| Lalitha Aaradhini |P.Rajeshwari|P.PriyaNandini

CRYPTOGRAPHY AND NETWORK SECURITY

MODULE-1

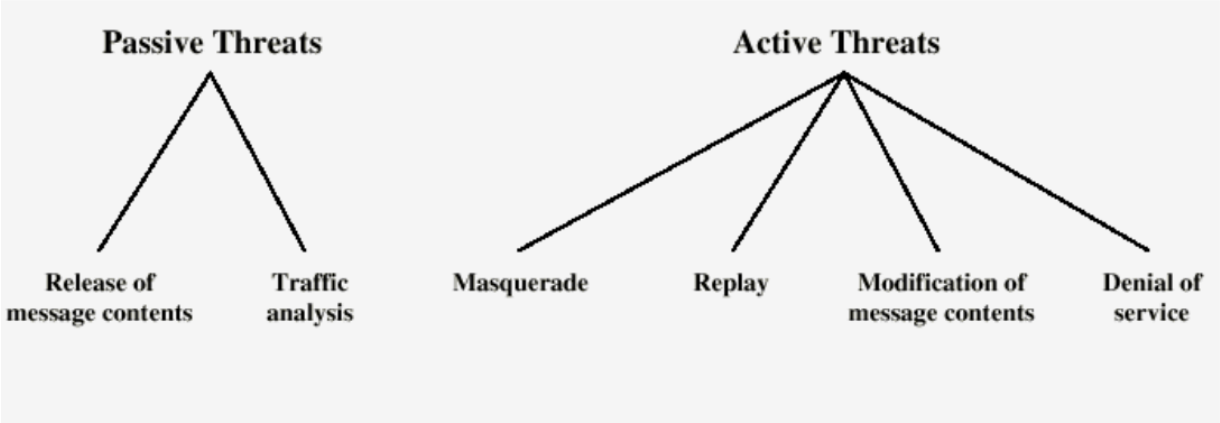
PART-B

1)Explain security attacks, security services and security mechanisms with neat diagrams?

Security attacks:A security attack is an activity or act made upon a system with the goal to obtain unauthorized access to information or resources. It is usually carried out by evading security policies that are in place in organizations or individual devices.

Types of security attacks

1)passive threats
2)active threats



Security services:It is a processing or communication service that is provided by a system to give a specific kind of production to system resources. Security services implement security policies and are implemented by security mechanisms.

1)Confidentiality
2)Authentication

i)Peer entity authentication
ii)Data origin authentication

3)Integrity
i)Connection-Oriented Integrity Service
ii)Connectionless-Oriented Integrity Service

4)Non-repudiation
5)Access Control
6)Availability

Security mechanisms: the security mechanisms are divided into those implemented in a specific protocol layer and those that are not specific to any particular protocol layer or security service. X.800 also differentiates reversible & irreversible encipherment mechanisms.

1)Specific security mechanisms
i)digital signature
ii)access control
iii)data integrity
iv)traffic padding
v)Routing control
vi)Notarization

2)Pervasive Security Mechanisms
i)Trusted Functionality
ii)Security Level
iii)Event Detection
iv)Security Audit Trail
v)Security Recovery

2)Classify cryptanalysis and explain the amount of information known to cryptanalysts? What is cryptanalysis?

The process of attempting to discover X or K or both is known as cryptanalysis. The strategy used by the cryptanalysis depends on the nature of the encryption scheme and the information available to the cryptanalyst.

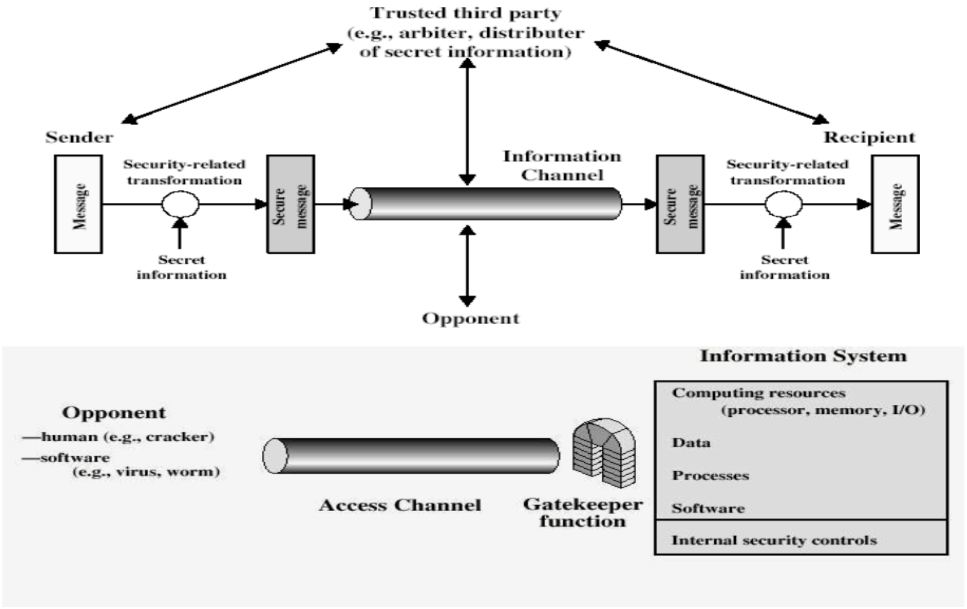
There are various types of cryptanalytic attacks based on the amount of information known to the cryptanalyst.

