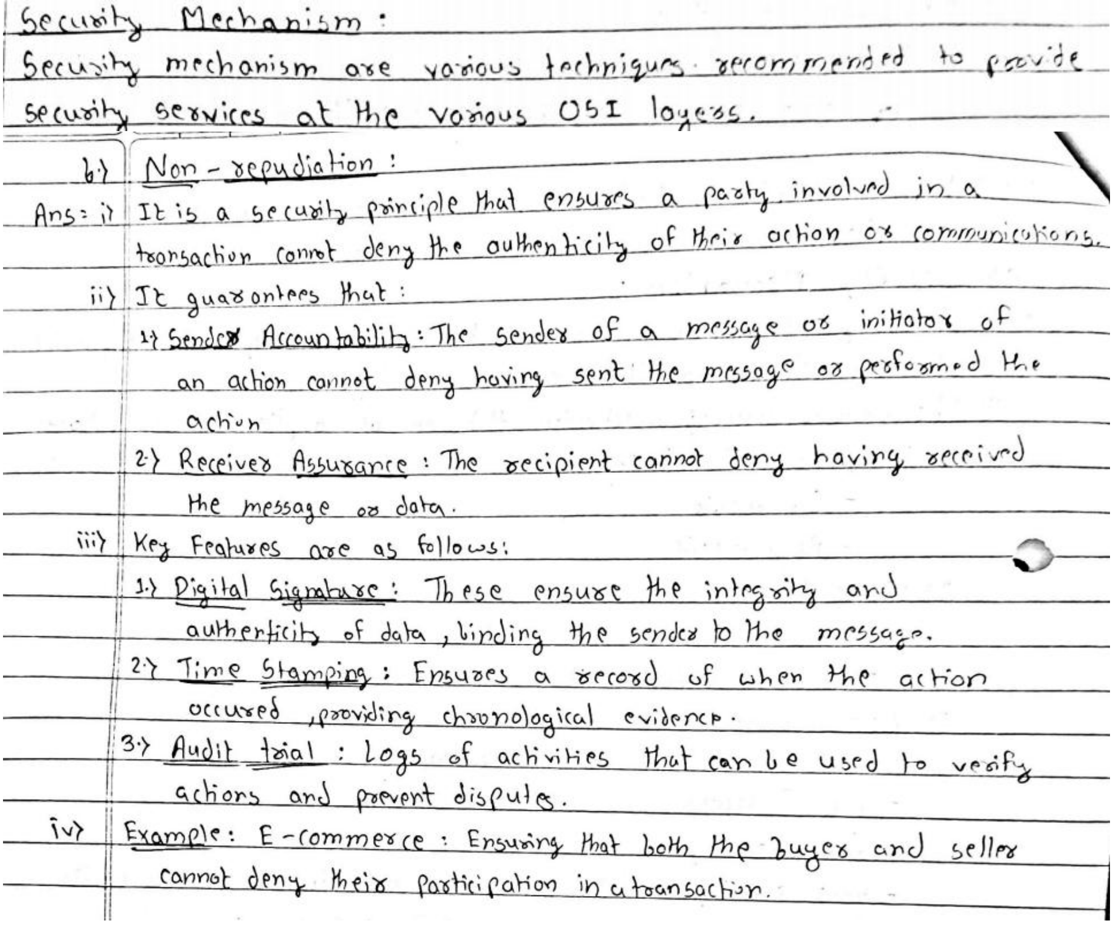
CSS IAT-1 2025:

Module 1:

1.Explain the following System security terms in detail with examples:

(b) Non-repudiation (Q1.a) What are the security mechanisms for non-repudiation?)



Security Mechanism :

Security mechanism are various techniques recommended to provide security services at the various OSI layers.

b) Non-repudiation :

Ans: i) It is a security principle that ensures a party involved in a transaction cannot deny the authenticity of their action or communications.

ii) It guarantees that :

1) Sender Accountability : The sender of a message or initiator of an action cannot deny having sent the message or performed the action

2) Receiver Assurance : The recipient cannot deny having received the message or data.

iii) Key Features are as follows:

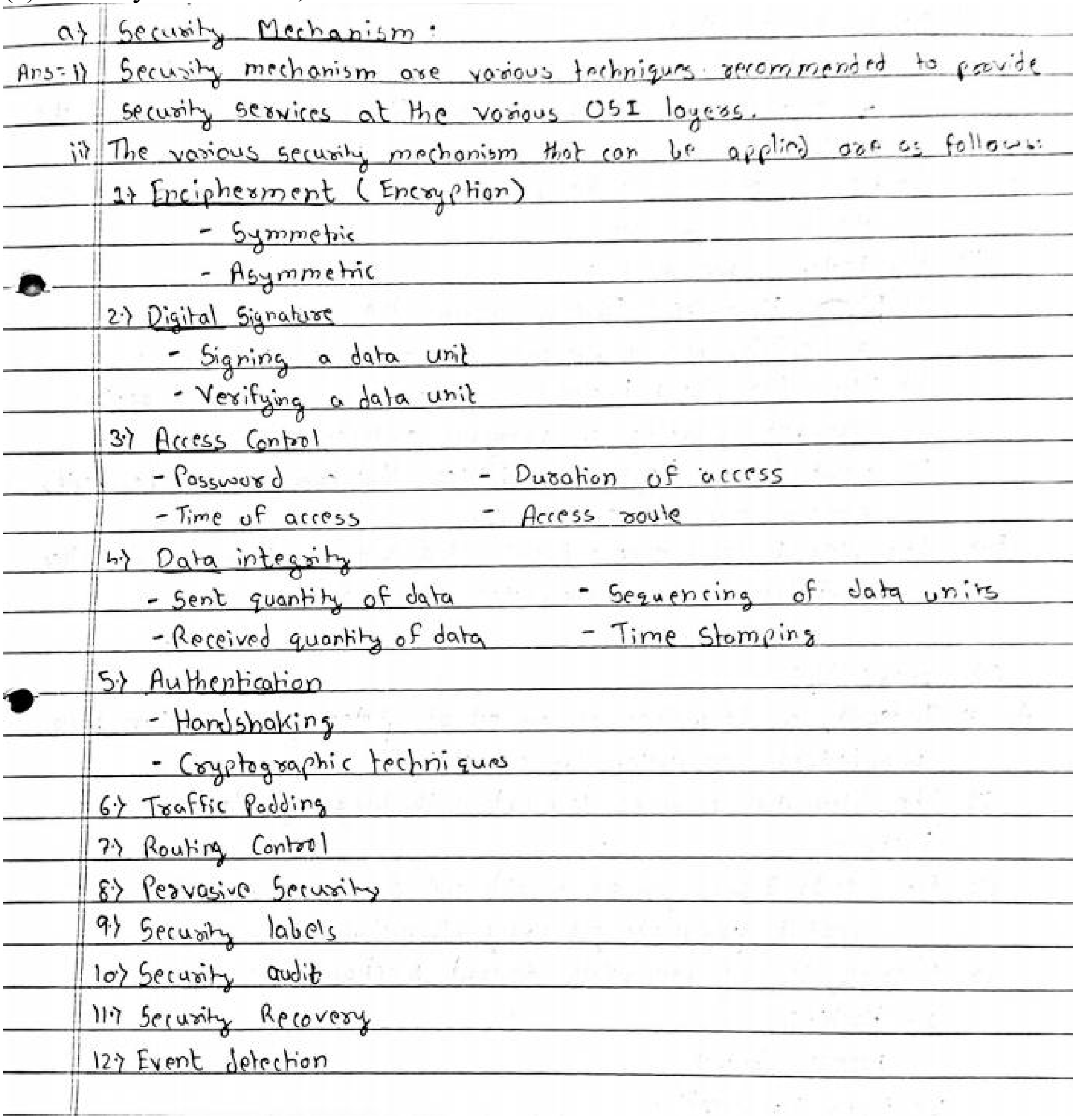
1) Digital Signature : These ensure the integrity and authenticity of data, binding the sender to the message.

2) Time Stamping : Ensures a record of when the action occured, providing chronological evidence.

3) Audit trial : Logs of activities that can be used to verify actions and prevent disputes.

iv) Example : E-commerce : Ensuring that both the buyer and seller cannot deny their participation in a transaction.

(a) Security mechanism;



a) Security Mechanism :

Ans:- i) Security mechanism are various techniques recommended to provide security services at the various OSI layers.

ii) The various security mechanism that can be applied are as follows:

1) Encipherment (Encryption)
- Symmetric
- Asymmetric

2) Digital Signature
- Signing a data unit
- Verifying a data unit

3) Access Control
- Password - Duration of access
- Time of access - Access route

4) Data integrity
- Sent quantity of data - Sequencing of data units
- Received quantity of data - Time Stamping

5) Authentication
- Handshaking
- Cryptographic techniques

6) Traffic Padding

7) Routing Control

8) Pervasive Security

9) Security labels

10) Security audit

11) Security Recovery

12) Event detection

2.Explain the following Ciphers with illustrative example:

(a) Playfair cipher; (Q1.b) What are the strengths and weaknesses of Playfair Cipher?)

The **Playfair cipher** is a manual symmetric encryption technique that encrypts **pairs of letters (digraphs)** instead of single letters. It was invented by **Charles Wheatstone** in 1854 but is named after Lord Playfair, who promoted its use.

The Playfair Cipher Algorithm:

The Algorithm consists of 2 steps:

