Register Number | | | | | | | | | |

Sri Sivasubramaniya Nadar College of Engineering, Kalavakkam – 603 110

(An Autonomous Institution, Affiliated to Anna University, Chennai)

Department of Computer Science and Engineering

Continuous Assessment Test– II

Question Paper

Degree & Branch	B.E CSE				**Semester**	V
Subject Code & Name	UCS1505 - INTRODUCTION TO CRYPTOGRAPHIC TECHNIQUES				**Regulation: 2018**	
Academic Year	2020-21	**Batch**	2018-22	**Date**	**29.9.20**	**FN**
Time: 90 Minutes	**Answer All Questions**				**Maximum: 50 Marks**	

Part – A Answer all the questions (10×2 = 20 Marks)
(MCQ type –Randomly post 10 questions to the student)

<KL2>	1.) Which of the following is used for authenticating a message in SSL? a) Message Arbitrary Code b) Machine Authentication Code c) Machine Access Cipher **d) Message Authentication Code**	<CO2>
<KL2>	In CBC MAC, if the message length is not a multiple of cipher block length a) A new block with a length accommodating all the message bits is added. b) The remaining of block is padded with 1. c) Message bits that exceed the nearest multiple are discarded. **d) The remaining of block is padded with 0.**	<CO2>
<KL2>	Which of the following is /are offered by the Hash functions? a) Authentication b) Non repudiation c) Data Integrity **d) All of the above**	<CO2>
<KL2>	Which of the following options are correct according to the definition of the Hash Function? a) Hash Functions are mathematical functions b) They compress the input values c) The hash functions work on arbitrary length input but produces fixed length output. **d) All of the above**	<CO2>
<KL2>	What is the value of opad in the HMAC structure in hexadecimal? a) 3E b) 32 c) B6 **d) 5C**	<CO2>
<KL2>	Let H be a hash function, for two distinct messages x and x1, if H(x)=H(x1) then this is called a) perfect secrecy b) MAC generation **c) collision** d) encryption	<CO2>
<KL2>	Which of the following is a reasonable combination of encryption scheme and a secure message authentication code a) Encrypt-and-authenticate b) Authenticate-then-encrypt	<CO2>

	c) Encrypt-then-authenticate **d) All of the Above**	
<KL2>	The DES Algorithm Cipher System consists of _____rounds (iterations) each with a round key a) 12 b) 18 c) 9 **d) 16**	<CO2>
<KL2>	In the DES algorithm the round key is _____ bit and the Round Input is _____bits. **a) 48, 32** b) 64,32 c) 56, 24 d) 32, 32	<CO2>
<KL2>	The number of unique substitution boxes in DES after the 48 bit XOR operation are **a) 8** b) 4 c) 6 d) 12	<CO2>
<KL3>	A MAC function compresses two long distinct inputs of length l1 and l2 and produces output of length n1,n2 then which of the following is true? a) n1>n2 b) n1<n2 **c) n1=n2** d) n1!=n2	<CO3>
<KL3>	A transmits c1(encryption of m1) and subsequentially c2(encryption of m2) to B. You has some control over network and deliver c2 before c1 which causes mismatch between A and B and you send back c1 to A and then send c1 again to B. What are the attacks you have done and mention them in order? a) Reordering, Replay, Reflection b) Replay, Reflection, Reordering **c) Reordering, Reflection, Replay** d) Reordering, Replay, Reflection	<CO3>
<KL3>	In a substitution permutation network given a input of 16 bits what are the following sequences performed for 2 rounds? **a) sub key k1 mixing with given Input, substitution, permutation, output1** **sub k2 mixing with output 1, substitution, permutation** b) sub key k1 mixing with given Input, substitution, permutation, output1 sub k2 mixing with given Input, substitution, permutation c) sub key k1 mixing with given Input, permutation, substitution, output1 sub k2 mixing with output 1, permutation, substitution	<CO3>
<KL3>	For an m bit hash value, if we pick data blocks at random, we can expect to find two data blocks with the same hash value within ____ attempts. a) 2^m b) 2^(m-1) **c) 2^(m/2)** d) (2^m) – 1	<CO3>
<KL3>	In HMAC algorithm which of the following holds true? MD – Message Digest, H- Hash function, Si – Input signature, So – Output signature, M- Input Message, || - padding or concatenation a) MD= H(Si || H(So || M)) b) MD= H(Si || M) || H(So || M) **c) MD= H(So || H(Si || M))** d) None of the above	<CO3>
<KL3>	What is the correct order of the following statements in producing the message digest using HMAC algorithm starting with the message bits? 1. Temporary message digest is produced. 2. Left pad the input signature with message bits. 3. Hash the result using hash function H. (This statement can be used more than once) 4. Temporary digest is padded with output signal.	<CO3>