Ciphertext only– A copy of cipher text alone is known to the cryptanalyst. Known **plaintext**– The cryptanalyst has a copy of the cipher text and the corresponding plaintext.

Chosen plaintext – The cryptanalysts gain temporary access to the encryption machine. They cannot open it to find the key, however; they can encrypt a large number of suitably chosen plaintexts and try to use the resulting cipher texts to deduce the key.

Chosen ciphertext – The cryptanalyst obtains temporary access to the decryption machine, uses it to decrypt several string of symbols, and tries to use the results to deduce the key.

3)Illustrate models for inter network security with a neat diagram?



The general model shows that there are four basic tasks in designing a particular security service:
1. Design an algorithm for performing the security-related transformation. The algorithm should be such that an opponent cannot defeat its purpose
2. Generate the secret information to be used with the algorithm
3. Develop methods for the distribution and sharing of the secret information
4. Specify a protocol to be used by the two principles that makes use of the security algorithm and the secret information to achieve a particular security service

4)Summarize various types of transposition techniques?

Transposition technique is an encryption method which is achieved by performing permutation over the plain text. Mapping plain text into cipher text using a transposition technique is called transposition cipher.

Rail fence is the simplest of such ciphers, in which the plaintext is written down as a sequence of diagonals and then read off as a sequence of rows.
Plaintext = meet at the school house To encipher this message with a rail fence of depth 2, We write the message as follows: m e a t e c o l o s e t t h s h o h u e The encrypted message is MEATECOLOSETTHSHOHUE

Row Transposition Ciphers-A more complex scheme is to write the message in a rectangle, row by row, and read the message off, column by column, but permute the order of the columns. The order of columns then becomes the key of the algorithm.
E.g:
plaintext = meet at the school house Key = 4 3 1 2 5 6 7 PT = m e e t a t t h e s c h o o l h o u s e
CT = ESOTCUEEHMHLAHSTOETO

Pure transposition cipher is easily recognized because it has the same letter frequencies as the original plaintext.

5)Illustrate Caesar cipher? And calculate the encryption and decryption for the plain text p=" COME TO MY HOME" by using caesar cipher with key=3?

The earliest known use of a substitution cipher and the simplest was by Julius Caesar. The Caesar cipher involves replacing each letter of the alphabet with the letter standing 3 places further down the alphabet.
e.g., plain text : pay more money
Cipher text: SDB PRUH PRAHA
Note that the alphabet is wrapped around, so that the letter following "z" is "a". For each plaintext letter p, substitute the cipher text letter c such that C = E(p) = (p+3) mod 26 A shift may be any amount, so that general Caesar algorithm is C = E (p) = (p+k) mod 26 Where k takes on a value in the range 1 to 25. The decryption algorithm is simply P = D(C) = (C-k) mod 26

Refer part-A 1st question for the solution.

6)Why do we use transposition techniques in cryptography?

Transposition is a simpler and more powerful technique than substitution because it not only substitutes the text, but also permutates the text.
—----------

7) Recognize possible types of attacks?

REFER PART B-1

8)Summarize 1. Transposition techniques 2. Steganography

1)**TRANSPOSITION TECHNIQUES**: refer part b 4

2)Steganography:
The methods of steganography conceal the existence of the message, whereas the methods of cryptography render the message unintelligible to outsiders by various transformations of the text. A simple form of steganography, but one that is time consuming to construct is one in which an arrangement of words or letters within an apparently innocuous text spells out the real message. e.g., (i) the sequence of first letters of each word of the overall message spells out the real (hidden) message.
(ii) Subset of the words of the overall message is used to convey the hidden message. Various other techniques have been used historically, some of them are
1. Character marking – selected letters of printed or typewritten text are overwritten in pencil. The marks are ordinarily not visible unless the paper is held to an angle to bright light.
2. Invisible ink – a number of substances can be used for writing but leave no visible trace until heat or some chemical is applied to the paper.
3. Pin punctures – small pin punctures on selected letters are ordinarily not visible unless the paper is held in front of the light.
4. Typewritten correction ribbon – used between the lines typed with a black ribbon, the results of typing with the correction tape are visible only under a strong light.
—----------

9)Describe the following a) Security attacks b) Security mechanisms
Refer part B 1 question

10)Explain various types of security attacks?
Refer part B 1 question

11)Classify cipher techniques in cryptography?
Refer part-A 2nd question

12)Distinguish plain text and cipher text?