1. **Generate the key Square(5×5)**
2. **Algorithm to encrypt the plain text**

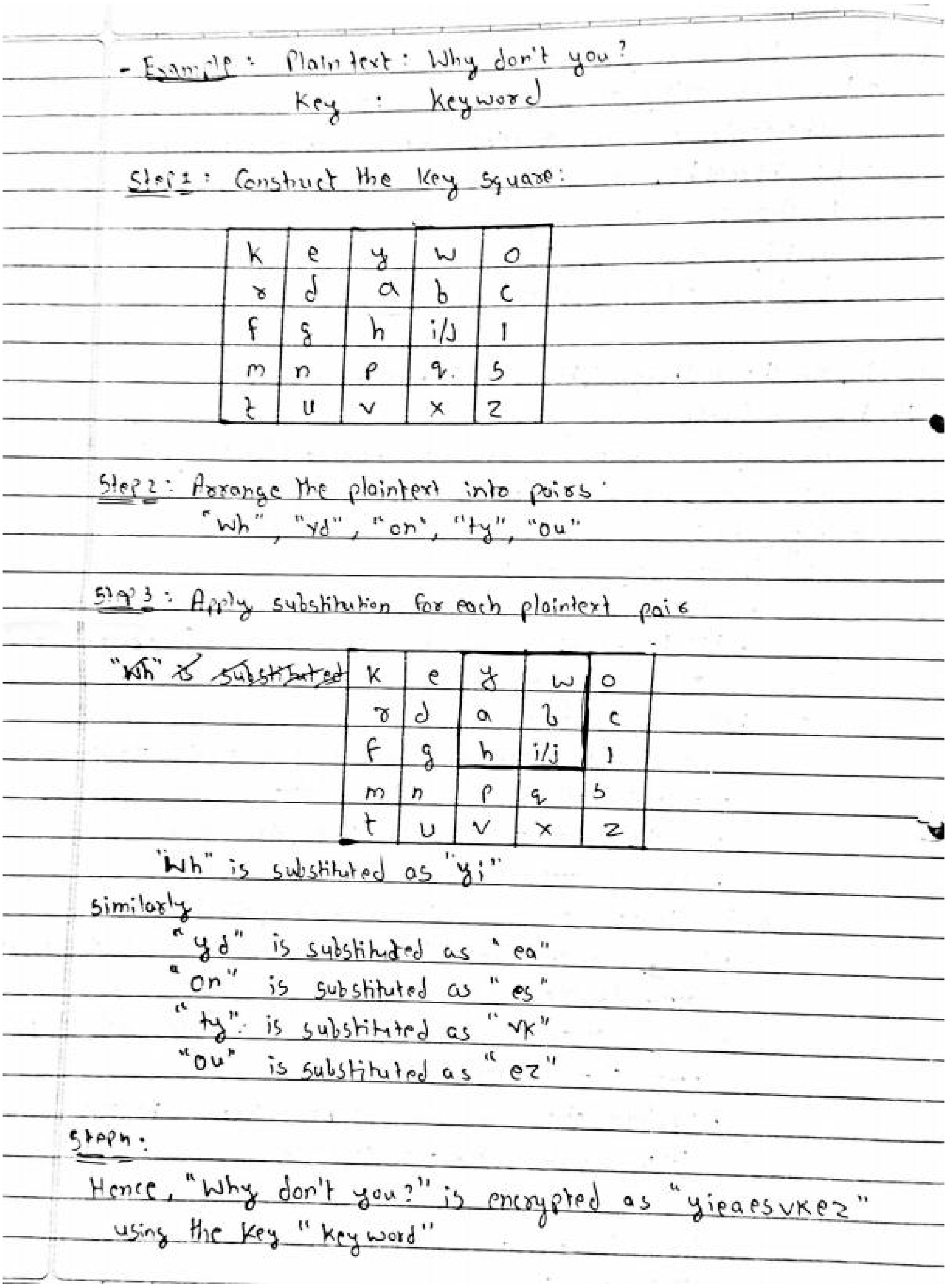
Strengths of Playfair Cipher

✔ **More secure than simple substitution ciphers** – Encrypting digraphs makes frequency analysis harder.

✔ **Resistant to direct letter frequency attacks** – Since it encrypts **pairs of letters**, single-character frequency analysis is ineffective.

Weaknesses of Playfair Cipher

❌ **Not secure against modern cryptanalysis** – Still vulnerable to **digraph frequency analysis**.
❌ **Key exchange problem** – The **keyword** must be securely shared between sender and receiver.



- Example : Plain text : Why don't you ?
Key : keyword

Step 1 : Constuct the key square:

k	e	y	w	o
r	d	a	b	c
f	g	h	i/j	l
m	n	p	q	s
t	u	v	x	z

Step 2 : Arrange the plaintext into pairs :
"wh", "yd", "on", "ty", "ou"

Step 3 : Apply substitution for each plaintext pair

"Wh" ~~is substituted~~

k	e	y	w	o
r	d	a	b	c
f	g	h	i/j	l
m	n	p	q	s
t	u	v	x	z

"Wh" is substituted as "yi"
Similarly
"yd" is substituted as "ea"
"on" is substituted as "es"
"ty" is substituted as "vk"
"ou" is substituted as "ez"

Step 4 :
Hence, "Why don't you?" is encrypted as "yieaesvkez" using the key "keyword"

(b) Transposition cipher (Q1.b) Explain with examples keyed and keyless transposition cipher)

b) Transposition cipher

Ans = - There are two types of transposition ~~cifer~~ cipher as follows:

1) Keyed Transposition Cipher:

- In keyed transposition, a random key is used to describe the transposition sequence and carry out transposition
- Algorithm: i) Arrange the plaintext in a column under a given key
  ii) Re-arrange the plaintext columnwise in key's alphabetic order
- Example: Plaintext: "Save the king from attack".
  Key: "ENCRYPT"

Step 1: Arrange the plaintext in a column under a given key.

E	N	C	R	Y	P	T
2	3	1	5	7	4	6
s	a	v	e	t	h	e
k	i	n	g	f	r	o
m	a	t	t	o	c	k

Step 2: Rearrange the plaintext columnwise in key's alphabetic order

Take column C marked as 1st in order → vnt

~~Similarly~~ E marked as 2nd in order → skm

N marked as 3rd in order → aia

Similarly other keys are encrypted

~~Step 3~~

The ciphertext obtained is "vntskmaiahrcegteoktfa"

2) Keyless Transposition Cipher:

- In keyless transposition, a transposition sequence is described without a random key.
- Example of keyless transposition cipher is ~~r~~ Railfence cipher.
- Algorithm: i) Based on the rail size arrange the plaintext
  ii) Rearrange the plaintext row-wise to get the ciphertext

- Example: Plaintext: "Save the King"
  Assume Rail size: 3

Step 1: Based on rail size arrange the plaintext

rail 1 →	s				t				i		
rail 2 →		a		e		h		k		n	
rail 3 →			v				e				g

Step 2: Rearrange the plaintext row wise to get the cipher text

∴ The cipher text is: "stiaehknveg"

3.List down the different types of active & passive attacks.(Q1.d)

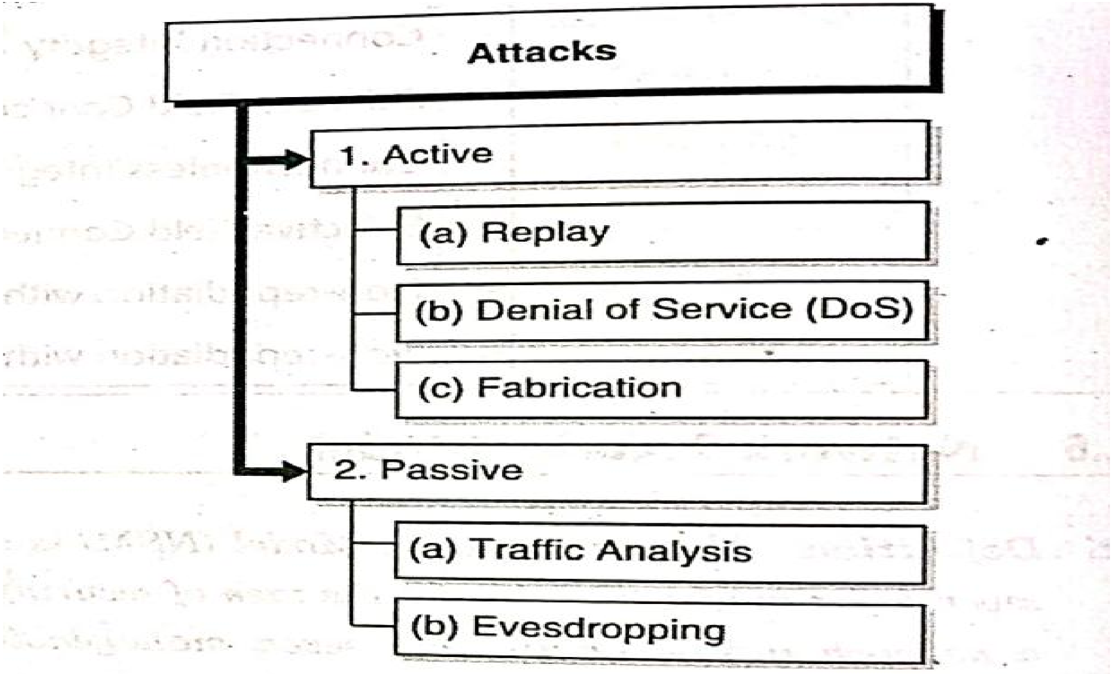
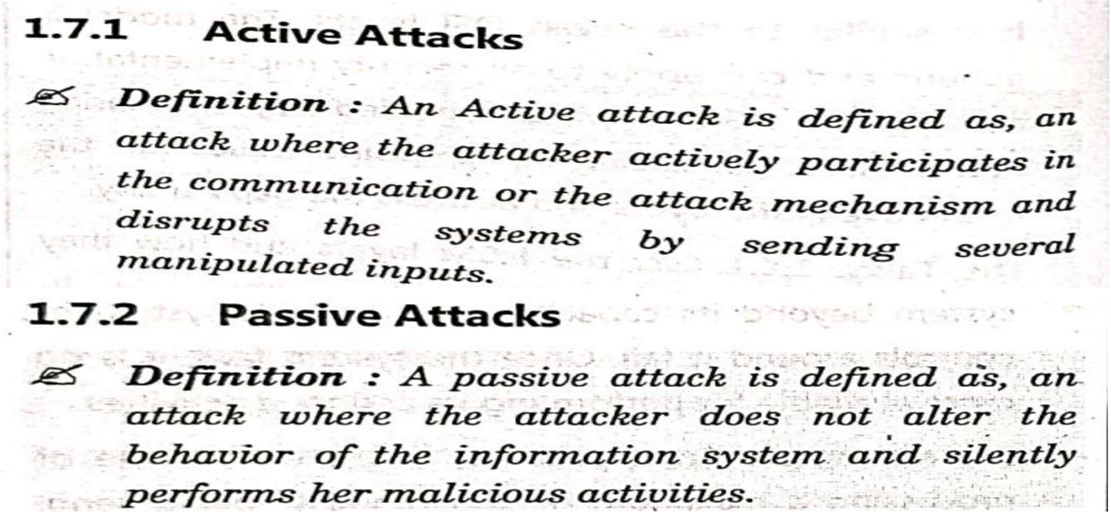


Fig. 1.7.1 : Types of Security Attacks



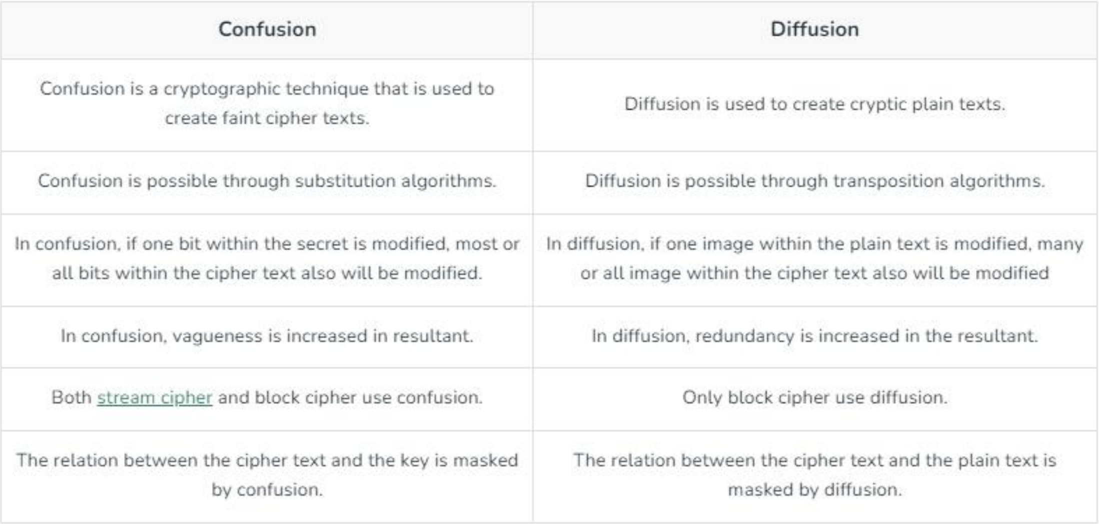
1.7.1 Active Attacks

✍ ***Definition :*** *An Active attack is defined as, an attack where the attacker actively participates in the communication or the attack mechanism and disrupts the systems by sending several manipulated inputs.*