	5. Message Digest is produced a) 2->3-> 5-> 4-> 3-> 1 **b) 2-> 3-> 1-> 4-> 3-> 5** c) 2-> 5-> 3-> 4-> 3-> 1 d) None of the above	
<KL3>	Consider an SPN with 64 bit block length based on collection of 8 bit S boxes (S1,….,S8). Fill the following blank Key mixing: Set x :=_____, where k is the current-round sub-key; Substitution: Set x := _____where xi is the i th byte of x; Permutation: Permute the bits of x to obtain the output of the round. **a) x EXOR k, S1(x1)|| • • • ||S8(x8)** b) x EXOR x, S1(x1)|| • • • ||S10(x10) c) x EXOR x, S1(x1)|| • • • ||S8(x8) d) x EXOR k, S0(x0)|| • • • ||S8(x8)	<CO3>
<KL3>	For an n-bit tag and a k-bit key, the level of effort required for brute force attack on a MAC algorithm is a) 2^k b) 2^n c) min(2^k,2^n) d) 2^k/2^n	<CO3>
<KL3>	AES uses a _____ bit block size and a key size of _____ bits. a) 128; 128 or 256 b) 64; 128 or 192 c) 256; 128, 192, or 256 **d) 128; 128, 192, or 256**	<CO3>
<KL3>	For the AES-128 algorithm there are _____ similar rounds and _____ round is different. a) 2 pair of 5 similar rounds ; every alternate **b) 9 ; the last** c) 8 ; the first and last d) 10 ; no	<CO3>

Part – B Answer all the questions (2×5 = 10 Marks)

<KL3>	1 a. Give an example what is vrfyk(m,t) in MAC algorithm. (2) b. When m=2 bits, t=2 bits, k=2 bits, List all the possible m,t and k.(2) c. What is meant by oracle in the context of adversary. (1)	<CO3>
<KL2>	2. a. What is avalanche effect. (2) b.How to derive sub-keys from master key. Give an example. (2) c. What is meant by one round in feistel network? (1)	<CO2>

Part – C Answer any TWO questions (2×10 = 20 Marks)

<KL3>	3 a. With m=2 bits, t=2 bits, what is meant by unforgery?(1) b. Draw a flowchart combining Mac-forgeA,π and Mac(Gen, Mac, Vrfy) scheme. (3) c. What is chosen message attack and adaptive chosen message attack in the context of adversary? Which one is best for him?(2) d. Give a scenario validating the Mac-sForge scheme.(2) e. if k=3 bits, T=4 bits, M=8 bits. For T=1110, M=10110110, what is meant by brute force attack on MAC.(2)	<CO3>
<KL3>	4 a. List out all combination of message tag pair if T=2, M=4 bits. How many repetition you can find? (1) b. Give some sample data for the following scheme. (3)	<CO3>

	• Mac: on input a key $k \in \{0,1\}^n$ and a message m of length $\ell(n) \cdot n$, do the following (we set $\ell = \ell(n)$ in what follows): 1. Parse m as $m = m_1, \ldots, m_\ell$ where each m_i is of length n. 2. Set $t_0 := 0^n$. Then, for $i = 1$ to ℓ: Set $t_i := F_k(t_{i-1} \oplus m_i)$. Output t_ℓ as the tag. c. What are the cases CBC - MAC is secure and when it is not secure. (2) d. What is collision and collision resistent ? Give an example (2) e. How is it possible to forge a valid tag by adversary ? (2)	
<KL2>	5. a. What is meant by Inverting a Feistel network ? (2) b. List out the procedure in one round DES function. (2) c. In what cases DES is more vulnerable to attacks? (2) d. Give two differences of AES and DES (2). e. What are weak keys in DES? (2)	<CO2>

Prepared By	Reviewed By	Approved By
Course Coordinator	PAC Team	HOD

29/09/20

NAME : VANATHI. G

CLASS : CSE-C

REG NO : 185001188

SUB : UCS1505 - Introduction to Cryptographic Techniques

EXAM : CAT - 2

PART-C

③

(a) * Definition of unforgeable:

$\Pi = (Gen, Mac, Vrfy)$ is existentially unforgeable if

$Pr[Mac\text{-}forge_{A,\pi}(n) = 1] \leq negl(n)$

where A → PPT adversary, $negl(n) \cong 1/2^{80}$

* Since m is 2 bits long, $m \in \{00, 01, 10, 11\}$ and after $t = Mac_k(m)$, t is also 2 bits long. This means $t \in \{00, 01, 10, 11\}$

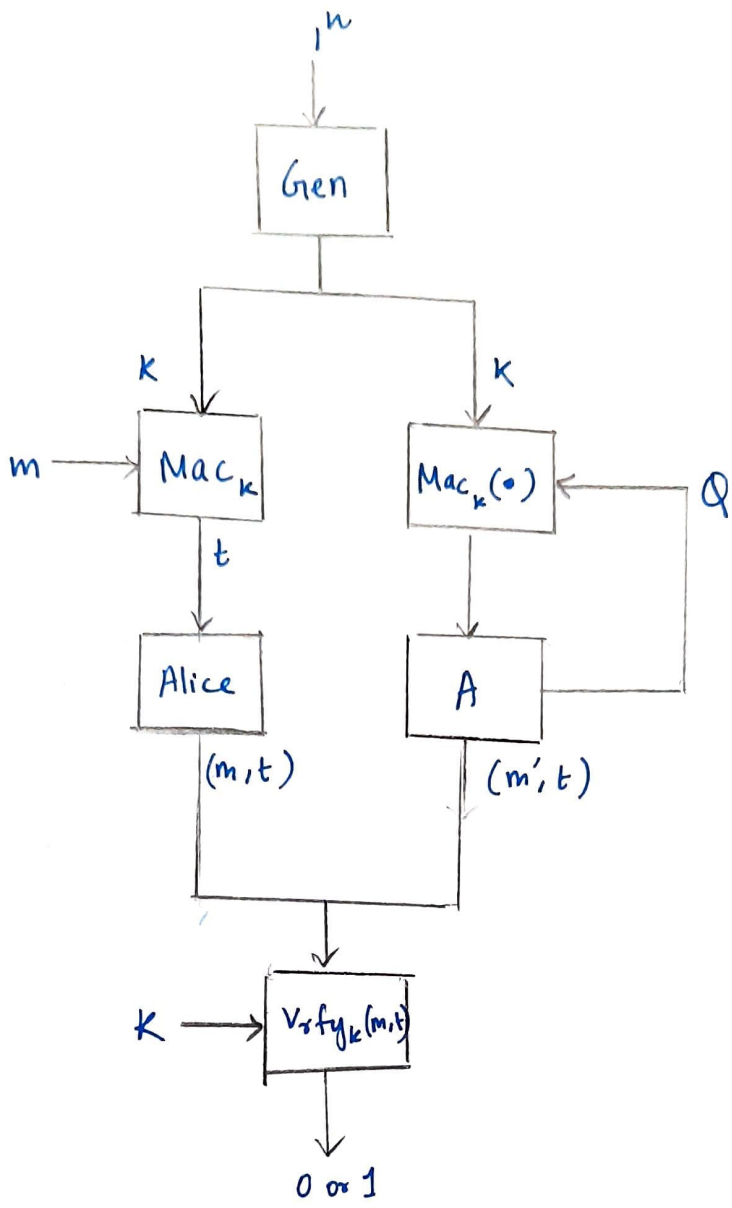
* If we assume each 'm' is uniquely mapped to a 't' i.e, there are no collisions, the adversary cannot forge a valid tag on another message m' of his choice. (no t exists such that $Vrfy_k(m', t)$ succeeds)

* Therefore, for $m = 2$ x $t = 2$, (assuming unique mappings) the MAC is unforgeable.

(b) * Let $\Pi = Mac(Gen, Mac, vrfy)$

Let A be the adversary.

* $Mac\text{-}forge_{A,\Pi}(n)$ is a randomized experiment & the probability of A winning this should be negligible



→ In the above diagram, Alice is the sender & 'A' is the adversary.

