CNS Important Questions FOR CIE-1

1.Illustrate a brief note on security goals.
Ans:

10 Illustrate a brief note on security goals.

Security Goals :-

There are three security goals : confidentiality, integrity and availability.

Confidentiality :-

Confidentiality is probably the most common aspect of information security. We need to protect our confidential information. An organization needs to guard against those malicious actions that endanger the confidentiality of its information. In the military concealment of sensitive information is the major concern. In banking, customers accounts need to be kept secret. Confidentiality not only applies to the storage of the information, it also applies to the transmission of information. When we send a piece of information to be stored in a remote computer or when we retrive information from a remote computer, we need to conceal it during transmission

Integrity :-

Information needs to be changed constantly. F a bank when a customer deposits or withd money, the balance of her account needs to b changed. Integrity means that changes need to be done only by authorized entities. Information is ~~useless if it is not available~~ and through au rized mechanisms. Integrity violation is not necessaril the result of a malicious act ; an interruption the system, such as power surge, may also creat unwanted changes in some information.

Availability :-

The third component of information security is Availability. The information created and stored by an organization needs to be available to authorized entities. Information is useless if it is not available. Information needs to be constantly changed which means it must be accessible authorized entities. The unavailability of information is just as harmful for an organization as the lack of confidentiality or integrity. Imagine what would happen to a bank if th customers could not access their accounts for transactions.

active and passive ~~act~~ attacks in

2.Apply the extended Euclidean algorithm, find the greatest common divisor of the following pairs and the value of s and t.

a) 4 and 7
b) 291 and 42
c) 84 and 320
d) 400 and 60

Ans:

4 and 7

Given $a = 7$, $b = 4$

Using Extended Euclidean Algorithm :-

q	r_1	r_2	r	s_1	s_2	s	t_1	t_2	t
1	7	4	3	1	0	1	0	1	-1
1	4	3	1	0	1	-1	1	-1	2
3	3	1	0	1	-1	4	-1	2	-7
×	(1) gcd	0	×	(-1)	4	×	(2)	-7	×

We assume that $s_1 = 1$, $s_2 = 0$, $t_1 = 0$, $t_2 = 1$

$s = s_1 - s_2 \times q$

$t = t_1 - t_2 \times q$

We get $\gcd(7, 4) = 1$, $s = -1$, $t = 2$

$(-1)7 + (2)4 = 1$ //

291 and 42.

Given $a = 291$, $b = 42$.

Using Extended Euclidean Algorithm :-

q	r_1	r_2	r	s_1	s_2	s	t_1	t_2	t
6	291	42	39	1	0	1	0	1	-6
1	42	39	3	0	1	-1	1	-6	7
13	39	3	0	1	-1	14	-6	7	-97
×	(3) gcd	0	×	(-1) s	14	×	(7) t	-97	×

We get $\gcd(291, 42) = 3$, $s = -1$, $t = 7$

$(-1)291 + 7(42) = 3$ //

c) 84 and 320

Given $a = 320$, $b = 84$

By Extended Euclidean Algorithm,

q	r_1	r_2	r	s_1	s_2	s	t_1	t_2	t
3	320	84	68	1	0	1	0	1	-3
1	84	68	16	0	1	-1	1	-3	4
4	68	16	4	1	-1	5	-3	4	-19
4	16	4	0	-1	5	-21	4	-19	80
x	(4) gcd	0	x	(5) s	-21	x	(-19) t	80	x

We assume that $s_1 = 1$, $s_2 = 0$, $t_1 = 0$, $t_2 = 1$

We get $\gcd(320, 84) = 4$, $s = 5$, $t = -19$

$\because 5(320) + (-19)84 = 4$ //

d) 400 and 60

Given $a = 400$, $b = 60$

By Extended Euclidean Algorithm,

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
x	(20) gcd	0	x	(-1) s	3	x	(7) t	-20	x

We get $\gcd(400, 60) = 20$, $s = -1$, $t = 7$

$\because (-1)400 + 7(60) = 20$ //

3.Examine the term "congruence" in the context of modular arithmetic and its relevance to cryptographic algorithms.?
Ans:

CONGRUENCE (≡)

If two numbers A and B have the property that their difference A-B is integrally divisible by a number C (i.e., (A-B)/C is an integer), then A and B are said to be "congruent modulo C." The number C is called the modulus , and the statement "A is congruent to B (modulo C)" is written mathematically as

$$A \equiv B \pmod{C}$$

This says that " A is congruent to B modulo C".

Examining the expression closer:

1. ≡ is the symbol for congruence, which means the values A and B are in the same **equivalence class**.
2. (mod C) tells us what **operation** we applied to A and B.
3. when we have both of these, we call "≡" **congruence modulo** C.

e.g. $26 \equiv 11 \pmod 5$

$26 \bmod 5 = 1$ so it is in the equivalence class for 1.

$11 \bmod 5 = 1$ so it is in the equivalence class for 1, as well.

So, 26 is congruent to 11 modulo 5

Congruence in modular arithmetic is crucial for cryptographic algorithms due to its role in:

1. RSA Algorithm: Uses modular exponentiation for encryption ($c \equiv m^e \pmod{n}$) and decryption ($m \equiv c^d \pmod{n}$).
2. Diffie-Hellman Key Exchange: Relies on operations like $g^a \pmod{p}$ for secure key exchange.
3. Elliptic Curve Cryptography (ECC): Uses modular arithmetic for defining operations on elliptic curves over finite fields.
4. Hash Functions: Ensures fixed-size outputs through modular arithmetic operations.

