Conventional Cryptography

* Explain Types of Cryptography.

=> The study of Encryption method or Principles is know as Cryptography.

Cryptography contains different type of Method For the encrypt the data.

Using This Cryptography Methods we can convert readable data into unreadable form of data.

There are Two Types of Cryptography.

(a) Symmetric Key
(b) Asymmetric Key

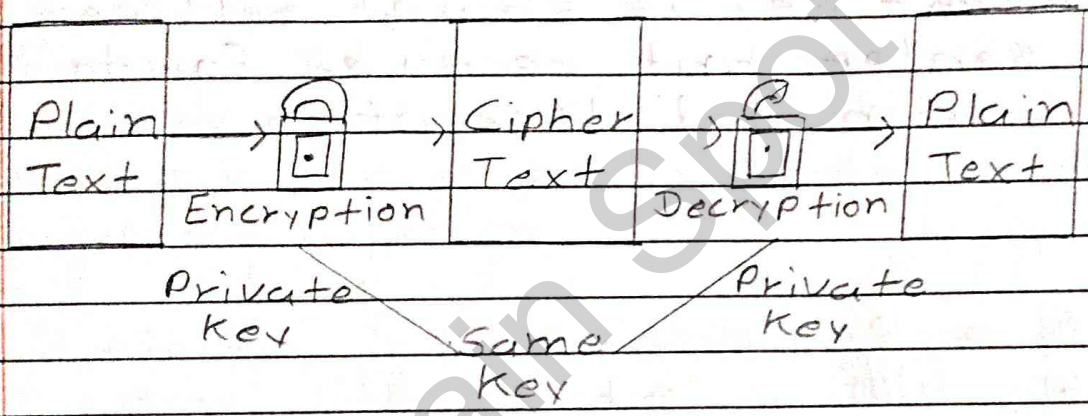
a Symmetric Key:

In Symmetric Key cryptography, the ~~ra~~ same key is used For both encryption and Decryption.

This Method is a Fast and efficient in working.

Single Key is shared between Sender and Receiver For the encryption and decryption.

Symmetric Key are well-suited For bulk data encryption and high-speed communication.



Symmetric is also known as a Private Key.

Plain text and Cipher text as same as Original size of text.

Usually the size of Key is 128 or 256 bits.

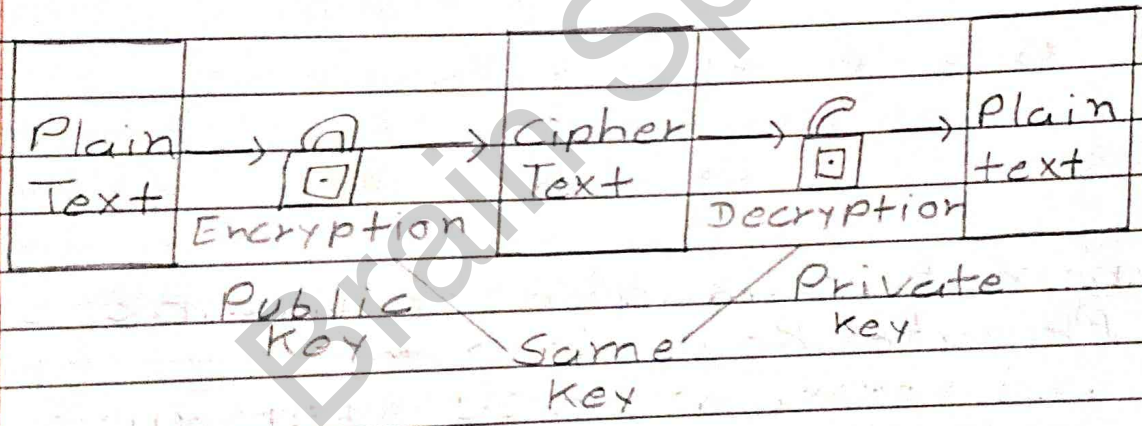
In this method, attacker gains access to the key and they can Encrypt and Decrypt all the data.

b Asymmetric Key:

In Asymmetric Key Cryptography the different key is used for encryption and decryption.

This method is very slower and complex in working.

Different key is shared between the sender and receiver for do encryption and decryption.



Asymmetric key is also known as Public key Cryptography.

Cipher text size is bigger than the plain text size.

Usually, the size of key is 1000 bits.