→ Both Alice & A know the key 'k' by running Gen(1^n)

→ Alice uses usual Mac procedure (Gen, Mac, Vrfy) to produce tag 't' & sends it along with m to Bob

→ The adversary has a set of messages (Q or queries) and an oracle $Mac_k(\cdot)$. Based on his observations, he generates m' (new message) with same tag t

→ A succeeds if $Vrfy_k(m', t) = 1$

(c) ★ In a chosen message attack, the adversary can obtain ciphertexts for arbitrary plaintext messages

★ In an adaptive chosen message attack, the adversary can request ciphertexts of more plaintexts after making observations of ciphertexts for some plaintexts

★ Here, the ciphertext is basically the tag. The oracle is a blackbox where the adversary can give any message to it & get the hash value (tag)

★ Here, adaptive chosen message attack is used because the adversary wants to infer something from the Oracle's outputs to forge tags for his own messages

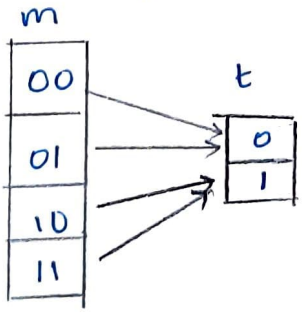
---

(d) ★ Consider a situation where m = 2 bits & t = 1 bit

★ In this case, $m \in \{00, 01, 10, 11\}$ and $t \in \{0, 1\}$

★ One tag $t' \in t$ is definitely mapped to more than one message 'm' (collisions)

★ If the hashing is as follows for a key 'k'



then the

$$Pr[Mac\text{-}forge_{A,\Pi}(n) = 1] = 0.5$$

★ Basically, Probability of winning = $\frac{1}{2^n}$ where n is output size

⇒ here $\frac{1}{2^1} = 0.5$. Therefore the adversary wins 50% of the time

∴ The Mac is not existentially unforgeable as the probability of winning by A is non-negligible

(e) ★ Given,

$k = 3$ bits

$t = 4$ bits

$M = 8$ bits

★ For $T = 1110$

$M = 10110110$

★ Brute-force attack:

→ Since we know one T & M pair, ~~we use key 'k' to compute~~ compute the 4-bit MAC on known message (M) for all possible keys

→ Atleast one key will produce the correct MAC (we can verify using T). 2^k combinations i.e 8 combinations were tried in this case

→ Now, we have the key 'k' and one T & M pair. Since M = 8 bits & t = 4 bits, collisions are definitely present so we can generate more m' using k & MAC algorithm such that m' has the same tag.

(5)

(a) Inverting a Feistel Network:

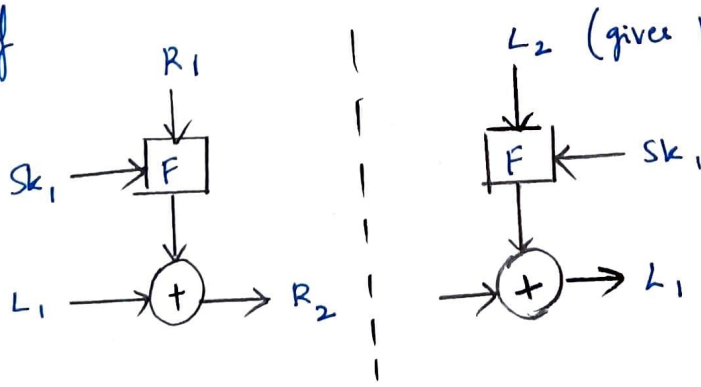
→ We basically do the encryption steps again but in reverse order

→ If the subkeys are $Sk_1 \ldots Sk_{16}$,

- 1st round with Sk_{16} undoes the 16th round of encryption
- Similarly perform in reverse order until 16th round of decryption with Sk_1 undoes the 1st encryption round

→ Note that during encryption, we encrypt only left half of the input & right-half is used in 'F' & copied over to left-half of output

→ Therefore, while inverting the Feistel network, we can use left-half of ciphertext to decrypt the right half



(b) ★ One round of DES consists of the following operations:

→ Split input into 2 halves L_i & R_i (32 bits each)

→ $L_i = R_{i-1}$

$R_i = L_{i-1} \oplus F(R_{i-1}, K_i)$

→ F takes 32-bit R_i as input & 48-bit subkey as input :

(i) E-box (Expansion box)

- provides diffusion
- expands R from 32-bits to 48-bits by copying certain bits twice

(ii) X-OR with subkey (to add basically)