Plain Text: This is the message or data in its natural format and in a readable form. Plain text is human-readable and extremely vulnerable from a confidentiality perspective. Plain text is also called cleartext. Plain text is a message or data that has not been turned into a secret.

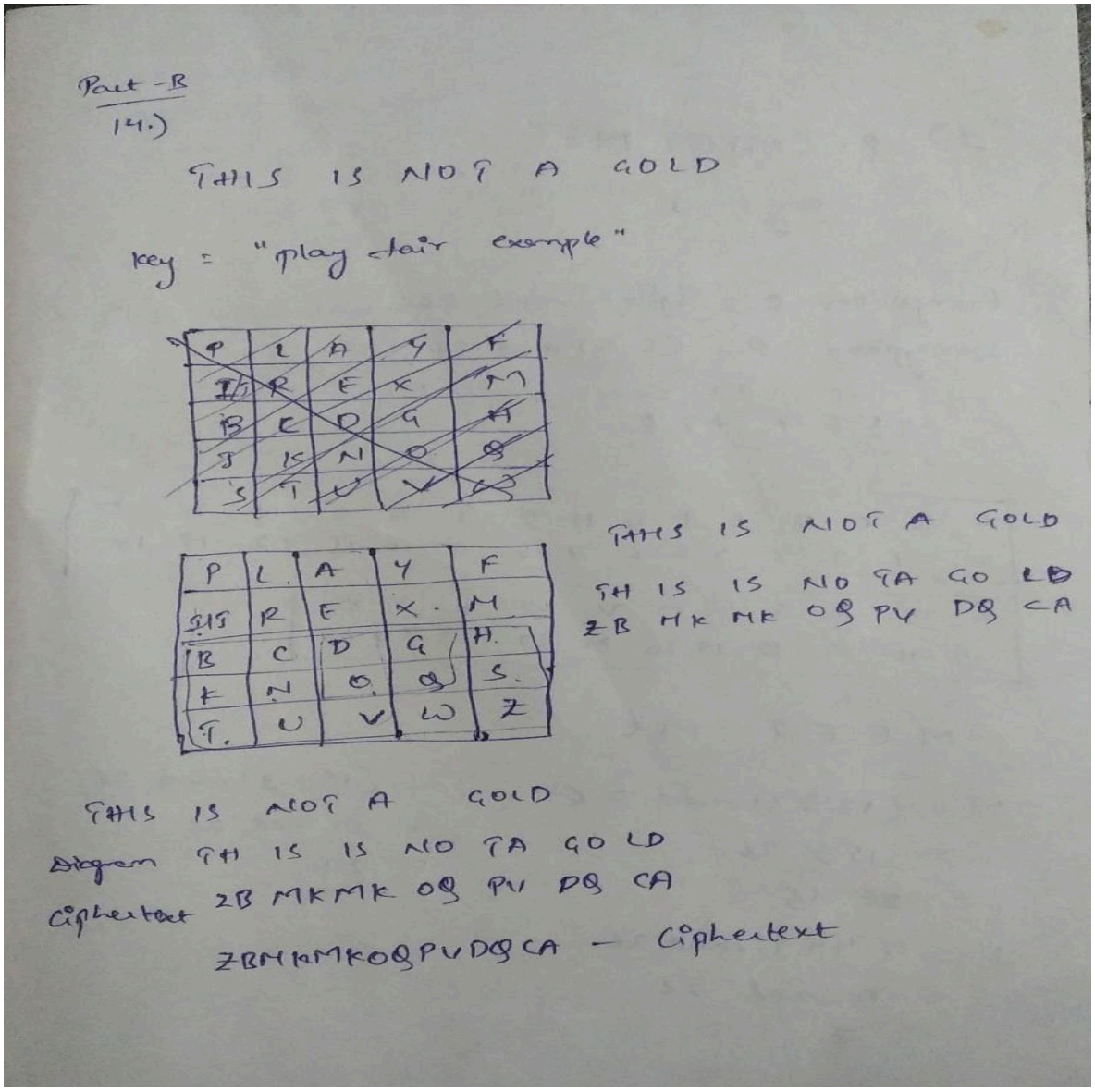
Cipher Text or Cryptogram: This is the altered form of plaintext message so as to be unreadable for anyone except the intended recipients. In other words, it has been turned into a

secret. An eavesdropper or an attacker seeing the ciphertext would be unable to easily read the **message or determine its content.**