These applications leverage the properties of congruences to maintain security, efficiency, and integrity in cryptographic processes.

4.Difference Between DES And AES Algorithms.
Ans:

	AES	DES
1.	AES stands for Advanced Encryption Standard	DES stands for Data Encryption Standard
2.	The date of creation is 2001.	The date of creation is 1977.
3.	Byte-Oriented.	Bit-Oriented.
4.	Key length can be 128-bits, 192-bits, and 256-bits.	The key length is 56 bits in DES.
5.	Number of rounds depends on key length: 10(128-bits), 12(192-bits), or 14(256-bits)	DES involves 16 rounds of identical operations

6.	The structure is based on a substitution-permutation network.	The structure is based on a Feistel network.
7.	The design rationale for AES is open.	The design rationale for DES is closed.
8.	The selection process for this is secret but accepted for open public comment.	The selection process for this is secret.

9.	AES is more secure than the DES cipher and is the de facto world standard.	DES can be broken easily as it has known vulnerabilities. 3DES(Triple DES) is a variation of DES which is secure than the usual DES.
10.	The rounds in AES are: Byte Substitution, Shift Row, Mix Column and Key Addition	The rounds in DES are: Expansion, XOR operation with round key, Substitution and Permutation

11.	AES can encrypt 128 bits of plaintext.	DES can encrypt 64 bits of plaintext.
12.	It can generate Ciphertext of 128, 192, 256 bits.	It generates Ciphertext of 64 bits.
13.	AES cipher is derived from an aside-channel square cipher.	DES cipher is derived from Lucifer cipher.
14.	AES was designed by Vincent Rijmen and Joan Daemen.	DES was designed by IBM.

15.	No known crypt-analytical attacks against AES but side channel attacks against AES implementations possible. Biclique attacks have better complexity than brute force but still ineffective.	Known attacks against DES include Brute-force, Linear crypt-analysis, and Differential crypt-analysis.
16.	It is faster than DES.	It is slower than AES.
17.	It is flexible.	It is not flexible.
18.	It is efficient with both hardware and software.	It is efficient only with hardware.

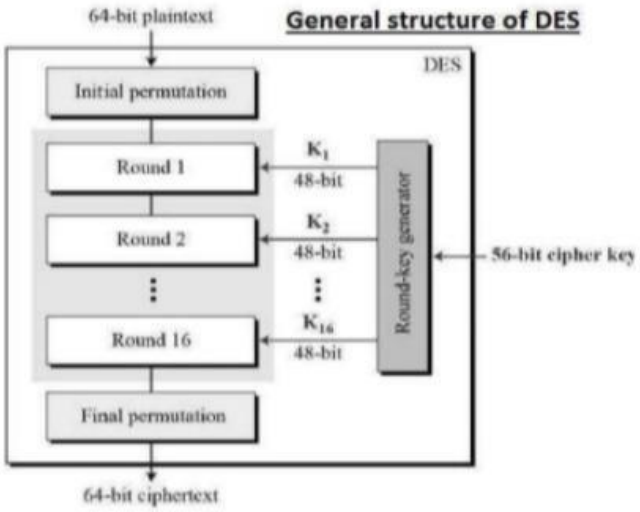
5.explain DES Algorithm in details.
Ans:

Data Encryption Standard (DES)

The Data Encryption Standard (DES) is a symmetric-key block cipher published by the National Institute of Standards and Technology (NIST).

DES is an implementation of a Feistel Cipher. It uses 16 round Feistel structure. The block size is 64-bit. Though, key length is 64-bit, DES has an effective key length of 56 bits, since 8 of the 64 bits of the key are not used by the encryption algorithm (function as check bits only).

General structure of DES



DES Symmetric key Block Cipher algorithm. DES follows Feistel cipher structure.
Plain Text Block Size :
64 Bits Cipher Text Size :
64 Bits
Master Key Size : 64 / 56
Bits No. Of Rounds 16
Round Key / Subkey Size: 48 Bits.

Initial Permutation & Inverse Initial Permutation

The initial permutation and its inverse are defined by tables, as shown in Tables.
The tables are to be interpreted as follows.
The input to a table consists of 64 bits numbered from 1 to 64.
The 64 entries in the permutation table contain a permutation of the numbers from 1 to 64.
Each entry in the permutation table indicates the position of a numbered input bit in the output, which also consists of 64 bits.
The initial and final permutations are straight Permutation boxes (P-boxes) that are inverses of each other.
Note:
Initial Permutation & Inverse Initial Permutations have no cryptography significance in DES.

Input Table

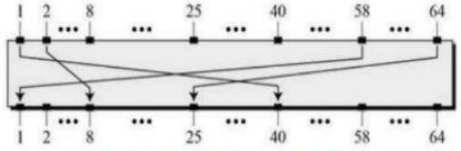
1	2	3	4	5	6	7	8
9	10	11	12	13	14	15	16
17	18	19	20	21	22	23	24
25	26	27	28	29	30	31	32
33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48
49	50	51	52	53	54	55	56
57	58	59	60	61	62	63	64

(a) Initial Permutation (IP)

58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6
64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1
59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5
63	55	47	39	31	23	15	7

In output
At 1st place 58
At 2nd place 50

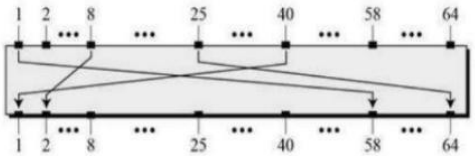
At 3rd place 42 ..