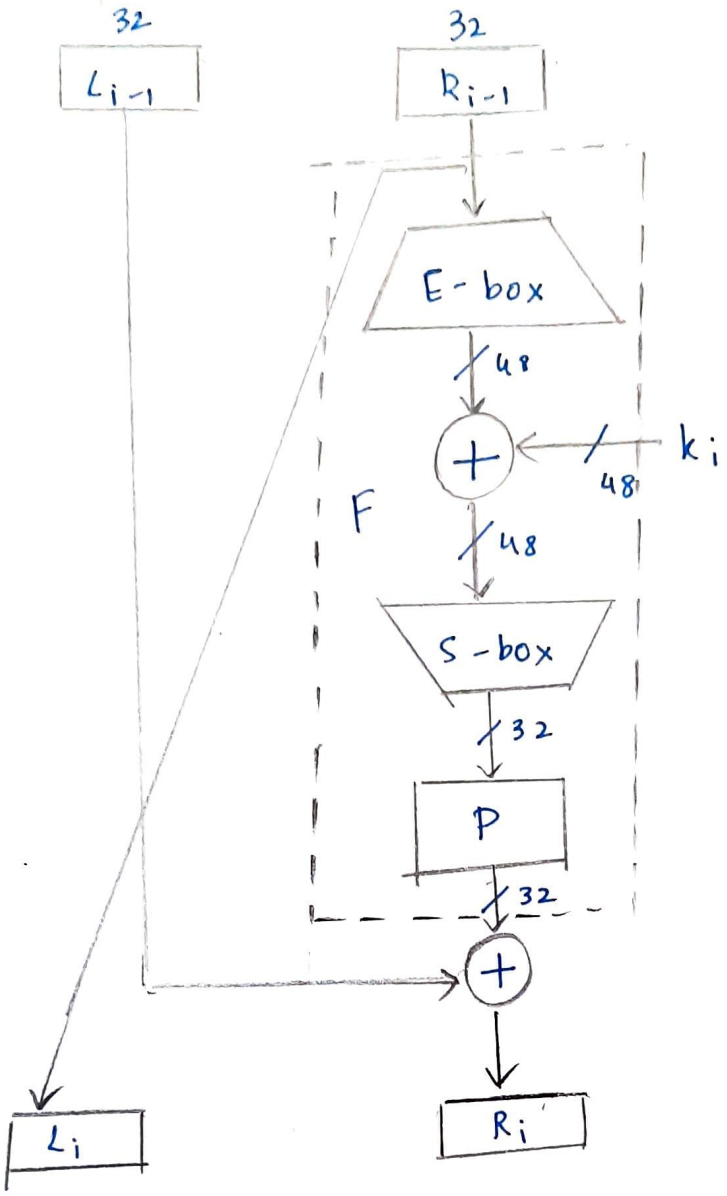
(iii) S-boxes (Substitution boxes)

- provide confusion
- the 48-bits are split into 8 groups of 6-bits & sent to 8 different S-boxes
- In each S-box, first & last bit of input (6-bits) is used to select row and middle 4-bits are used to select column
- The value at (row, col) in S-box is given as output (4-bits)
- Therefore we get 8 sets of 4-bits i.e, 32-bits as total output from this round

(iv) P- Permutation

- provides diffusion again
- It is just a 32-bit permutation performed using a table

→ Finally the output of F is ~~given as L_i~~ X-ORed with L_{i-1} and given as output R_i. R_{i-1} is given as output L_i from the network



(c) Vulnerabilities of DES:

(i) Brute-force attack -

Every key combination is tried until correct one is found & then we can decrypt the cipher. Only 2^{64} possible combinations for key is there.

(ii) More powerful attacks -

Differential cryptanalysis & Linear cryptanalysis can break DES using chosen plaintexts; not as practical as brute force attacks

(d)

DES	AES
→ Works on the Feistel network structure	→ works on SP principle to create confusion & diffusion
→ 16 rounds	→ 10, 12, 14 rounds depending on key size
→ Data block is divided into two halves & encrypted	→ All the bits are encrypted at once (as a block)

(e) ★ Weak keys -

→ In the DES algorithm, we do a fixed no. of left shifts for each round; in total after 16 rounds, 28 shifts are performed for each half of subkey

→ Now, if either half of the subkey is all 0s or all 1s i.e, $k_L = 0^{28}$ & $k_R = 0^{28}$ or $k_L = 0^{28}$ & $k_R = 1^{28}$ $k_L = 1^{28}$ & $k_R = 0^{28}$ or $k_L = 1^{28}$ & $k_r = 1^{28}$ then the rotations have no effect & all subkeys will be the same

→ Therefore these four keys are weak keys.