1.7.2 Passive Attacks

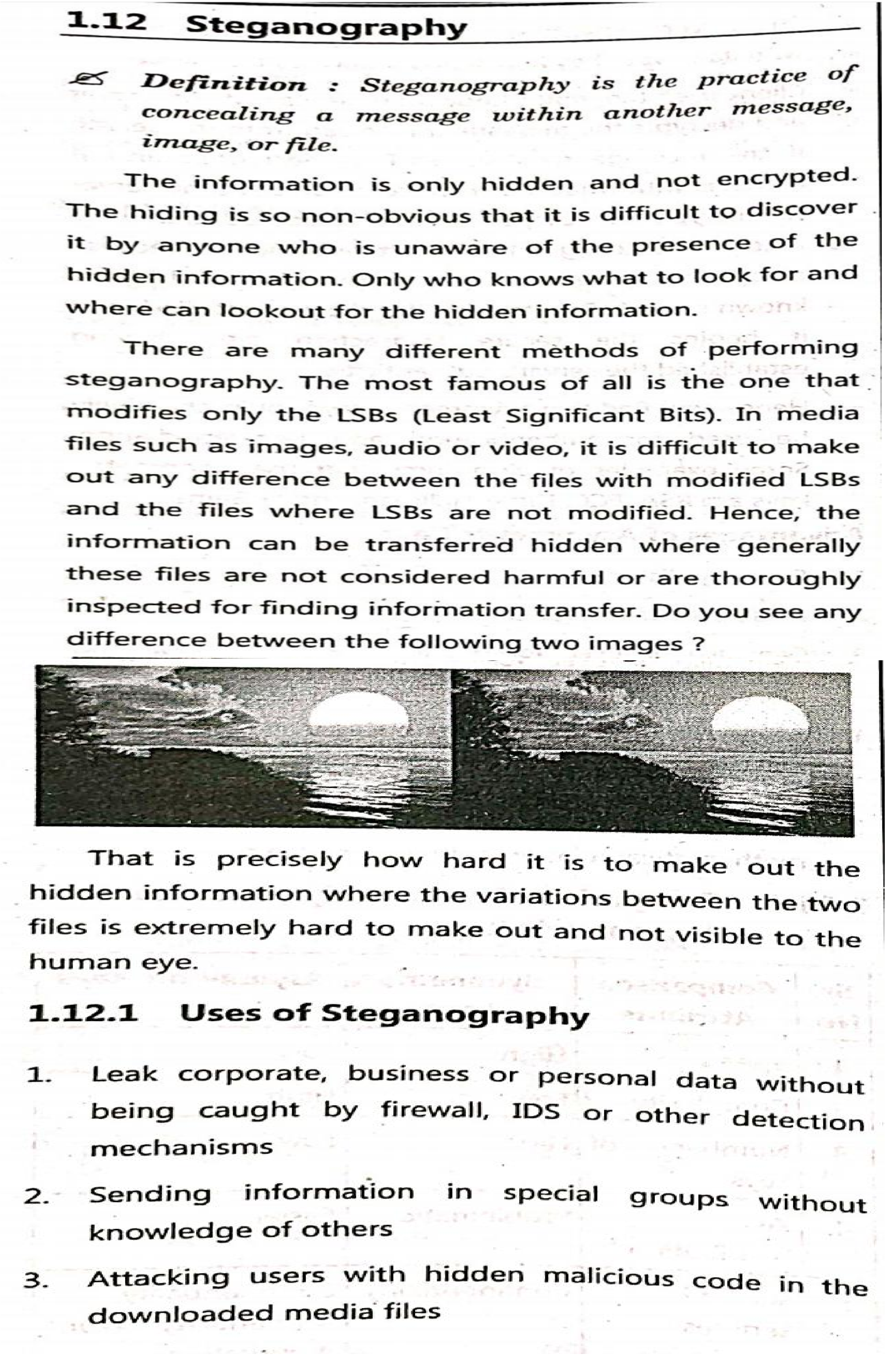
✍ ***Definition :*** *A passive attack is defined as, an attack where the attacker does not alter the behavior of the information system and silently performs her malicious activities.*

4. What is the difference between diffusion and confusion?(Q1.c)



Confusion	Diffusion
Confusion is a cryptographic technique that is used to create faint cipher texts.	Diffusion is used to create cryptic plain texts.
Confusion is possible through substitution algorithms.	Diffusion is possible through transposition algorithms.
In confusion, if one bit within the secret is modified, most or all bits within the cipher text also will be modified.	In diffusion, if one image within the plain text is modified, many or all image within the cipher text also will be modified
In confusion, vagueness is increased in resultant.	In diffusion, redundancy is increased in the resultant.
Both stream cipher and block cipher use confusion.	Only block cipher use diffusion.
The relation between the cipher text and the key is masked by confusion.	The relation between the cipher text and the plain text is masked by diffusion.

5. Write a short note on steganography.(Q1.d)



1.12 Steganography

✍ ***Definition : Steganography is the practice of concealing a message within another message, image, or file.***

The information is only hidden and not encrypted. The hiding is so non-obvious that it is difficult to discover it by anyone who is unaware of the presence of the hidden information. Only who knows what to look for and where can lookout for the hidden information.

There are many different methods of performing steganography. The most famous of all is the one that modifies only the LSBs (Least Significant Bits). In media files such as images, audio or video, it is difficult to make out any difference between the files with modified LSBs and the files where LSBs are not modified. Hence, the information can be transferred hidden where generally these files are not considered harmful or are thoroughly inspected for finding information transfer. Do you see any difference between the following two images ?

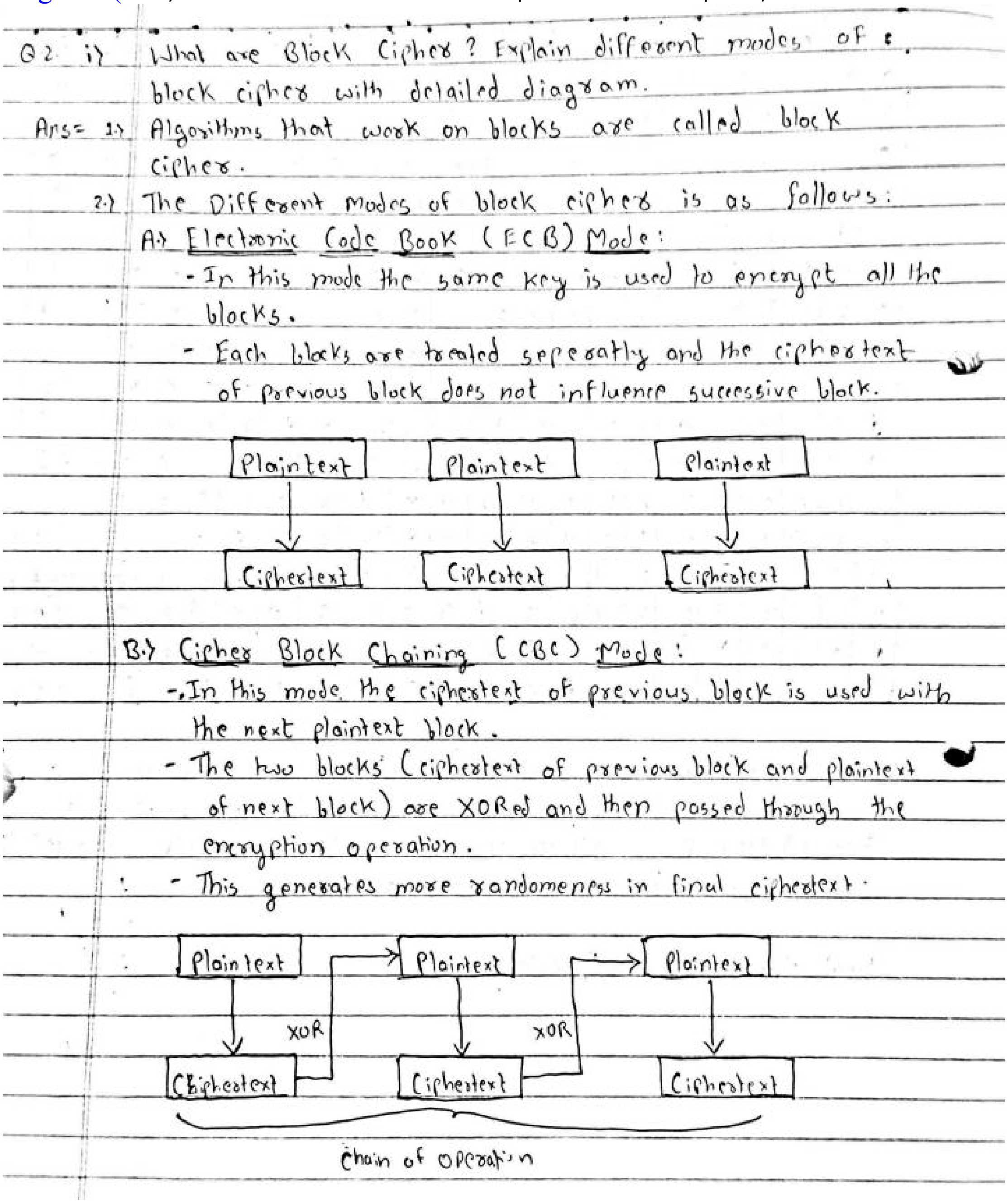
That is precisely how hard it is to make out the hidden information where the variations between the two files is extremely hard to make out and not visible to the human eye.

1.12.1 Uses of Steganography

1. Leak corporate, business or personal data without being caught by firewall, IDS or other detection mechanisms
2. Sending information in special groups without knowledge of others
3. Attacking users with hidden malicious code in the downloaded media files

Module 2:

1. What are Block Ciphers? Explain different modes of block ciphers with detailed diagram. (Q2.a) What are the different modes of operation in block cipher?)



Q2. i) What are Block Cipher ? Explain different modes of block cipher with detailed diagram.

Ans= 1.) Algorithms that work on blocks are called block cipher.

2.) The Different modes of block cipher is as follows:

A.) Electronic Code Book (ECB) Mode:

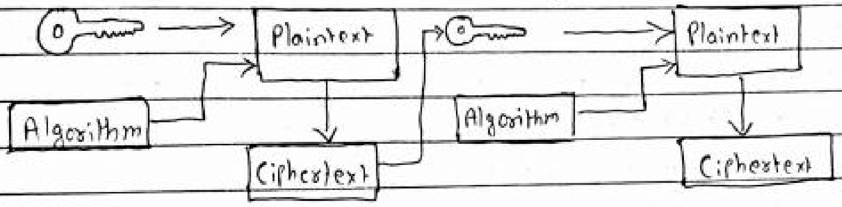
- In this mode the same key is used to encrypt all the blocks.
- Each blocks are treated seperatly and the ciphertext of previous block does not influence successive block.

B.) Cipher Block Chaining (CBC) Mode:

- In this mode the ciphertext of previous block is used with the next plaintext block.
- The two blocks (ciphertext of previous block and plaintext of next block) are XORed and then passed through the encryption operation.
- This generates more randomeness in final ciphertext.