(b) Inverse Initial Permutation (IP^{-1})

40	8	48	16	56	24	64	32
39	7	47	15	55	23	63	31
38	6	46	14	54	22	62	30
37	5	45	13	53	21	61	29
36	4	44	12	52	20	60	28
35	3	43	11	51	19	59	27
34	2	42	10	50	18	58	26
33	1	41	9	49	17	57	25

In output
At 1st place 40
At 2nd place 8
At 3rd place 48 ..



Rounds

Rounds

The left and right halves of each 64- bit intermediate value are treated as separate 32-bit quantities, labeled L (left) and R (right).
As in any classic Feistel cipher, the overall processing at each round can be summarized in the following formulas:

$$L_i = R_{i-1}$$

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

The round key $\mathbf{K_i}$ is 48 bits. The R input is 32 bits. This **R** input is first expanded to 48 bits by using a table that defines a permutation plus an expansion that involves duplication of 16 of the **R** bits.

The resulting 48 bits are XORed with $\mathbf{K_i}$. This 48-bit result passes through a substitution function that produces a 32-bit output, which is permuted as defined by Table.
The role of the **S-boxes** in the function F is illustrated in Figure 3.7.The substitution consists of a set of eight S-boxes, each of which accepts 6 bits as input and produces 4 bits as output. These transformations are defined in Table 3.3, which is interpreted as follows: The first and last bits of the input to box $\mathbf{S_i}$ form a 2-bit binary number to select one of four substitutions defined by the four rows in the table for $\mathbf{S_i}$. The middle four bits select one of the sixteen columns. The decimal value in the cell selected by the row and column is then converted to its 4-bit representation to produce the output. For example, in S1, for input 011001, the row is 01 (row 1) and the column is 1100 (column 12). The value in row 1, column 12 is 9, so the output is 1001.

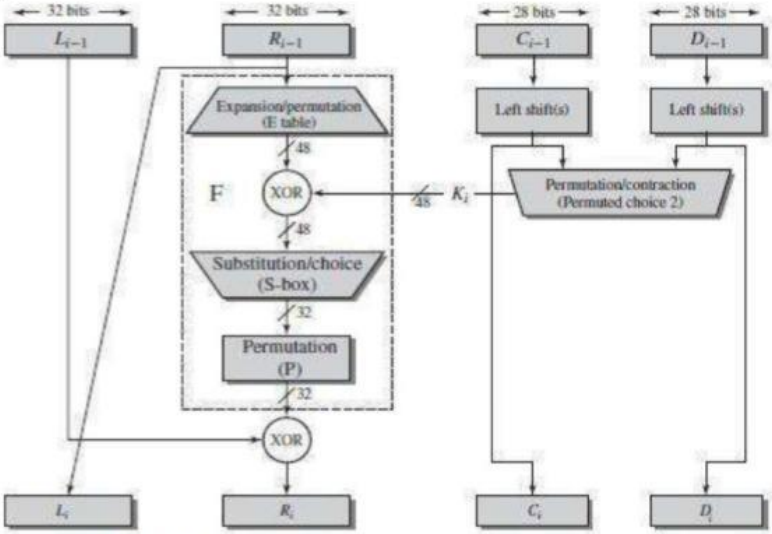


Figure 3.6 Single Round of DES Algorithm

(c) Expansion Permutation (E)

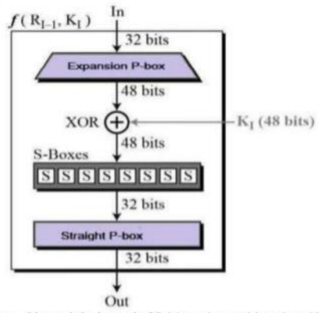
32	1	2	3	4	5
4	5	6	7	8	9
8	9	10	11	12	13
12	13	14	15	16	17
16	17	18	19	20	21
20	21	22	23	24	25
24	25	26	27	28	29
28	29	30	31	32	1

(d) Permutation Function (P)

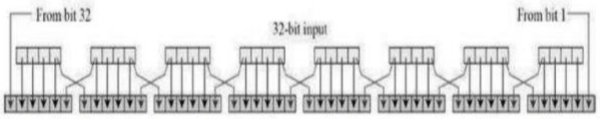
16	7	20	21	29	12	28	17
1	15	23	26	5	18	31	10
2	8	24	14	32	27	3	9
19	13	30	6	22	11	4	25

Round Function

The heart of this cipher is the DES function, *f*. The DES function applies a 48-bit key to the rightmost 32 bits to produce a 32-bit output.