PART - B

(1)

(a) $Vrfy_k(m, t)$ is the verification algorithm that takes key k, message m & tag t as input & outputs 1 if t is valid. This is done at the receiver's side

Ex : Assume $k = 00$ hashes $m = 1101$ to $t = 0010$

$Vrfy_k(m, t)$ where $m = 1101$ & $t = 0010$ with the same k would output 1 in this case

~~If t was 0011 for instance,~~

If an adversary modified m to $m' = 1001$,

$Vrfy_k(m', t) = 0$ (invalid)

(b)

m_1	m_0
0	0
0	1
1	0
1	1

m

t_1	t_0
0	0
0	1
1	0
1	1

t

k_1	k_0
0	0
0	1
1	0
1	1

k

(c) → The oracle denoted as $Mac_k(\cdot)$ is a blackbox where the adversary can give a set of Messages (M) and get the tag values for $m \in M$

→ The oracle enables the adversary to carry out an adaptive chosen message attack where the adversary can forge tags based on inferences he makes from outputs of the oracle

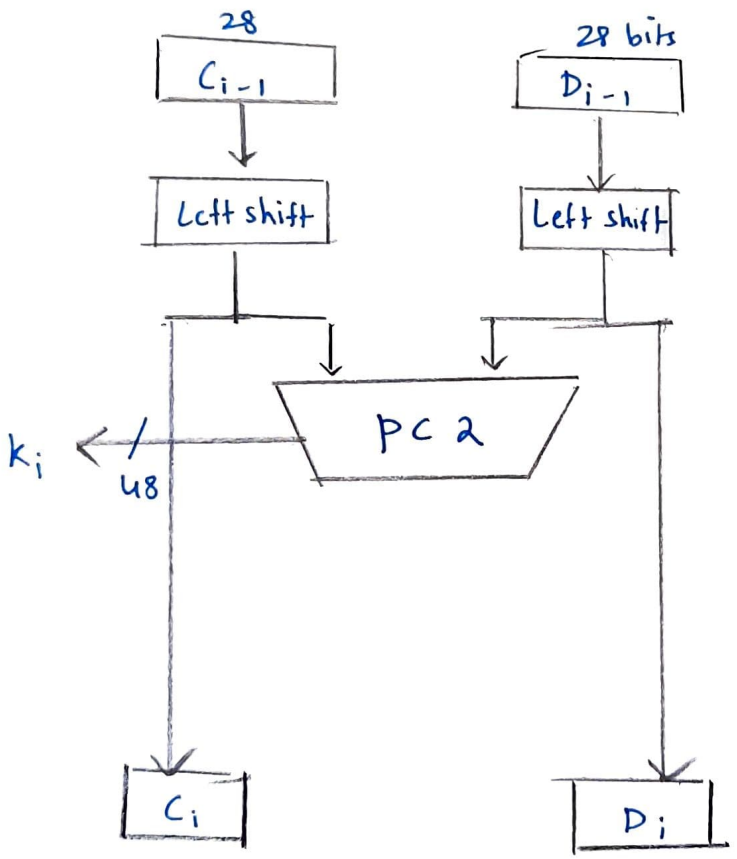
(a) ★ Avalanche effect :

A change of one input bit / key bit should result in a change of approximately half of the output bits

★ This is a very desirable property of encryption algorithms to prevent guessing keys, inferring something about plaintext from ciphertext difficult etc.

★ In DES, the S-boxes & E-box contribute to avalanche effect

(b)



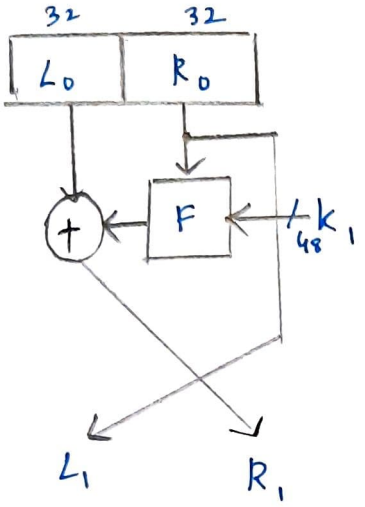
→ The initial permutation is split into two 28-bit halves L & R

→ In each stage,

- L & R are rotated (indiv.) 1/2 places based on key schedule

- 24 - bits from each half are selected & permutated by PC2
- L & R are combined & sent to F as subkey

(C)



→ One round consists of splitting the input into L_i & R_i

→ Then sending R_i & k_i (subkey) to function 'F' to generate some intermediate value

→ Encrypt L_i by doing X-OR with output of F

→ Send R_i as L_{i+1} & output of X-OR as R_{i+1}