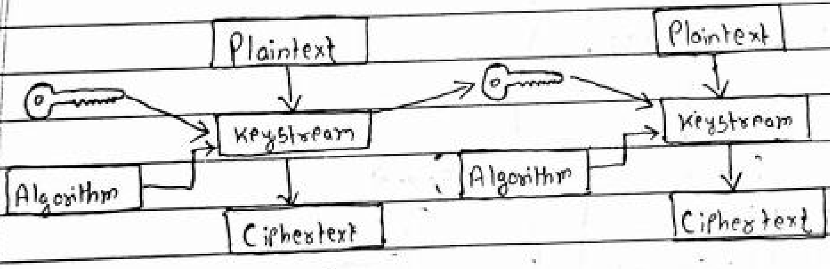
C) Cipher Feedback (CFB) Mode:

- In this mode the block cipher work like a stream cipher.
- The ciphertext of previous block is XORed with the key for the next block.
- This way the key increasingly becomes random and brings more randomness in the overall encryption process.



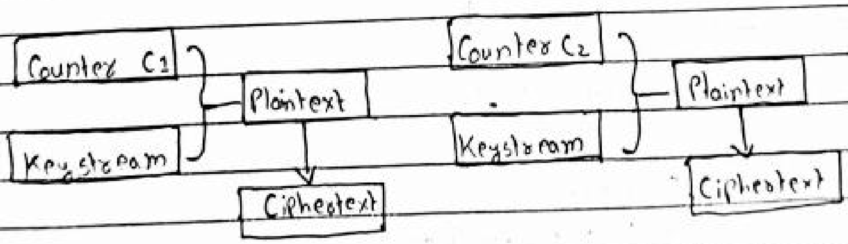
D) Output Feedback (OFB) Mode:

- In this mode the block cipher works like a stream cipher.
- The keystream used in previous block is XORed with the keystream of next block.



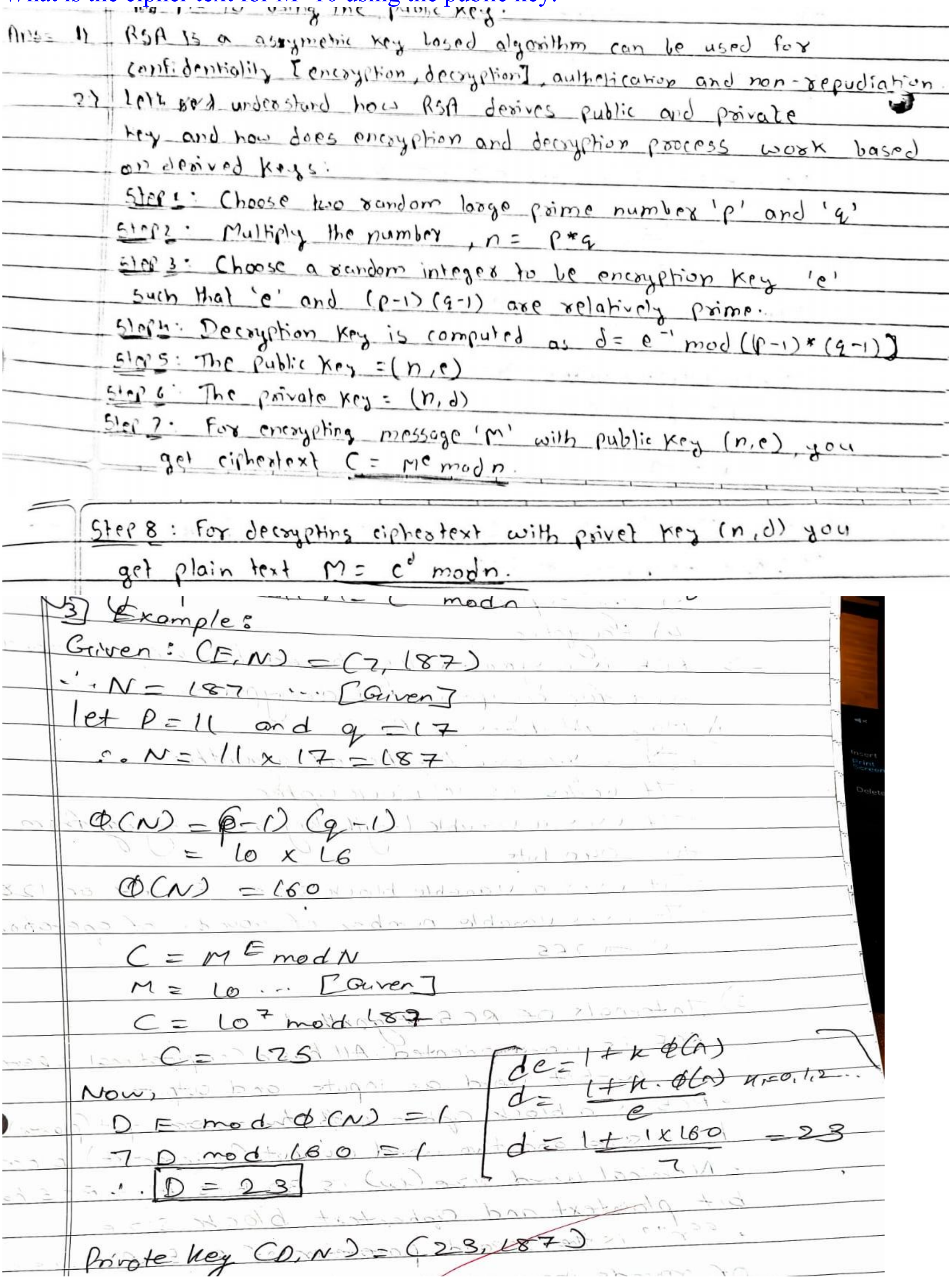
E) Counter (CTR) Mode:

- In this mode the key is converted into the keystream and the keystream is XORed with a counter that increases for every block.



Numericals:

2. Elaborate the steps of key generation using the RSA algorithm. In RSA system the public key (E, N) of user A is defined as (7,187). Calculate Φ (N) and private key 'D'. What is the cipher text for M=10 using the public key.



Ans:- 1) RSA is a asymmetric key based algorithm can be used for confidentiality [encryption, decryption], authentication and non-repudiation.

2) Let's see understand how RSA derives public and private key and how does encryption and decryption process work based on derived keys:

Step 1: Choose two random large prime number 'p' and 'q'

Step 2: Multiply the number, $n = p*q$

Step 3: Choose a random integer to be encryption key 'e' such that 'e' and $(p-1)(q-1)$ are relatively prime.

Step 4: Decryption key is computed as $d = e^{-1} \bmod ((p-1)*(q-1))$

Step 5: The public key $= (n, e)$

Step 6: The private key $= (n, d)$

Step 7: For encrypting message 'M' with public key (n, e), you get ciphertext $C = M^e \bmod n$.

Step 8: For decrypting ciphertext with privet key (n, d) you get plain text $M = C^d \bmod n$.

3) Example:

Given : $(E, N) = (7, 187)$

$\therefore N = 187$ ..... [Given]

let $P = 11$ and $q = 17$

$\therefore N = 11 \times 17 = 187$

$\Phi(N) = (p-1)(q-1)$

$= 10 \times 16$

$\Phi(N) = 160$

$C = M^E \bmod N$

$M = 10$ ... [Given]

$C = 10^7 \bmod 187$

$C = 175$

Now,

$D\, E \bmod \Phi(N) = 1$

$7\, D \bmod 160 = 1$

$\therefore \boxed{D = 23}$

$de = 1 + k\,\phi(n)$

$d = \dfrac{1 + k \cdot \phi(n)}{e}$ $k = 0, 1, 2 \ldots$

$d = \dfrac{1 + 1 \times 160}{7} = 23$

Private key $(D, N) = (23, 187)$

$M = C^d \bmod N$

$= 175^{23} \bmod 187$

2^4	2^3	2^2	2^1	2^0
16	8	4	2	1
1	0	1	1	1

- $175^1 \bmod 187 = \underline{175}$
- $175^2 \bmod 187 = \underline{144}$
- $175^4 \bmod 187 = \underline{166}$
- $175^8 \bmod 187$

$(175^4)^2 \bmod 187$

$= (166)^2 \bmod 187 = 67$

- $175^{16} \bmod 187$

$(175^8)^2 \bmod 187$

$= (67)^2 \bmod 187 = \underline{1}$

$= (175 \times 144 \times 166 \times 1) \bmod 187$

$= 10$

Result : $\phi(N) = 160$

$D = 23$

Ciphertext for $M = 10$ is 175.

3. Explain RSA cryptosystem. In RSA Given n=221 and e=5 find d.(Q2.b)

RSA Cryptosystem

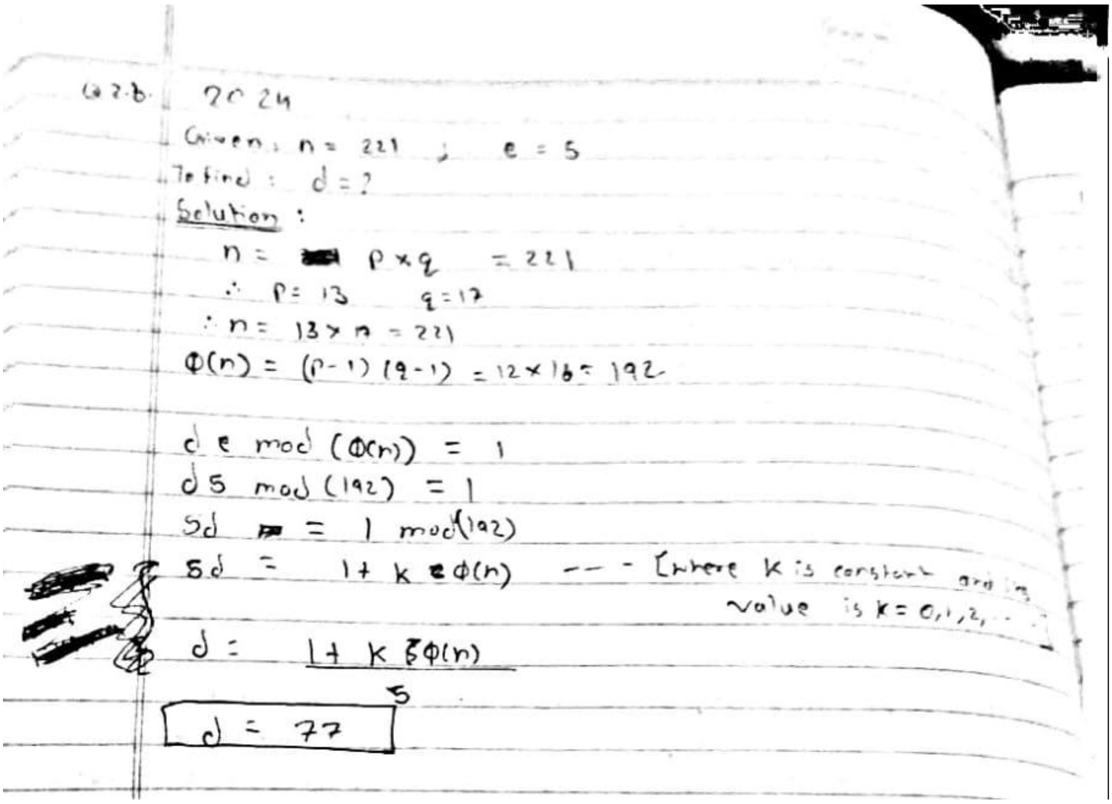
The **RSA (Rivest-Shamir-Adleman) cryptosystem** is a widely used **asymmetric encryption algorithm** that relies on the mathematical properties of prime numbers and modular arithmetic. It provides both **encryption** and **digital signatures**, ensuring **confidentiality, integrity, and authentication** in secure communications.