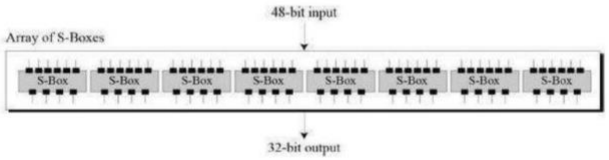
Expansion Permutation Box − Since right input is 32-bit and round key is a 48-bit, we first need to expand right input to 48 bits. Permutation logic is graphically depicted in the following illustration −



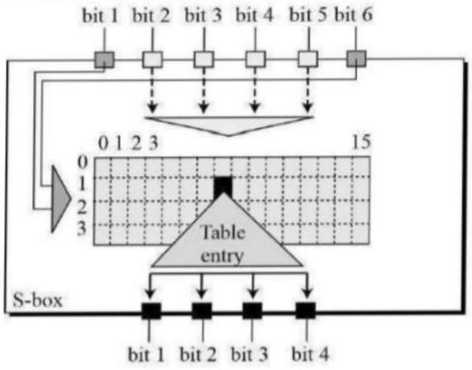
The graphically depicted permutation logic is generally described as table in DES specification illustrated as shown −

32	01	02	03	04	05
04	05	06	07	08	09
08	09	10	11	12	13
12	13	14	15	16	17
16	17	18	19	20	21
20	21	22	23	24	25
24	25	26	27	28	29
28	29	31	31	32	01

XOR (Whitener). − After the expansion permutation, DES does XOR operation on the expanded right section and the round key. The round key is used only in this operation.
Substitution Boxes. − The S-boxes carry out the real mixing (confusion). DES uses 8 S-boxes, each with a 6-bit input and a 4-bit output. Refer the following illustration −



The S-box rule is illustrated below −



There are a total of eight S-box tables.
The output of all eight s-boxes is then combined in to 32 bit section.

Table 3.3 Definition of DES S-Boxes

S_1	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
	4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13
S_2	15	1	8	14	6	11	3	4	9	7	2	13	12	0	5	10
	3	13	4	7	15	2	8	14	12	0	1	10	6	9	11	5
	0	14	7	11	10	4	13	1	5	8	12	6	9	3	2	15
	13	8	10	1	3	15	4	2	11	6	7	12	0	5	14	9
S_3	10	0	9	14	6	3	15	5	1	13	12	7	11	4	2	8
	13	7	0	9	3	4	6	10	2	8	5	14	12	11	15	1
	13	6	4	9	8	15	3	0	11	1	2	12	5	10	14	7
	1	10	13	0	6	9	8	7	4	15	14	3	11	5	2	12
S_4	7	13	14	3	0	6	9	10	1	2	8	5	11	12	4	15
	13	8	11	5	6	15	0	3	4	7	2	12	1	10	14	9
	10	6	9	0	12	11	7	13	15	1	3	14	5	2	8	4
	3	15	0	6	10	1	13	8	9	4	5	11	12	7	2	14
S_5	2	12	4	1	7	10	11	6	8	5	3	15	13	0	14	9
	14	11	2	12	4	7	13	1	5	0	15	10	3	9	8	6
	4	2	1	11	10	13	7	8	15	9	12	5	6	3	0	14
	11	8	12	7	1	14	2	13	6	15	0	9	10	4	5	3
S_6	12	1	10	15	9	2	6	8	0	13	3	4	14	7	5	11
	10	15	4	2	7	12	9	5	6	1	13	14	0	11	3	8
	9	14	15	5	2	8	12	3	7	0	4	10	1	13	11	6
	4	3	2	12	9	5	15	10	11	14	1	7	6	0	8	13

S_7	4	11	2	14	15	0	8	13	3	12	9	7	5	10	6	1
	13	0	11	7	4	9	1	10	14	3	5	12	2	15	8	6
	1	4	11	13	12	3	7	14	10	15	6	8	0	5	9	2
	6	11	13	8	1	4	10	7	9	5	0	15	14	2	3	12
S_8	13	2	8	4	6	15	11	1	10	9	3	14	5	0	12	7
	1	15	13	8	10	3	7	4	12	5	6	11	0	14	9	2
	7	11	4	1	9	12	14	2	0	6	10	13	15	3	5	8
	2	1	14	7	4	10	8	13	15	12	9	0	3	5	6	11

The 32-bit output from the eight S-boxes is then permuted, so that on the next round, the output from each S-box immediately affects as many others as possible.

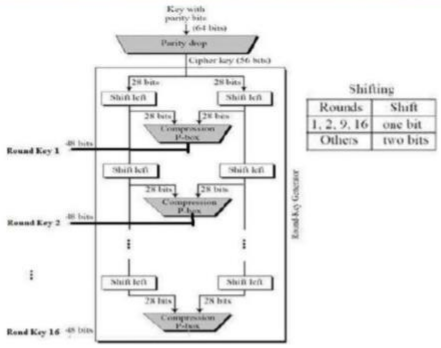
Straight Permutation

− The 32 bit output of S-boxes is then subjected to the straight permutation with rule shown in the following illustration:

16	07	20	21	29	12	28	17
01	15	23	26	05	18	31	10
02	08	24	14	32	27	03	09
19	13	30	06	22	11	04	25

DES Key Generation

The round-key generator creates sixteen 48-bit keys out of a 56-bit cipher key. The process of key generation is depicted in the following illustration −



Shifting

Rounds	Shift
1, 2, 9, 16	one bit
Others	two bits

Table 3.4 DES Key Schedule Calculation

(a) Input Key

1	2	3	4	5	6	7	8
9	10	11	12	13	14	15	16
17	18	19	20	21	22	23	24
25	26	27	28	29	30	31	32
33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48
49	50	51	52	53	54	55	56
57	58	59	60	61	62	63	64

(b) Permuted Choice One (PC-1)