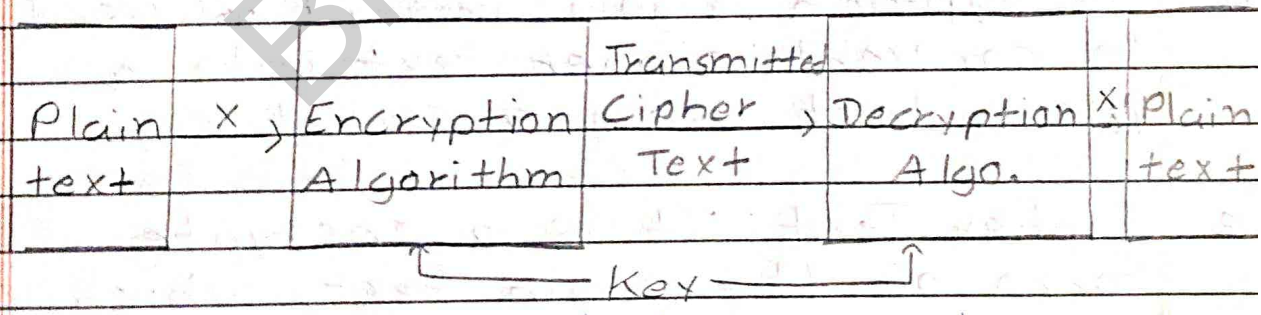
* Explain Conventional Encryption.

=> Conventional Encryption is an oldest method of the encryption.

Conventional Encryption is also known as Symmetric Cipher Method.

Conventional Encryption is a type of encryption in which we have to use same key for encryption and decryption.

This key is also known as Private Key as Symmetric key as Secret Key as Conventional key.



Here, Sender and Receiver share a comman key for the encryption and decryption.

This model is consistes Mainly Five Partes

(a) Plain Text
(b) Encryption Algorithm
(c) Secret key
(d) Decryption Algorithm
(e) Cipher Text

a Plain text : This is a original data that can send by sender.

b Encryption Algorithm: It is used to convert plain text into a cipher text using a secret key.

c Secret Key: It is a value or string which is used to convert plain text into cipher text.

d Decryption Algorithm: It is used to convert cipher text into a plain text using a secret key.

e Cipher Text: It is a encrypte form of the plain text, which is created using a secret key.

In this model, secret key take as input and decodes the cipher text into a plain text.

And Give a Plain text as Output.

* Explain Types of Attacks on Conventional Encryption.

=> There are Two Types of Attacks on Conventional Encryption

(a) Cryptanalysis
(b) Brute Force Attack

(a) Cryptanalysis:

Cryptanalysis is a study of cryptographic algorithm.

There are Five Types of Cryptanalysis Attack.

(i) Ciphertext Only
(ii) Chosen Ciphertext
(iii) Known Plaintext
(iv) Chosen Plaintext
(v) Chosen Text.

i) Ciphertext Only:

In this types of Attack, only some ciphertext is already known and attacker tries to find the encryption method and It's Plain Text

(ii) Chosen Ciphertext:

In this type of attack, attacker gather the information by obtaining the chosen Ciphertext.

(iii) Known Plain text:

There are some Plain text and Cipher text pair is already known.

The attacker map them to find the encryption key.

(iv) Chosen Plain text:

In this type of attack, the attacker select the random plain texts.

After that attacker try to find the cipher text with its encryption key.

(v) Chosen Text:

In this type of attack, Plain text is chosen by the attacker with its cipher text generted with secret key.

(6) Brute Force Attack:

In this type of attack, attacker trying the every possible key for every plain text or cipher text.

Attacker Try to access the user accounts using the different parameteres.

It is a hacking method that uses trial and error to creak the cipher text encryption key.

* Explain Caesar Cipher with its example.

=> Caesar Cipher is a simple encryption method which is given by Julius Caesar.

In Caesar Cipher, Every latter of the alphabet is replaces by three place.

According to value of Key, we have to shift the alphabet.

If value of K is 4, then we have to perform Four letter of alphabet shifting.

Example : Three Place Shifting.

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

- Cipher text $C = (P + K) \bmod 26$

- Plain text $P = (C - K) \bmod 26$

where, P = Plain text
C = Cipher text
K = key

Ex. Plain text: BrainSpot with Key value = 3.

Cipher text: EudlqVSrW

=> Advantages:

This method is simple for working and we can easily implement the method.