Key Components of RSA

RSA is based on **public-key cryptography**, meaning it uses a **pair of keys**:

1. **Public Key** – Used for encryption (known to everyone).
2. **Private Key** – Used for decryption (kept secret by the owner).

The security of RSA is based on the **difficulty of factoring large prime numbers**.



Q2.b. 2024

Given: $n = 221$; $e = 5$

To find: $d = ?$

Solution :

$n = p \times q = 221$

$\therefore p = 13 \quad q = 17$

$\therefore n = 13 \times 17 = 221$

$\Phi(n) = (p-1)(q-1) = 12 \times 16 = 192$

$d\,e \bmod (\Phi(n)) = 1$

$d\,5 \bmod (192) = 1$

$5d = 1 \bmod (192)$

$5d = 1 + k \times \Phi(n)$ --- [where k is constant and its value is $k = 0, 1, 2, \ldots$]

$d = \dfrac{1 + k \times \Phi(n)}{5}$

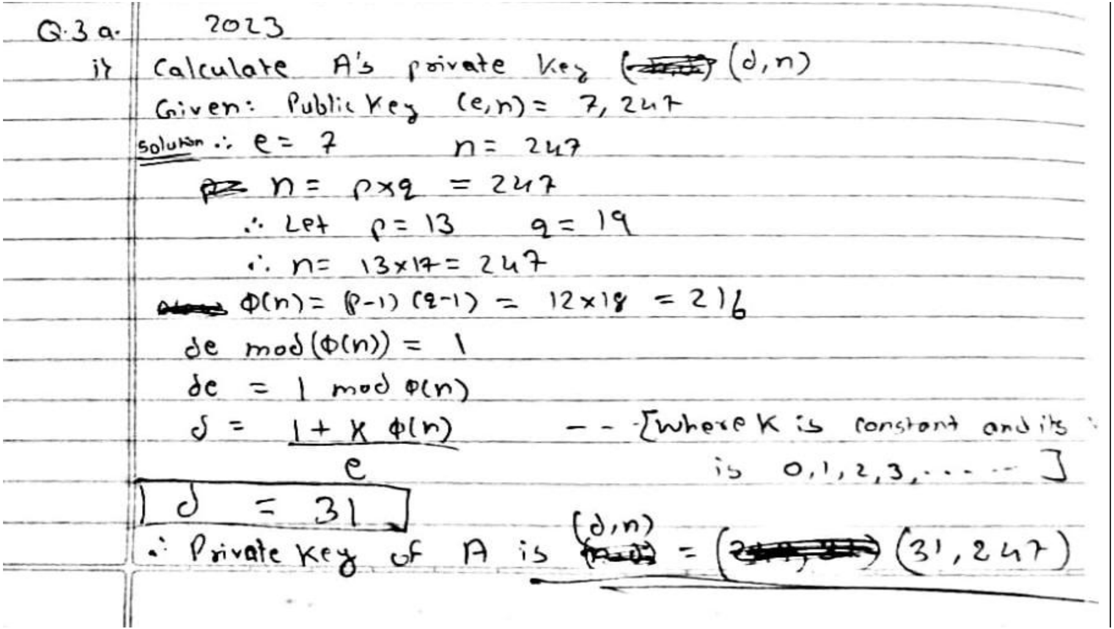
$\boxed{d = 77}$

4. If A and B wishes to use RSA to communicate securely, A chooses public key (e,n) as (7,247) and B chooses public key (e, n) as (5,221)

i)Calculate A's private key

ii) Calculate B's Private Key

iii) What will be the cipher text sent by A to B, If A wishes to send M-5 to B (Q3.a)



Q.3 a. 2023

i) Calculate A's private Key (d, n)

Given: Public Key (e,n) = 7, 247

Solution ∴ e = 7   n = 247

$n = p \times q = 247$

∴ Let p = 13   q = 19

∴ $n = 13 \times 17 = 247$

$\phi(n) = (p-1)(q-1) = 12 \times 18 = 216$

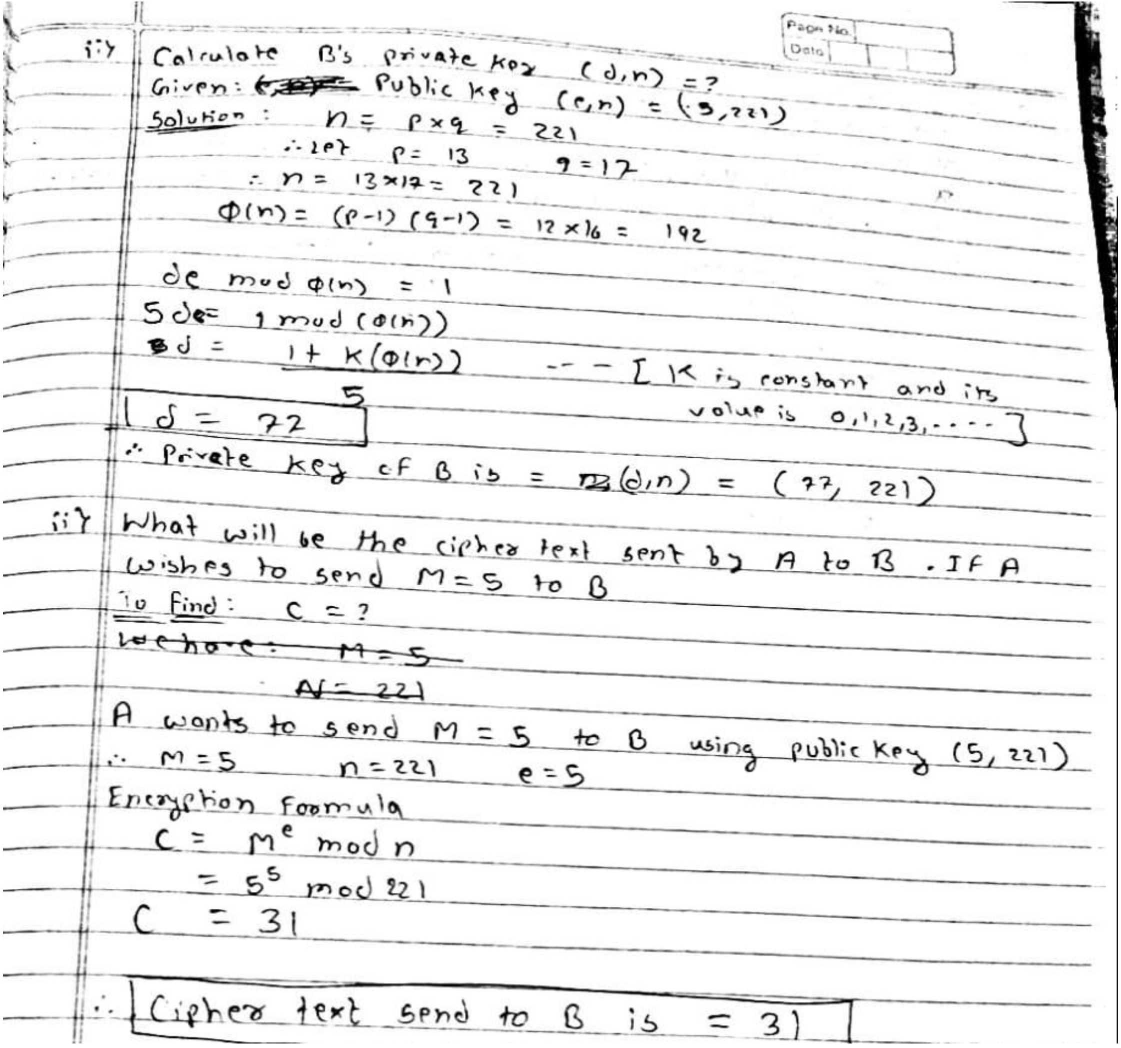
$de \bmod (\phi(n)) = 1$

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

$d = \frac{1 + K\,\phi(n)}{e}$ -- [where K is constant and its is 0,1,2,3,......]

$\boxed{d = 31}$

∴ Private Key of A is $\overset{(d,n)}{}$ = (31, 247)



Page No.

Date

ii) Calculate B's private Key (d,n) = ?

Given: Public key (e,n) = (5,221)

Solution: $n = p \times q = 221$

∴ Let p = 13   q = 17

∴ $n = 13 \times 17 = 221$

$\phi(n) = (p-1)(q-1) = 12 \times 16 = 192$

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

$5de = 1 \bmod (\phi(n))$

~~B~~ $d = \frac{1 + K(\phi(n))}{5}$ -- [K is constant and its value is 0,1,2,3,....]

$\boxed{d = 72}$

∴ Private key of B is = (d,n) = (77, 221)

iii) What will be the cipher text sent by A to B . If A wishes to send M = 5 to B

To Find: C = ?

~~Where: M = 5~~

~~N = 221~~

A wants to send M = 5 to B using public Key (5, 221)