57	49	41	33	25	17	9
1	58	50	42	34	26	18
10	2	59	51	43	35	27
19	11	3	60	52	44	36
63	55	47	39	31	23	15
7	62	54	46	38	30	22
14	6	61	53	45	37	29
21	13	5	28	20	12	4

(c) Permuted Choice Two (PC-2)

14	17	11	24	1	5	3	28
15	6	21	10	23	19	12	4
26	8	16	7	27	20	13	2
41	52	31	37	47	55	30	40
51	45	33	48	44	49	39	56
34	53	46	42	50	36	29	32

(d) Schedule of Left Shifts

Round Number	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Bits Rotated	1	1	2	2	2	2	2	2	1	2	2	2	2	2	2	1

DES Decryption

As with any Feistel cipher, decryption uses the same algorithm as encryption, except that the application of the subkeys is reversed.

DES Analysis

DES Analysis

Two desired properties of a block cipher are the Avalanche effect and the completeness.
Avalanche effect :

A small change in plaintext results in the very great change in the ciphertext.

EXAMPLE 6.7 To check the avalanche effect in DES, let us encrypt two plaintext blocks (with the same key) that differ only in one bit and observe the differences in the number of bits in each round.

```
Plaintext: 0000000000000000          Key: 22234512987ABB23
Ciphertext: 4789FD476E82A5F1
Plaintext: 0000000000000001          Key: 22234512987ABB23
Ciphertext: 0A4ED5C15A63FEA3
```

Completeness effect:
Completeness effect means that each bit of ciphertext needs to depends on many bits on the plaintext. The diffusion and confusion produced by P-Boxes and S-Boxes in DES, show a very strong completeness effect.

DES Weaknesses Analysis

Weakness in Cipher Design:
It is not clear why the designers of DES used the initial and final permutations; these have no security benefits.
In the expansion permutation, the first and fourth bits of every 4-bit series are repeated.
Weakness in Cipher Key:
o DES Key size is 56 bits. To do Brute force attack on a given ciphertext block, the adversary needs to check 2^{56} keys.
With available technology it is possible to check 1 million keys per second

6.Different Type Of Security Attacks.
Ans:

Cryptographic Attacks

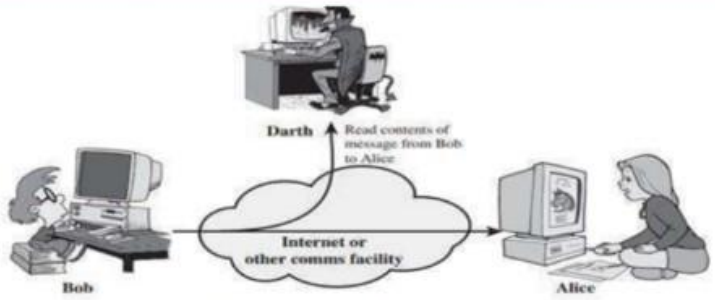
Accessing of data by unauthorized entity is called as attack
Passive Attacks
Active Attacks

Passive Attacks:
In a passive attack, the attacker's goal is just to obtain information. This means that the attack does not modify data or harm the system.
Active Attacks:
An active attack may change the data or harm the system. Attacks that threaten the integrity and availability are active attacks.

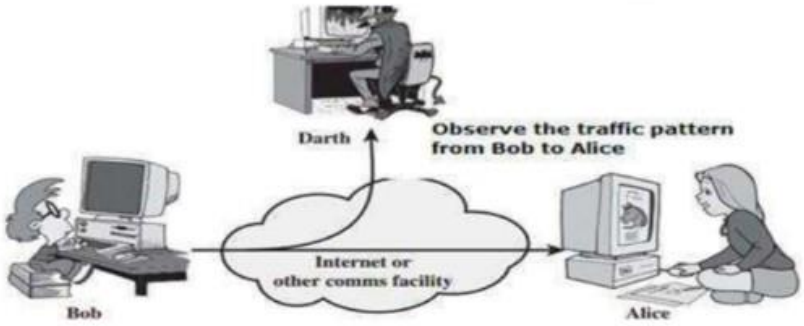
- Passive attacks
  - Interception
    - Release of message contents
    - Traffic analysis
- Active attacks
  - Interruption, modification, fabrication
    - Masquerade
    - Replay
    - Modification
    - Denial of service

Passive Attacks
(a) Release of message content –
Capture and read the content transmissions.
(b) Traffic Analysis–

- can't read the information, but observe the pattern
- determine the location and identity of communicating parties
- observe frequency and length of communication