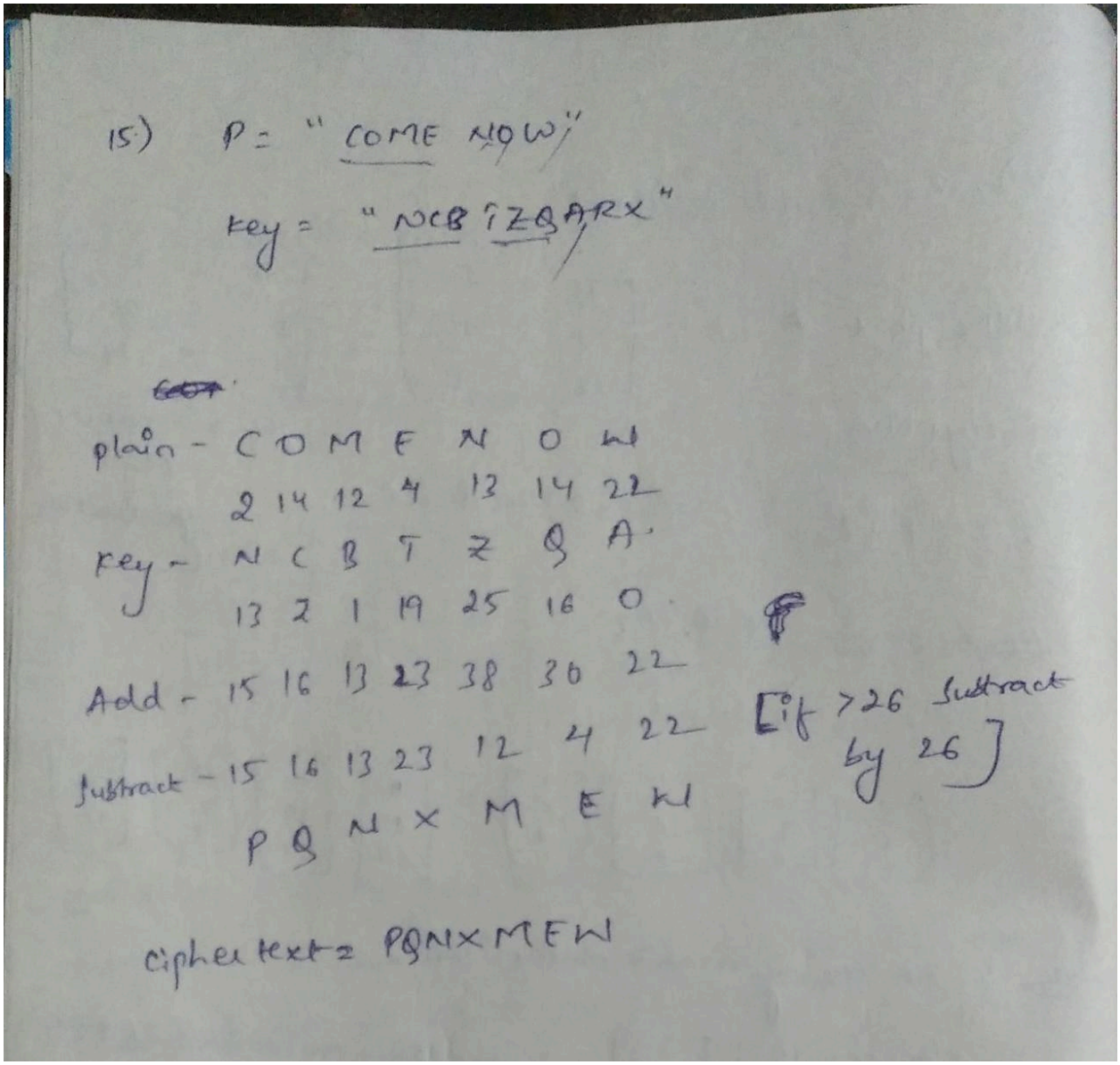
13)State the following plain text P=”TRUST MEE” into cipher text by using Hill cipher with key K= which is a 2X2 matrix (only encryption)?

A.) Same as part-A 4th question with random key (2X2)

14)Describe the following plain text message P=”THIS IS NOT A GOLD” into cipher text with key k=”play fair example” by using playfair cipher technique?



15)Outline the following plain text P=”COME NOW” into cipher text by using one-time pad cipher(Vernam cipher) with key K=”NCBTZQARX”?



16)Identify the following plain text message P=1110001 into cipher text by using a one- time pad cipher with key K=1011001.calculate both encryption and decryption for the above message?

16) P = 1110001

Key = 1011001 [Encryption & Decryption]

plain - 1 1 1 0 0 0 1

B B B A A A B

key - 1 0 1 1 0 0 1

B A B B A A B [Encryption].

