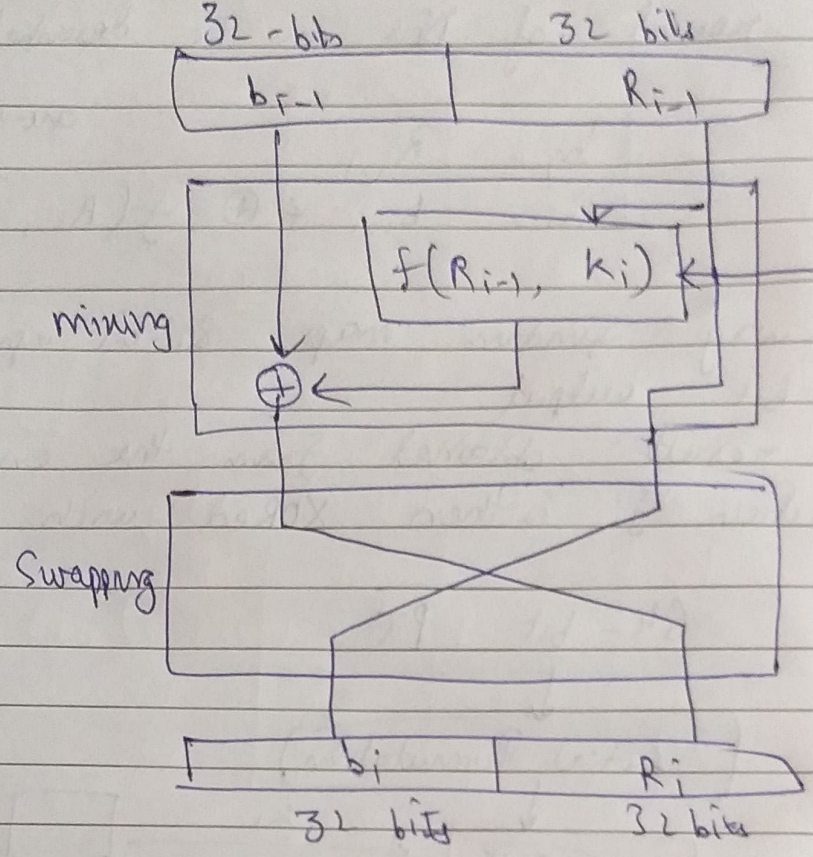
$$b_i = R_{i-1}$$
$$R_i = b_{i-1} \oplus f(R_{i-1}, k_i)$$

one-way function.

- One-way function maps 80-bit input to a 32-bit output.
- The result obtained from the one-way function 'f' is then XORed with b_{i-1} bitwise.



- Single Round in DES.



c) In DSA, if the value of $S=0$, the integrity of the message (M) and value of 'r' may be compromised.

- Since r, s are necessary for authentication of sender, if it is compromised, we cannot validate the authenticity of message 'M'. Hence, we need new value of 'k'.

- Proof by Contradiction:-

if $S=0$

$S = (k^{-1} SHA(M) + x.r) \bmod$

$\therefore \quad (K^{-1} \cdot SHA(M) + x \cdot r) = 0$

Hence, it is a multiple of 'q'.

Now, as it is a multiple, we can use trial and error can be performed and the time complexity is no longer valid.

$\therefore$ The system can be hacked into.