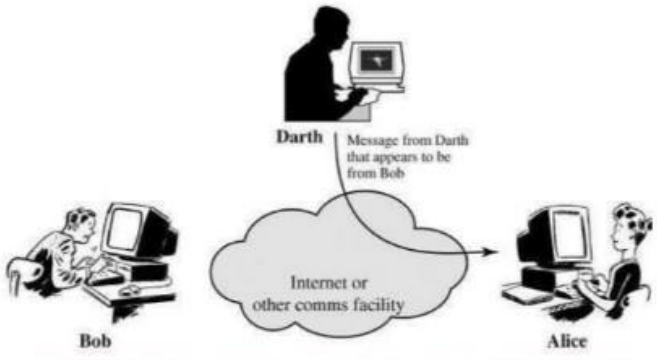
(a) Release of Message content



(b) Traffic Analysis

Active Attacks

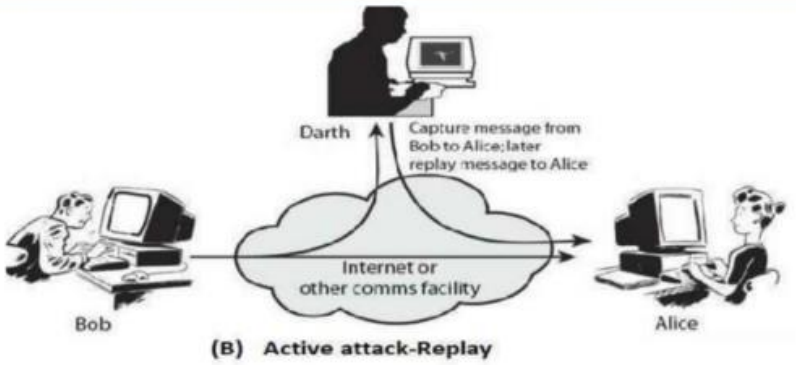
(a) Masquerading: Masquerading or snooping happens when the attacker impersonates somebody else.



Active Attack – Masquerade

(b) Replay–

The attacker obtains a copy of a message sent by a user and later tries to replay it.

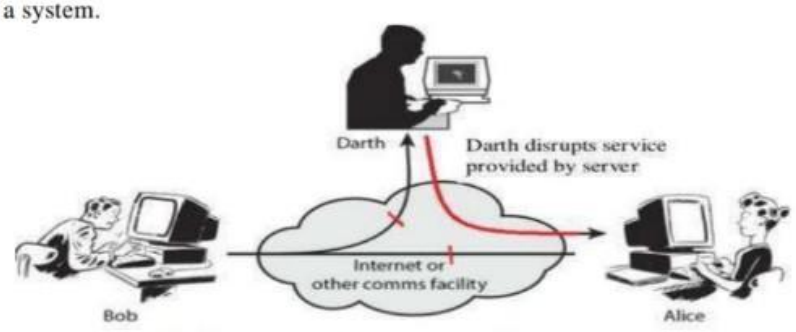


(B) Active attack-Replay

(c) Modification: After intercepting or accessing information, the attacker modifies the information then send to receiver.

Active Attack – Modification of messages

(d) Denial of service: Denial of service (Dos) is a very common attack.it may slow down or totally interrupt the service of a system.



(d) Active attack - Denial of Service

7. Find all solutions to the following sets of linear equations:
   a. $3x + 5y \equiv 4 \pmod 5$ $2x + y \equiv 3 \pmod 5$

Ans:

Ans

Given $3x+5y \equiv 4 \pmod 5$ -①

$2x+y \equiv 3 \pmod 5$ -②

a)

$2x + y = 3 \pmod 5$.

Sol Let take them into matrix form first we get

$$\begin{bmatrix} 3 & 5 \\ 2 & 1 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} 4 \\ 3 \end{bmatrix} \pmod 5$$

$$\begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} 3 & 5 \\ 2 & 1 \end{bmatrix}^{-1} \begin{bmatrix} 4 \\ 3 \end{bmatrix} \pmod 5$$

Suppose $A^{-1} = \begin{bmatrix} 3 & 5 \\ 2 & 1 \end{bmatrix}$.

$\because A^{-1} = \dfrac{\text{cofactor of } A}{\det \text{ of } A}$.

$\det(A) = ad - bc = 3 - 10 = -7$.

cofactor of $3 = 1$

cofactor of $2 = -5$

cofactor of $5 = -2$

cofactor of $1 = 3$.