Add 2 1 2 1 0 0 2

Subtract 2 1 2 1 0 0 2

C B C B A A C

Cipher - CBCBAAC

2 1 2 1 0 0 2

cipher C B C B A A C [Decryption]

1 0 1 1 0 0 1

key

1 1 1 0 0 0 1

cipher-key

1 1 1 0 0 0 1

plain

B B B A A A B

plain - BBBAAAB

17)Interpret poly-alphabetic ciphers with examples and its applications?

A polyalphabetic cipher is any cipher based on substitution, using multiple substitution alphabets.The Vigenère cipher is probably the best-known example of a polyalphabetic cipher, though it is a simplified special case. The relationship between a character in the plain text and the characters in the ciphertext is one-to-many.Polyalphabetic Cipher is described as substitution cipher in which plain text letters in different positions are enciphered using different crypto alphabets.Polyalphabetic ciphers are much stronger.

ex:Vigenère Cipher - GeeksforGeeks

18)Recall plain text, ciphers text, symmetric and asymmetric key cryptography?

Plain Text: This is the message or data in its natural format and in a readable form. Plain text is human-readable and extremely vulnerable from a confidentiality perspective. Plain text is also called cleartext. Plain text is a message or data that has not been turned into a secret.

Cipher Text or Cryptogram: This is the altered form of plaintext message so as to be unreadable for anyone except the intended recipients. In other words, it has been turned into a secret. An eavesdropper or an attacker seeing the ciphertext would be unable to easily read the message or determine its content.

symmetric key:Symmetric key cryptography is a type of encryption scheme in which the similar key is used both to encrypt and decrypt messages.Symmetric-key cryptography is called a shared-key, secret-key, single-key, one-key and eventually private-key cryptography. With this form of cryptography, it is clear that the key should be known to both the sender and the receiver that they shared. The complexity with this approach is the distribution of the key.

Asymmetric key:It is called a Public-key cryptography. There are two different keys including one key that is used for encryption and only the other corresponding key should be used for decryption. There is no other key that can decrypt the message and not even the initial key used for encryption. The style of the design is that every communicating party needs only a key pair for communicating with any number of other communicating parties.

19)Explain security mechanisms and a model for network security?

Security mechanisms:refer part b 1

Model for network security:refer part b 3

20)Distinguish Caesar ciphers and mono- alphabetic ciphers with examples?

Caesar cipher:refer part b 5th

Monoalphabetic cipher:A monoalphabetic substitution cipher, also known as a simple substitution cipher, relies on a fixed replacement structure. That is, the substitution is fixed for each letter of the alphabet. Thus, if "a" is encrypted to "R", then every time we see the letter "a" in the plaintext, we replace it with the letter "R" in the ciphertext

A simple example is where each letter is encrypted as the next letter in the alphabet: "a simple message" becomes "B TJ QMF NFL TBHF". In general, when performing a simple substitution manually, it is easiest to generate the ciphertext alphabet first, and encrypt by comparing this to the plaintext alphabet. The table below shows how one might choose to, and we will lay them out for this example.

Plaintext Alphabet	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
Ciphertext Alphabet	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A

PART-A

1.)Enumerate the Caesar cipher? And calculate the encryption and decryption for the following plain text P=”MEET ME” by using caesar cipher with Key k =3?

1.) P = "MEET ME"

key k = 3

Encryption C = (P+K) mod 26.

Decryption P = (C-K) mod 26.