∴ M = 5   n = 221   e = 5

Encryption Formula

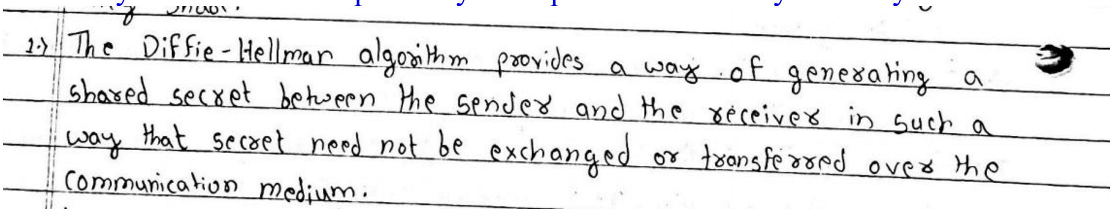
$C = M^e \bmod n$

$= 5^5 \bmod 221$

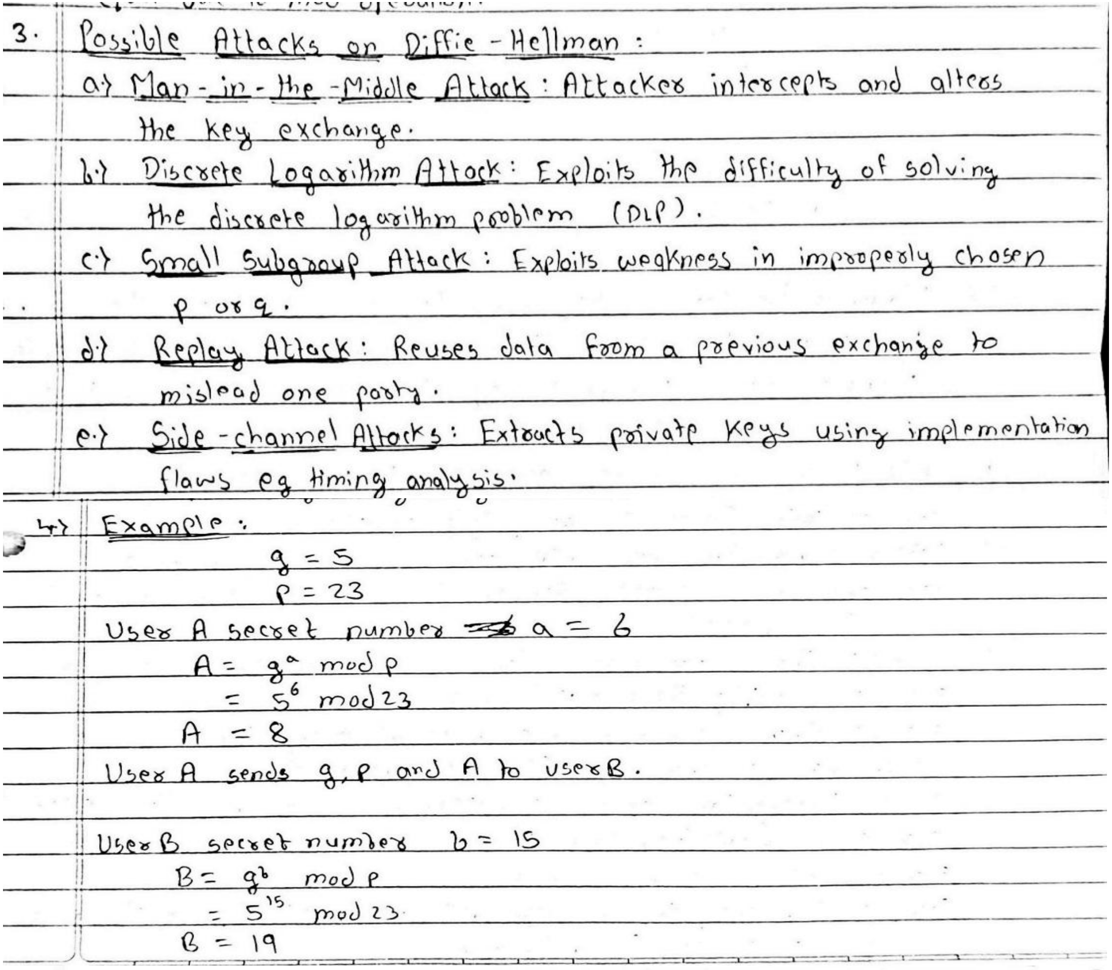
$C = 31$

∴ $\boxed{\text{Cipher text send to B is} = 31}$

5. Explain Diffie Hellman key agreement algorithm. Also discuss the possible attacks on it. Consider the example where A and B decide to use the Diffie Hellman algorithm to share a key. They choose p=23 and g=5 as the public parameters. Their secret keys are 6 and 15 respectively. Compute the secret key that they share.



1.) The Diffie-Hellman algorithm provides a way of generating a shared secret between the sender and the receiver in such a way that secret need not be exchanged or transferred over the communication medium.



3. Possible Attacks on Diffie-Hellman :

a) Man-in-the-Middle Attack : Attacker intercepts and alters the key exchange.

b) Discrete Logarithm Attack : Exploits the difficulty of solving the discrete logarithm problem (DLP).

c) Small Subgroup Attack : Exploits weakness in improperly chosen p or q.

d) Replay Attack : Reuses data from a previous exchange to mislead one party.

e) Side-channel Attacks : Extracts private keys using implementation flaws eg timing analysis.

4.) Example :

$g = 5$

$p = 23$

User A secret number ~~a~~ $a = 6$

$A = g^a \bmod p$

$= 5^6 \bmod 23$

$A = 8$

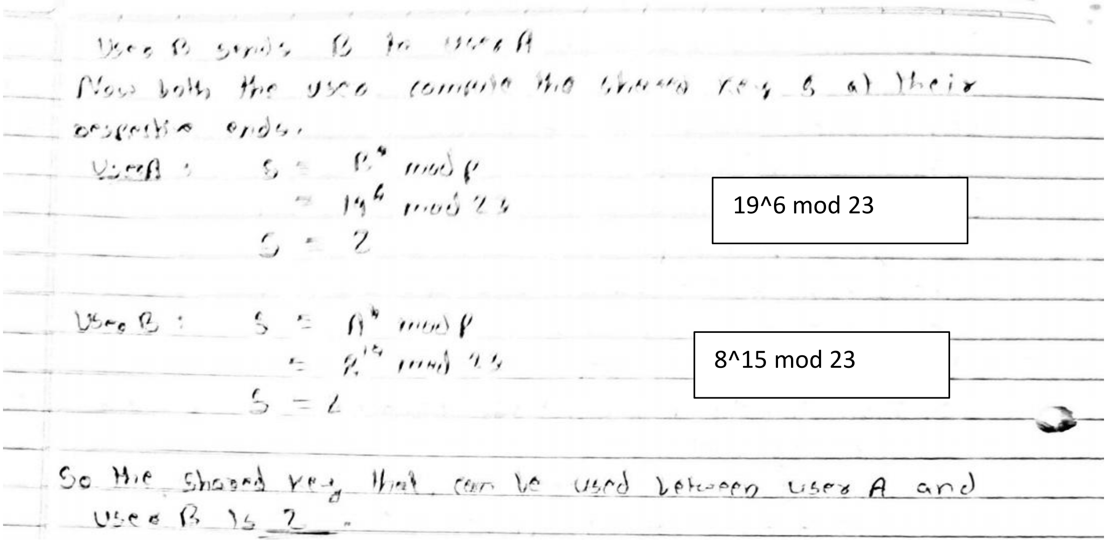
User A sends g, p and A to user B.

User B secret number $b = 15$

$B = g^b \bmod p$

$= 5^{15} \bmod 23$

$B = 19$



User B sends B to user A

Now both the user compute the shared key S at their respective ends.

UserA : $S = B^a \bmod p$

$= 19^6 \bmod 23$

$S = 2$

19^6 mod 23

User B : $S = A^b \bmod p$

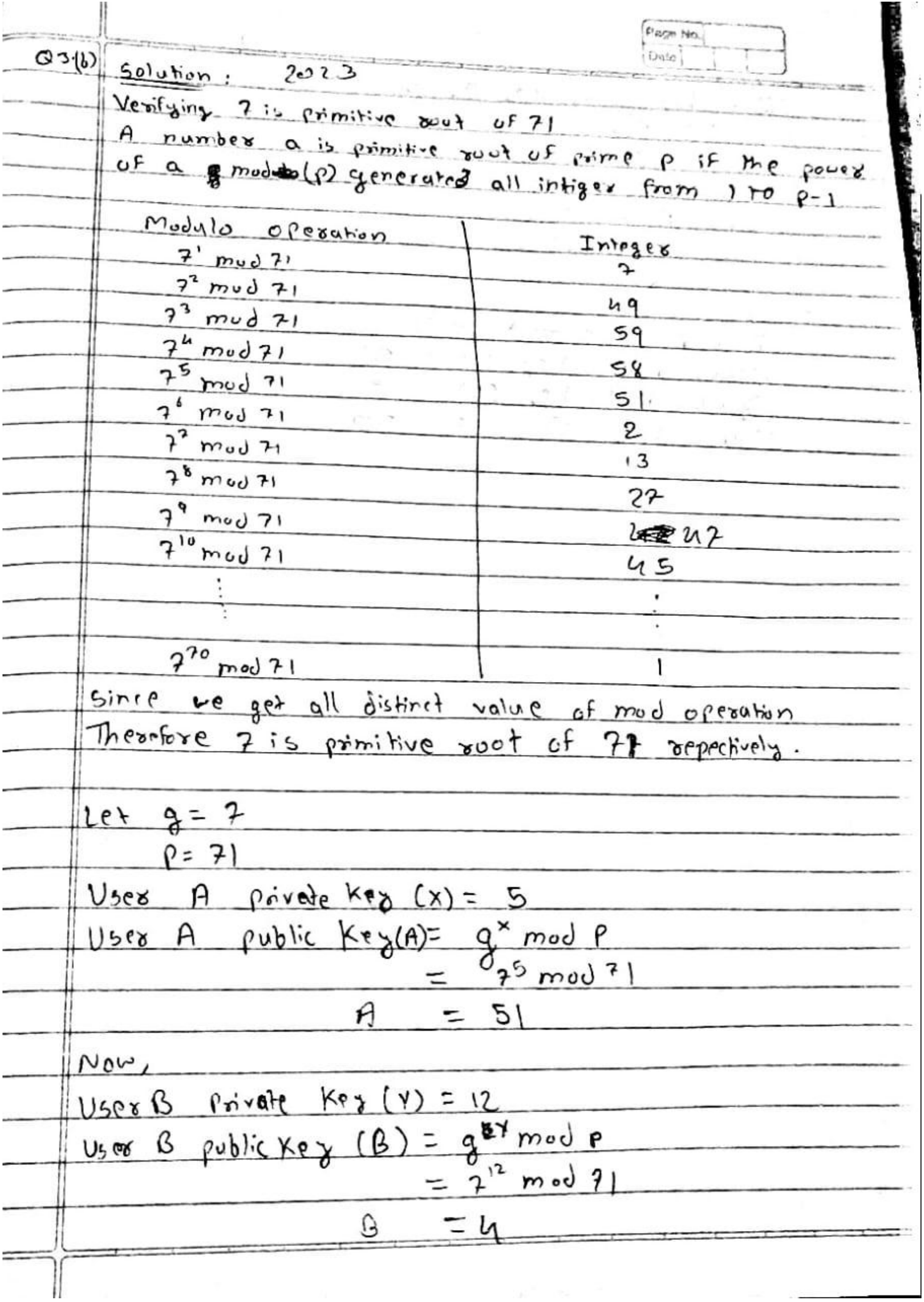
$= 8^{15} \bmod 23$

$S = 2$

8^15 mod 23

So the shared key that can be used between user A and user B is 2.

6. Users A and B use the Diffie-Hellman key exchange technique with a common prime 71 and primitive root 7. Show that 7 is primitive root of 71. If user A has private key x=5, what is A's Public Key R1? If user B has private key y=12, what is B's public key R2? What is the shared secret key?(Q3.b)



Page No.
Date

Q3.(b) Solution : 2023

Verifying 7 is primitive root of 71
A number a is primitive root of prime p if the power of a mod (p) generated all integer from 1 to p-1