cofactor of $A = \begin{bmatrix} 1 & -2 \\ -5 & 3 \end{bmatrix}$

then $A^1 = \begin{bmatrix} 1 & -5 \\ -2 & 3 \end{bmatrix}$

$A^{-1} = \dfrac{A^1}{\det(A)}$ or $\dfrac{A^1}{|A|}$

$A^{-1} = \dfrac{-1}{7} \begin{bmatrix} 1 & -5 \\ -2 & 3 \end{bmatrix}$

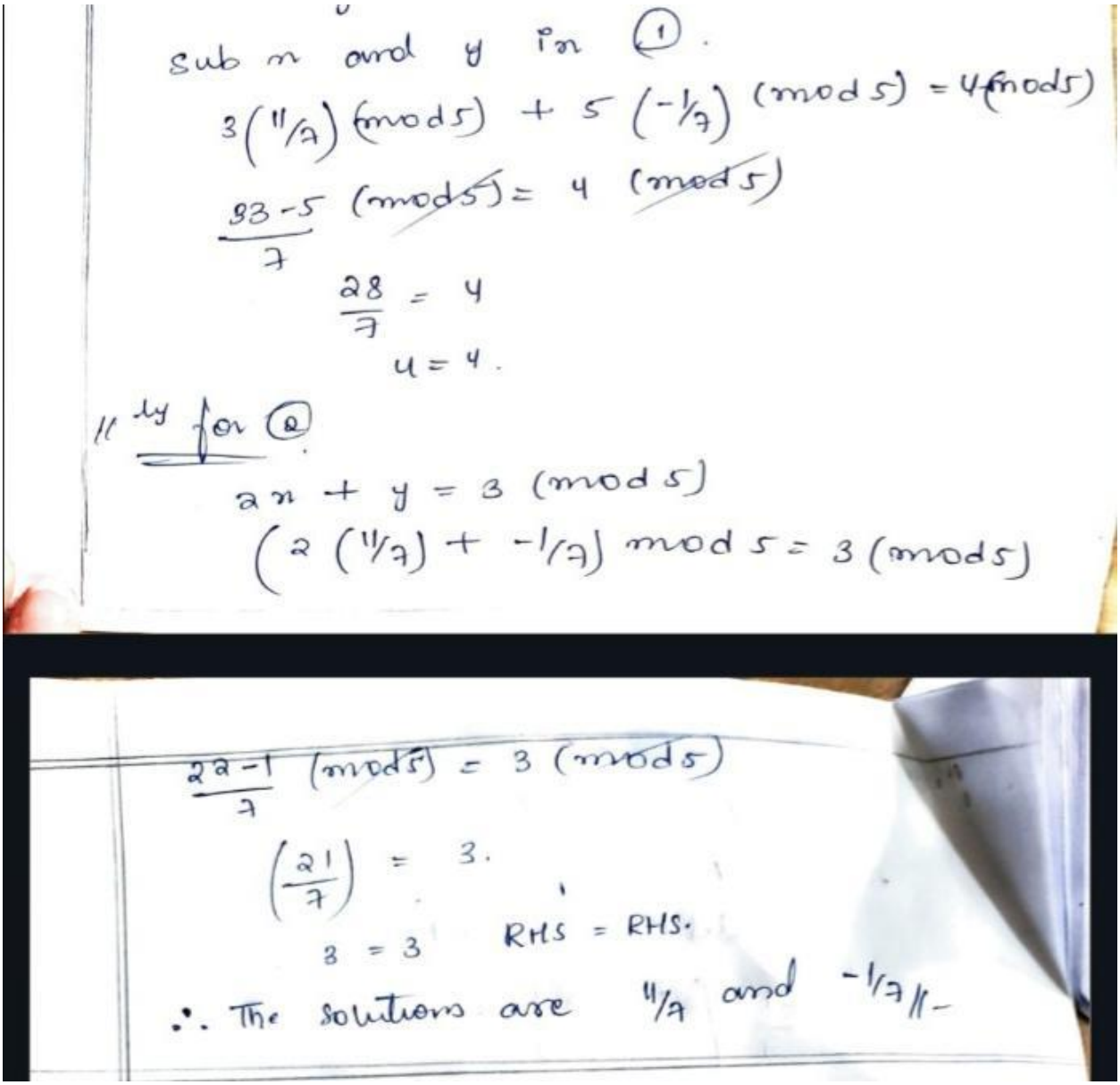
$$\begin{bmatrix} x \\ y \end{bmatrix} = \frac{1}{7} \begin{bmatrix} -1 & 5 \\ 2 & -3 \end{bmatrix} \begin{bmatrix} 4 \\ 3 \end{bmatrix} \pmod 5$$

$$\begin{bmatrix} x \\ y \end{bmatrix} = \frac{1}{7} \begin{bmatrix} 11 \\ -1 \end{bmatrix} \pmod 5$$

$$\begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} 11/7 \\ -1/7 \end{bmatrix} \pmod 5$$

$x = 11/7 \pmod 5$.

$y = -1/7 \pmod 5$



8. List all additive inverse pairs in modulus 20.
Ans:

List all the inverse pairs in modulus 20.
^
additive

Additive Inverse :-

In Z_n, two numbers a and b are additive inverses of each other if

$$a + b \equiv 0 \pmod{n}$$

In Z_n, additive inverse can be calculated as

$b = n - a$.

The ten pair of additive inverses in Z_{20} are:-

$a + b \equiv 0 \pmod{20}$:

(0,0) because $0+0 \equiv 0 \pmod{20}$
(1,19) because $1+19 \equiv 20 \equiv 0 \pmod{20}$
(2,18) because $2+18 \equiv 20 \equiv 0 \pmod{20}$
(3,17) because $3+17 \equiv 20 \equiv 0 \pmod{20}$
(4,16) because $4+16 \equiv 20 \equiv 0 \pmod{20}$
(5,15) because $5+15 \equiv 20 \equiv 0 \pmod{20}$
(6,14) because $6+14 \equiv 20 \equiv 0 \pmod{20}$
(7,13) because $7+13 \equiv 20 \equiv 0 \pmod{20}$
(8,12) because $8+12 \equiv 20 \equiv 0 \pmod{20}$
(9,11) because $9+11 \equiv 20 \equiv 0 \pmod{20}$

9.List all multiplicative inverse pairs in modulus 20.
Ans:

List all the multiplicative inverses pairs in modulus 20.

Multiplicative inverse :-

In Z_n, two numbers are multiplicative inverse of each other if

$$a \times b \equiv 1 \pmod{n}$$

There are only 6 pairs of ~~inverse~~ multiplicative inverse in modulus 20.

The numbers 0, 2, 4, 5, 6, 8 do not have multiplicative inverse.