MEET ME

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14

P	Q	R	S	T	U	V	W	X	Y	Z
15	16	17	18	19	20	21	22	23	24	25

MEET ME

M = (12+3) mod 26

= 15 % 26

= 15

E = (4+3) mod 26

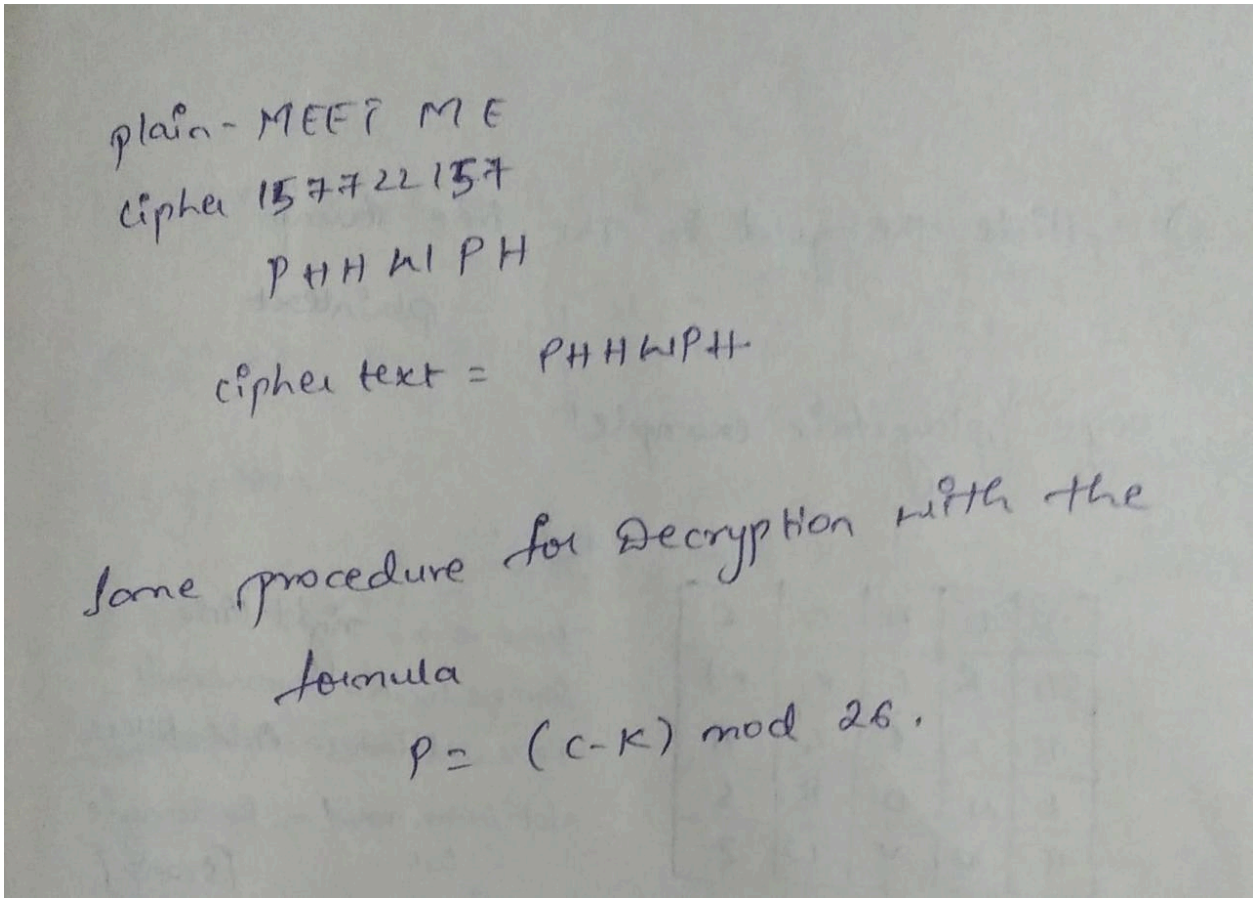
= 4 mod 26

= 7

T = (19+3) mod 26

= 22 mod 26

= 22



2.)Interpret and contrast all kinds of cipher techniques in cryptography?

https://www.educba.com/types-of-cipher/

3.)Explain the following plain text message P=”Hide the gold in the tree stump” into cipher text with key k=”play fair example” by using play fair cipher technique?

3) "Hide the gold in the tree stump"
- plaintext

Key = "playfair example"

P	L	A	Y	F
I/J	R	E	X	M
B	C	D	G	H
K	N	O	Q	S
T	U	V	W	Z

Rules:

Same row - right side
Same column - Downwards
Repeated letter - Add fillers
Not same row/col - Rectangle [Swap]