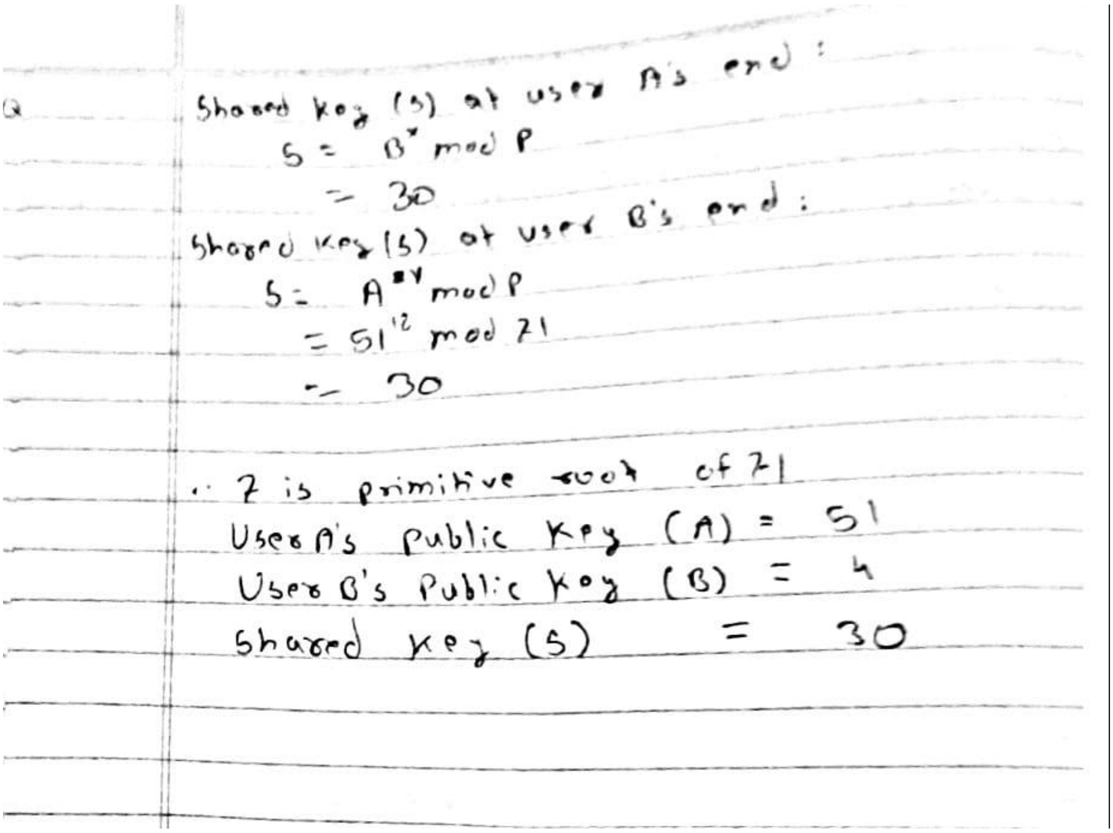
Modulo operation	Integer
7^{1} mod 71	7
7^{2} mod 71	49
7^{3} mod 71	59
7^{4} mod 71	58
7^{5} mod 71	51
7^{6} mod 71	2
7^{7} mod 71	13
7^{8} mod 71	27
7^{9} mod 71	47
7^{10} mod 71	45
⋮	⋮
7^{70} mod 71	1

Since we get all distinct value of mod operation
Therefore 7 is primitive root of 71 repectively.

Let $g = 7$
$p = 71$

User A private key $(x) = 5$
User A public Key$(A) = g^{x} \bmod p$
$= 7^{5} \bmod 71$
$A = 51$

Now,
User B Private Key $(y) = 12$
User B public Key $(B) = g^{y} \bmod p$
$= 7^{12} \bmod 71$
$B = 4$



Q

Shared key (S) at user A's end :

$S = B^{x} \bmod P$

$= 30$

Shared key (S) at user B's end :

$S = A^{y} \bmod P$

$= 51^{12} \bmod 71$

$= 30$

∴ 7 is primitive root of 71

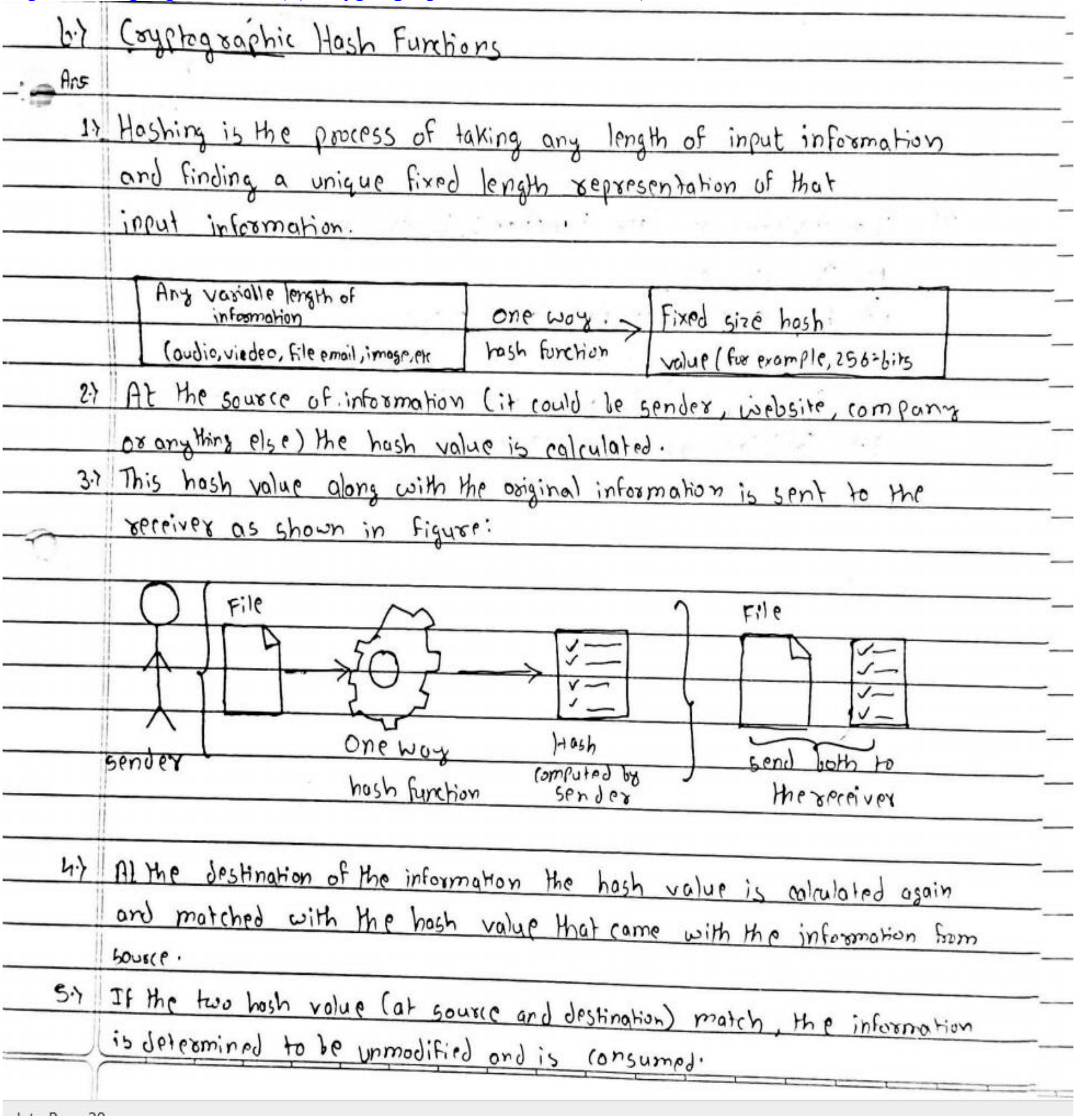
User A's public key (A) = 51

User B's Public key (B) = 4

Shared key (S) = 30

Module 3:

1. Explain cryptography hash function criteria and compare MD-5 and SHA-1(Q3.a)(Define and explain the properties of:(b) Cryptographic hash functions)



b.) Cryptographic Hash Functions

Ans

1.) Hashing is the process of taking any length of input information and finding a unique fixed length representation of that input information.

Any variable length of information (audio, viedeo, file email, image, etc) → one way hash function → Fixed size hash value (for example, 256-bits)

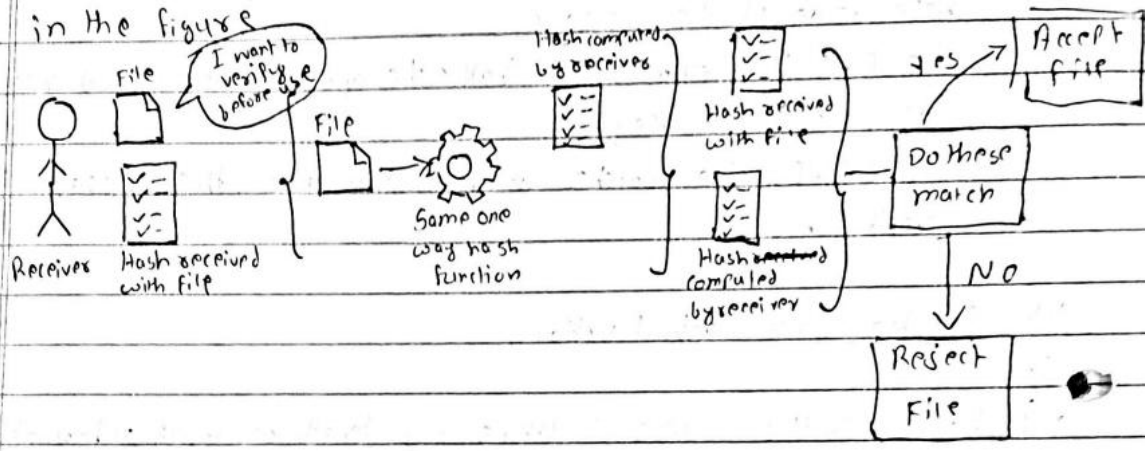
2.) At the source of information (it could be sender, website, company or anything else) the hash value is calculated.

3.) This hash value along with the original information is sent to the receiver as shown in figure:

4.) At the destination of the information the hash value is calculated again and matched with the hash value that came with the information from source.

5.) If the two hash value (at source and destination) match, the information is determined to be unmodified and is consumed.

6.> But if the two hash values do not match it proves that the information is altered and is often rejected. as shown in the figure


I want to verify before use
File
Receiver
Hash received with file
File
Same one way hash function
Hash computed by receiver
Hash received with file
Hash ~~received~~ computed by receiver
Do these match
Yes
Accept file
No
Reject File

7.> Characteristics of Hash Functions is as follows:

A.> One way only.

B.> Any length input, fixed length output

C.> No secrecy involved

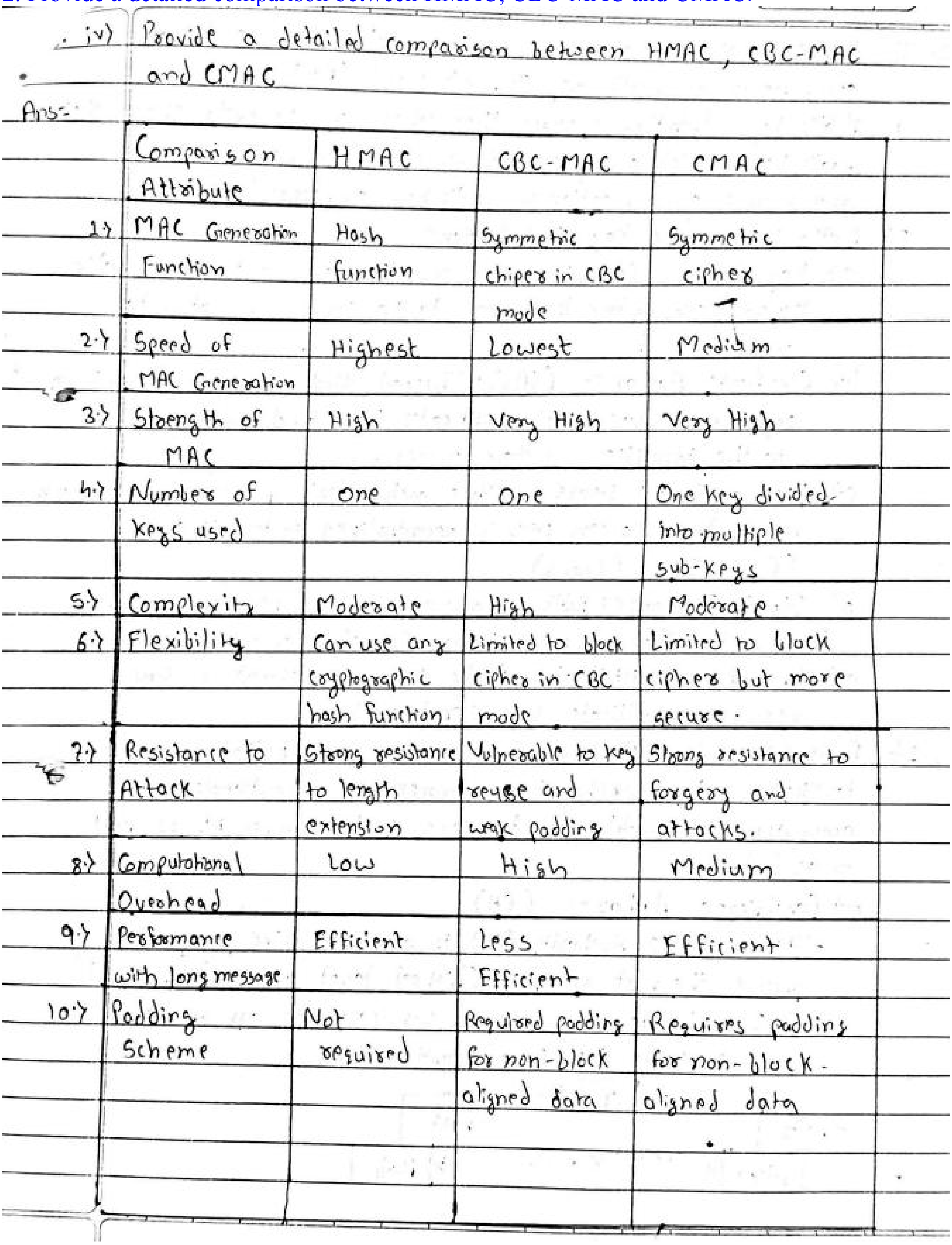
D.> Small input variation produces large output variation