(17)

The six pairs of multiplicative inverse in mod are –

1. (1, 1) because $1 \times 1 \equiv 1 \pmod{20}$
2. (3, 7) because $3 \times 7 \equiv 21 \equiv 1 \pmod{20}$
3. ~~(7, 3) because $7 \times 3 \equiv 21 \equiv 1 \pmod{20}$~~
3. (9, 9) because $9 \times 9 \equiv 81 \equiv 1 \pmod{20}$
4. (11, 11) because $11 \times 11 \equiv 121 \equiv 1 \pmod{20}$
5. (13, 17) because $13 \times 17 \equiv 221 \equiv 1 \pmod{20}$
6. (19, 19) because $19 \times 19 \equiv 361 \equiv 1 \pmod{20}$

10 Using Lagrange's theorem, find the orders of all the potential subgroups of the

following groups:

a. G =<Z_{18},+>

b. G =<Z_{29},+>

Ans:

Lagrange's theorem states that the order of any subgroup of a finite group divides the order of the group. Let's apply this theorem to determine the orders of all potential subgroups for the given groups.

a. $G = \langle \mathbb{Z}_{18}, + \rangle$

The group $\mathbb{Z}_{18}$ under addition modulo 18 has order 18. According to Lagrange's theorem, the order of any subgroup must divide 18. The divisors of 18 are:

$$1, 2, 3, 6, 9, 18$$

So, the possible orders of subgroups of $\mathbb{Z}_{18}$ are:

$$1, 2, 3, 6, 9, 18$$

b. $G = \langle \mathbb{Z}_{29}, + \rangle$

The group $\mathbb{Z}_{29}$ under addition modulo 29 has order 29. Since 29 is a prime number, its only positive divisors are 1 and 29. According to Lagrange's theorem, the order of any subgroup must divide 29. Thus, the possible orders of subgroups of $\mathbb{Z}_{29}$ are:

$$1, 29$$

Conclusion

- For $G = \mathbb{Z}_{18}$, the orders of all potential subgroups are: $1, 2, 3, 6, 9, 18$.
- For $G = \mathbb{Z}_{29}$, the orders of all potential subgroups are: $1, 29$.

11. Distinguish between a substitution cipher and a transposition cipher.
Ans:

S.NO	Substitution Cipher Technique	Transposition Cipher Technique
1.	In substitution Cipher Technique, plain text characters are replaced with other characters, numbers and symbols.	In transposition Cipher Technique, plain text characters are rearranged with respect to the position.
2.	Substitution Cipher’s forms are: Mono alphabetic substitution cipher and poly alphabetic substitution cipher.	Transposition Cipher’s forms are: Key-less transposition cipher and keyed transposition cipher.

3.	In substitution Cipher Technique, character's identity is changed while its position remains unchanged.	While in transposition Cipher Technique, The position of the character is changed but character's identity is not changed.
4.	In substitution Cipher Technique, The letter with low frequency can detect plain text.	While in transposition Cipher Technique, The Keys which are nearer to correct key can disclose plain text.

5.	The example of substitution Cipher is Caesar Cipher, monoalphabetic cipher, and polyalphabetic cipher.	The example of transposition Cipher is Rail Fence Cipher, columnar transposition cipher, and route cipher.
6.	Involves replacing plaintext letters or groups of letters with ciphertext letters or groups of letters according to a specific algorithm or key.	Involves rearranging the order of the plaintext letters or groups of letters according to a specific algorithm or key.

7.	The frequency distribution of the plaintext letters is typically obscured, but patterns can still be detected with statistical analysis.	The frequency distribution of the plaintext letters remains the same, but the order is scrambled, making it difficult to detect patterns with statistical analysis.

8.	Vulnerable to frequency analysis attacks, where the most commonly used letters or letter combinations in the language can be identified and used to deduce the key.	Less vulnerable to frequency analysis attacks, but still susceptible to attacks such as brute force and known plaintext attacks.

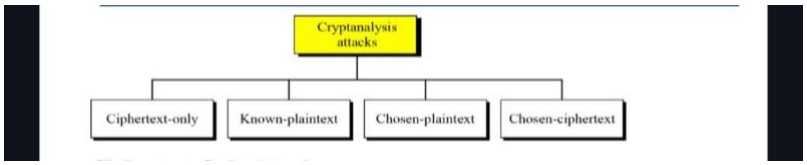
9.	Relatively easy to understand and implement, making it suitable for simple applications.	Can be more difficult to implement and understand, but can be more secure than substitution ciphers for certain applications.

12. List four kinds of cryptanalysis attacks.
Ans:

As cryptography is the science and art of creating secret codes, cryptanalysis is the science and art of breaking those Codes.

The four kinds of cryptanalysis attacks are:

- Ciphertext-Only Attack
- Known-Plaintext Attack
- Chosen-Plaintext Attack
- Chosen-Ciphertext Attack



13. What is the block size in DES? What is the cipher key size in DES? What is theround-key size in DES?

Ans:

In the Data Encryption Standard (DES), the following specifications apply:

- Block Size: DES operates on blocks of data that are 64 bits (8 bytes) in length. This means that each unit of plaintext or ciphertext processed by DES is 64 bits long.

- Cipher Key Size: The key used in DES is 56 bits long. Although the initial key provided is 64 bits, 8 of these bits are used solely for parity (error checking) and are not involved in the actual encryption process. Therefore, the effective key size for encryption is 56 bits.

- Round-Key Size: In each of the 16 rounds of DES, a 48-bit subkey (round-key) is generated from the 56-bit cipher key. These round-keys are derived using a process called key scheduling, where the 56-bit key is permuted and shifted to produce 16 different 48-bit round-keys.