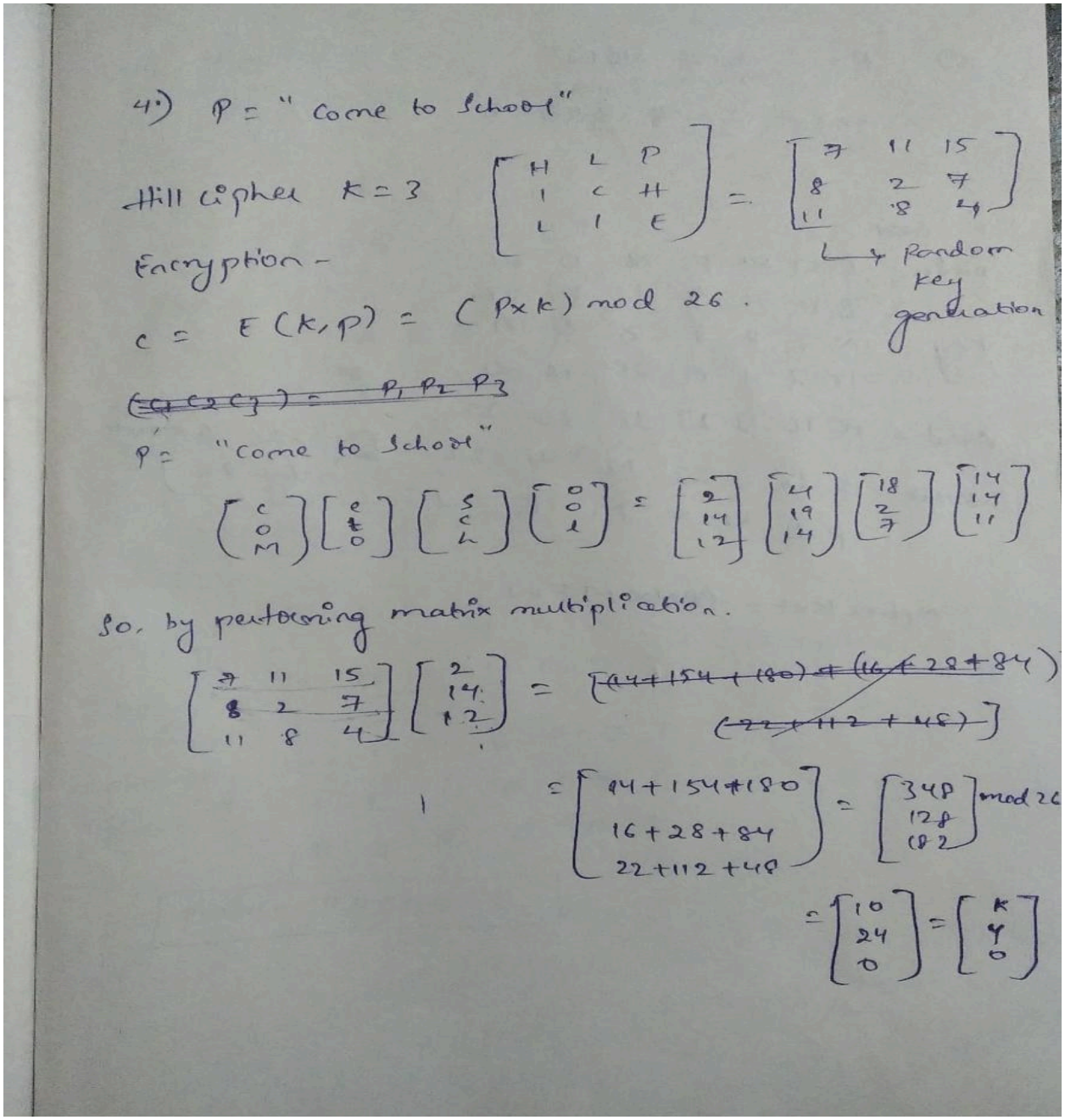
plaintext: Hide the gold in the tree stump

Diagram - Hi de th eg ol di nt he tr ee
BM OD ZB XD AN BE KU DM IU

ex es tu mp
XM MO VV IF

Ciphertext - BMODZBXDANBEKUDMIUXMMOUVIF

4.)Indicate the following plain text P=”Come To School” into cipher text by using Hill cipher with key K= 3?



$$\rightarrow \begin{bmatrix} 7 & 11 & 15 \\ 8 & 2 & 7 \\ 11 & 8 & 4 \end{bmatrix} \begin{bmatrix} 4 \\ 19 \\ 19 \end{bmatrix} = \begin{bmatrix} (28+209+210) \\ (32+38+98) \\ (44+152+56) \end{bmatrix}$$

$$= \begin{bmatrix} 447 \\ 168 \\ 252 \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} 5 \\ 12 \\ 18 \end{bmatrix} = \begin{bmatrix} F \\ M \\ S \end{bmatrix}$$

$$\rightarrow \begin{bmatrix} 7 & 11 & 15 \\ 8 & 2 & 7 \\ 11 & 8 & 4 \end{bmatrix} \begin{bmatrix} 18 \\ 2 \\ 7 \end{bmatrix} = \begin{bmatrix} (253) \\ (69) \\ (242) \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} 19 \\ 17 \\ 8 \end{bmatrix} = \begin{bmatrix} T \\ R \\ I \end{bmatrix}$$

$$\rightarrow \begin{bmatrix} 7 & 11 & 15 \\ 8 & 2 & 7 \\ 11 & 8 & 4 \end{bmatrix} \begin{bmatrix} 14 \\ 14 \\ 11 \end{bmatrix} = \begin{bmatrix} 417 \\ 217 \\ 310 \end{bmatrix} \bmod 26 = \begin{bmatrix} 1 \\ 9 \\ 24 \end{bmatrix}$$

$$= \begin{bmatrix} B \\ J \\ Y \end{bmatrix}$$

The ciphertext generated is:

KYOFMSTRIBJY

5.)Find the following plaintext message P=” cryptography provides High security ”into cipher text by using simple columnar transposition technique

a) Basic technique

b.)With multiple rounds

5i) Part-A

P- "cryptography provides High security"

Columnar transposition Technique

a) Basic technique

	1	2	3	4	5	6
1	C	R	Y	P	T	O
2	G	R	A	P	H	Y
3	P	R	O	U	I	D
4	F	S	H	I	G	H
5	S	F	C	U	R	I
6	T	Y				

6×6 = 36

Key = 432143 ← Random generation

[Make sure when generating the key, the digits should be >= Column size

→ no. of digits == Column size

Key = 432143

= ~~PPVIUZ YAOHCX~~

= PPVIU YAOHC R R R S F Y C G P F S T P P V I U Y A O H C

← Cipher text

6.)Compare and contrast all kinds of cipher techniques in cryptography?