E.> Collisions are possible.

goals.

Sr. No.	SHA-1	MD5
1.	It uses a 160-bit message digest. Hence it is stronger against Brute - force attacks than MD5.	It uses a 128 bit message digest. Hence it is weaker than SHA1 against Brute - force attacks.
2.	SHA-1 is not vulnerable against cryptanalysis.	MD5 is vulnerable against cryptanalysis
3.	SHA-1 is slower than MD5.	MD5 is faster than SHA-1.
4.	It uses big - endian method to represent the message.	It uses a little endian method to represent the message.
5.	SHA has 20 rounds.	MD5 has 64 rounds.
6.	Bit rotation counts for SHA - 1 are the same for all rounds.	In MD5 each round has its own bit rotation counts.

2. Provide a detailed comparison between HMAC, CBC-MAC and CMAC.



iv) Provide a detailed comparison between HMAC, CBC-MAC and CMAC

Ans:-

	Comparison Attribute	HMAC	CBC-MAC	CMAC
1.)	MAC Generation Function	Hash function	Symmetric chiper in CBC mode	Symmetric cipher
2.)	Speed of MAC Generation	Highest	Lowest	Medium
3.)	Strength of MAC	High	Very High	Very High
4.)	Number of Keys used	One	One	One key divided into multiple sub-keys
5.)	Complexity	Moderate	High	Moderate
6.)	Flexibility	Can use any cryptographic hash function.	Limited to block cipher in CBC mode	Limited to block cipher but more secure.
7.)	Resistance to Attack	Strong resistance to length extension	Vulnerable to key reuse and weak padding	Strong resistance to forgery and attacks.
8.)	Computational Overhead	Low	High	Medium
9.)	Performance with long message	Efficient	Less Efficient	Efficient
10.)	Padding Scheme	Not required	Required padding for non-block aligned data	Requires padding for non-block aligned data

2024:

Q1.a) What are the security mechanisms for non-repudiation? (2)

Q1.b) What are the strengths and weaknesses of Playfair Cipher? (2)

Q1.c) What is the difference between diffusion and confusion? (2)

Q1.d) Write a short note on steganography. (2)

Q2.a) What are the different modes of operation in block cipher? (7)

Q2.b) Explain RSA cryptosystem. In RSA Given n=221 and e=5 find d. (7)

Q3.a) Explain cryptography hash function criteria and compare MD-5 and SHA-1(7)

Q3.b) What is message digest? Explain HMAC algorithm.(7)

2023:

Q1.a) Compare MD5 and SHA 1 Hash functions.(2)

Q1.b) Explain with examples keyed and keyless transposition cipher.(2)

Q1.c) Explain the relationship between security services & mechanism. (2)

Q1.d) List down the different types of active & passive attacks. (2)

Q2.a) Explain Kerberos in detail (7)

Q2.b) i) Explain ECB & CBC modes of block cipher. (4)

ii) Compare AES and DES. (3)

Q3.a) If A and B wishes to use RSA to communicate securely, A chooses public key (e,n) as (7,247) and B chooses public key (e, n) as (5,221) (7)

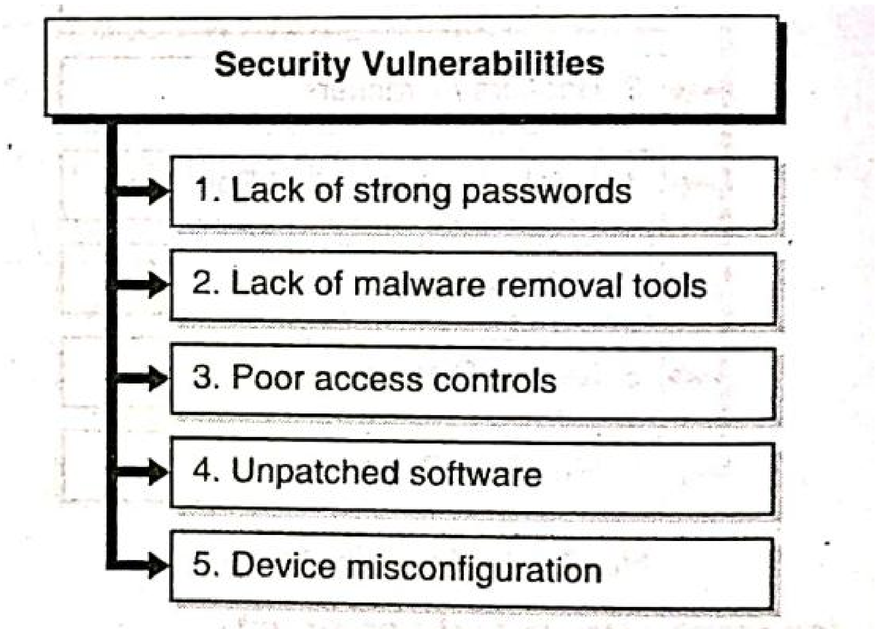
i)Calculate A's private key

ii) Calculate B's Private Key

iii) What will be the cipher text sent by A to B, If A wishes to send M-5 to B

Q3.b) Users A and B use the Diffie-Hellman key exchange technique with a common prime 71 and primitive root 7. Show that 7 is primitive root of 71. If user A has private key x=5, what is A's Public Key R1? If user B has private key y=12, what is B's public key R2? What is the shared secret key?(7)

Assignment:

i)	Explain the following System security terms in detail with examples: (a) Security mechanism;(b) Non-repudiation;(c) Integrity and (d) Confidentiality
ii)	How vulnerabilities are exploited to launch an attack? List various software vulnerabilities.  Security Vulnerabilities 1. Lack of strong passwords 2. Lack of malware removal tools 3. Poor access controls 4. Unpatched software 5. Device misconfiguration **Fig. 1.3.2 : Security Vulnerabilities**
iii)	A secure e-voting system is to be designed. Discuss the security goals that must be met and enlist the mechanisms for the same.
iv)	Explain the following Ciphers with illustrative example: (a) Playfair cipher; (b) Transposition cipher and (c) Vignere cipher
Q2	
i)	What are Block Ciphers? Explain different modes of block ciphers with detailed diagram.
ii)	Explain Diffie Hellman key agreement algorithm. Also discuss the possible attacks on it. Consider the example where A and B decide to use the Diffie Hellman algorithm to share a key. They choose p=23 and g=5 as the public parameters. Their secret keys are 6 and 15 respectively. Compute the secret key that they share.
iii)	Explain Advanced Encrypted Standards in detail. Highlight the difference between AES and DES.
iv)	Elaborate the steps of key generation using the RSA algorithm. In RSA system the public key (E, N) of user A is defined as (7,187). Calculate Φ (N) and private key 'D'. What is the cipher text for M=10 using the public key.
v)	Discuss RC5 Algorithm with reference to the following points: 1. Major Attributes of RC5.

	2. Internals of RC5 Algorithm. 3. Key Expansion. 4. Encryption.
vi)	Define, explain and give the major attributes of: (a) ElGamal Algorithm (b) Knapsack Algorithm
Q3	
i)	Explain the terms along with their applications in System Security: (a) Digital signatures and (b) Digital certificate
ii)	Explain public key distribution in detail while stating the components of Public Key Infrastructure (PKI).
iii)	Define and explain the properties of: (a) Message Authentication and (b) Cryptographic hash functions
iv)	Provide a detailed comparison between HMAC, CBC-MAC and CMAC.

Terna Engineering College

Computer Engineering Departmen:

FH 2024

Internal Assessment Test – I (IAT -I)

Subject: Cryptography & System Security (CSC602)

Max. Marks: 20

Sem: VI

Duration: 1 Hr

Note:

1. Attempt all questions.
2. Draw neat diagrams wherever necessary.
3. Write everything in ink (no pencil) only.
4. Assume suitable data if required.

Q. No.		Questions	Marks
Q1		Solve any three	6
	a)	What are the security mechanisms for non-repudiation?	2
	b)	What are the strengths and weaknesses of Playfair Cipher?	2
	c)	What is the difference between diffusion and confusion?	2
	d)	Write a short note on steganography.	2
Q2		Solve any one.	7
	a)	What are the different modes of operation in block cipher?	
	b)	Explain RSA cryptosystem. In RSA Given n=221 and e=5 find d.	
Q3		Solve any one.	7
	a)	Explain cryptography hash function criteria and compare MD-5 and SHA-1	
	b)	What is message digest? Explain HMAC algorithm.	

Terna Engineering College

Computer Department

Internal Assessment Test (IAT)

Subject: CSS **Sem: VI**

Max. Marks: 20 **Duration: 1 Hr**

Q1) Solve any THREE **(6)**

1(a). Compare MD5 and SHA 1 Hash functions. (2)

1(b) Explain with examples keyed and keyless transposition cipher. (2)

1(c) Explain the relationship between security services & mechanism. (2)

1 (d) List down the different types of active & passive attacks. (2)

(7)

Q2) Solve any ONE. (7)

2(a) Explain Kerberos in detail

OR

2(b) i) Explain ECB & CBC modes of block cipher. (4)

ii) Compare AES and DES. (3)

(7)

Q3) Solve any ONE.

a) If A and B wishes to use RSA to communicate securely, A chooses public key (e,n) as (7,247) and B chooses public key (e, n) as (5,221)
i)Calculate A's private key ii)Calculate B's Private Key

ii) What will be the cipher text sent by A to B, If A wishes to send M=5 to B

OR

b) Users A and B use the Diffie-Hellman key exchange technique with a common prime 71 and primitive root 7. Show that 7 is primitive root of 71. If user A has private key x=5, what is A's Public Key R1? If user B has private key y=12, what is B's public key R2? What is the shared secret key?