A.) Same as Part-a 2nd question.

7.)Convert the following plain text message P=”we are discovered save yourself” into ciphertext with key K=”deceptive” with key repetition?

7.) P: "we are discovered save yourself"

K: "deceptive"

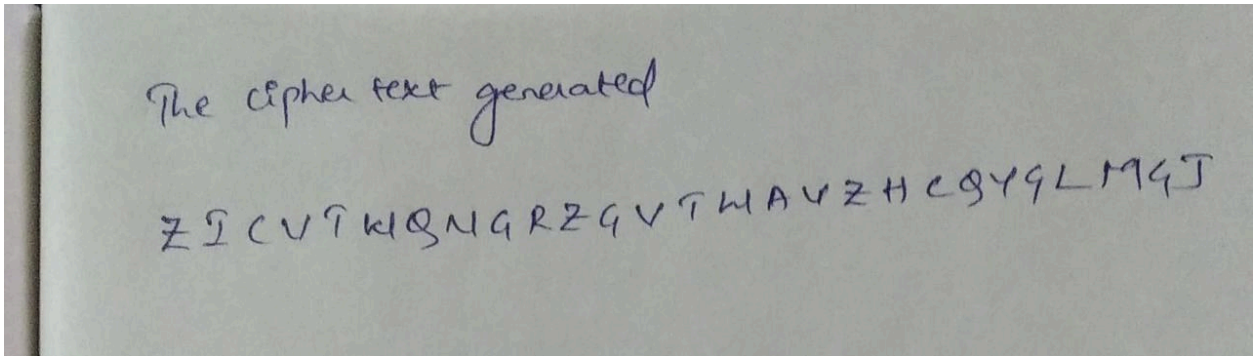
plaintext: "wearediscoveredsaveyourself

key: "deceptivedeceptivedeceptive

plain	22	4	0	17	4	3	8	18	2	14	21	4	17	4	3		
key	3	4	2	4	15	19	8	21	4	3	4	2	4	15	19		
cipher	25	8	2	21	19	22	16	39	6	17	25	6	21	19	22		
								↓									
								13									

plain	18	0	21	4	24	14	20	17	18	4	11	5					
key	8	21	4	3	4	2	4	15	19	8	21	4					
cipher	26	21	25	7	28	16	24	32	37	12	32	9					
	↓				↓			↓	↓		↓						
	0				2			6	11		6						

If the cipher digit is >=26 perform mod 26 operation with the digit



8.)Explain in details about the following terms with examples: a) security attacks b) security services c) security mechanism d) plain text e) cipher text f) substitution techniques g) transposition techniques

—----------

9.)Explain the concept of Key Range and Key Size, possible types of attacks?

A.)The concept of key range and key-size are related to each other. Key Range is the total number of keys from smallest to largest available key. An attacker usually is armed with the knowledge of the cryptographic algorithm and the encrypted message, so only the actual key value remains the challenge for the attacker.

• If the key is found, the attacker can get the original plaintext message. In the brute force attack, every possible key in the key-range is tried, until we get the right key.
• In the best case, the right key is found in the first attempt, in the worst case, the key is found in the last attempt. On an average, the right key is found after trying half of the possible keys in the key-range. Therefore by expanding the key range to a large extent, longer it will take longer for an attacker to find the key using brute-force attack.

• The concept of key range leads to the principle of key size. The strength of a cryptographic key is measured with the key size

• Key size is measured in bits and is represented using a binary number system. Thus if the key range from 0 to 8, then the key size is 3 bits or in other words we can say if the

size is bits then the key range is 0 to 256. Key size may be varying, depending upon the applications and the cryptographic algorithm being used, it can be 40 bits, 56 bits, 128 bits & so on. In order to protect the cipher-text against the brute-force attack, the key-size should be such that the attacker can not crack it within a specified amount of time.

• From a practical viewpoint, a 40-bit key takes about 3 hours to crack, however a 41-bit key would take 6 hours and 42-bit key would take 12 hours & so on. This means every additional bit doubles the amount of time required to crack the key. We can assume that a 128 bit key is quite safe, considering the capabilities of today's computers. However as the computing power and techniques improve, these numbers will change in future.

10.)Illustrate transposition techniques and substitution techniques?

A.) SUBSTITUTION TECHNIQUES

https://binaryterms.com/substitution-technique-in-cryptography.html

TRANSPOSITION TECHNIQUES

https://www.educba.com/transposition-techniques/