=> Disadvantages:

- This method encryption and decryption algorithm are well known.
- Attacker have to try only 25 keys for the decryption.
- Language of plain text is very simple, So we can easily reconghizable the text.
- Brute Force attack can be done on this encryption.

* Explain Playfair Cipher with its example.

=> Playfair Cipher method is best known for multiple letter encryption cipher.

Playfair Cipher encryption is used 5 x 5 matrix for the encryption.

This 5 x 5 matrix is constrcted using a keyword (Monarchy).

↳ Exampl of I and J ke count as one letter

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

=> Rules :

1 Diagraph : Split the Plain text into a two word pair, If Plain text has odd number of letter than add the any letter.

IF Any letter occurance is 2nd time than add extra letter in word pair.

Ex. JAXX => JA XB XC

2 To Determine Cipher text From 5 x 5 matrix:

a) If Pair letter appere in the same row -> Right move.

b) If Pair letter appere in the same column -> Move Down.

c) If Pair letter appere in the different row and column

Rectangle => Swap

Ex. Key : BrainSpot
Plaintext : Gandhi

=> 5 x 5 Key Matrix.

B	r	a	i/J	n
s	p	o	t	c
d	e	f	g	h
k	l	m	n	q
t	u	w	x	z

=> Diagraph : ga nd hi

→ For ga : Both in different Row and column.

B	r	(a) →	i/J	n
S	P	O	+	C
d	e	F ←	(g)	H
K	L	m	n	q
+	U	W	X	Z

Cipher text : Fi

→ For nd : Both in different Row and column.

B	r	a	i/J	n
S	P	O	+	C
(d)	e	f	g	H
K	L	m	(n)	q
+	U	W	X	Z

Cipher text : gk

→ For hi : Both in different Row and column.

B	r	a	(i/J) →	n
S	P	O	+	C
d	e	F	g ←	(H)
K	L	m	n	q
+	U	W	X	Z

Cipher text : Jg

Cipher text : Figkjg

* Explain Vernam Cipher with its example.

=> Vernam Cipher encryption method use XOR operation for the encryption.

In Vernam Cipher Length of key and Plain text are always equal.

We have to perform XOR operation with keyword and plain text.

Vernam Cipher $C_i = P_i \oplus K_i$

where, C_i = i^{th} letter cipher text
P_i = i^{th} letter plain text
K_i = i^{th} letter keyword

For every plain text letter, we have to perform XOR operation with keyword letter.

For Performing the XOR operation, we have to convert every

plain text and keyword letter into a 5-bit binary number.

IF Binary number is greater than or equal to 26, so, ~~we~~ leave it, else, subtracte with 26.

Ex. Key : OAK
Plain text : SON

-> For O and S,

O -> 14 S 1 0 0 1 0
S -> 18 O ⊕ 0 1 1 1 0

1 1 1 0 0 = 28

So, 28 - 26 = 2 -> C

-> For, O -> 14 0 1 1 1 0
A -> 0 0 0 0 0 0

0 1 1 1 0 = 14

So, 14 -> O

-> For, N -> 13 0 1 1 0 1
K -> 10 0 1 0 1 0

0 0 1 1 1 = 7

So, 7 -> H

(ii) Monoalphabetic Cipher (Simple substitution):

It is an improvement of Caesar cipher.

Instead of shifting the alphabets by some numbers this scheme uses some permutation of the letters in alphabet.

The sender and Receiver decide on a randomly selected permutation of the letters of the alphabet.

With 26 letters in alphabet, the possible permutations are 26! which is equal to 4×1026

- Permutation: It is a finite set of element's 's' is an ordered sequence of all the elements of 's' with each element operating exactly once.

Ex. S: {a, b, c}
Permutation = 3! = 6

abc, acb, bac, cab, cba

Ex. In general these are n! permutations of a set of n elements, because the first element can be chosen in one of n ways, the second n-1 ways and third in n-2 ways.

As a First step, the relative frequency of the letters can be determined and compared to a stand and Frequency distribution of english

- Relative Freq. of English letters.

A - 8.147	O - 7.567
B - 1.492	P - 1.929
C - 2.782	Q - 0.095
D - 4.253	R - 5.987
E - 12.702	S - 6.327
F - 2.228	T - 9.056
G - 2.015	U - 2.758
H - 6.094	V - 0.978
I - 6.966	W - 2.36
J - 0.153	X - 0.15
K - 0.772	Y - 0.1974
L - 4.025	Z - 0.074
M - 8.406	
N - 0.749	

Ex. Ciphertext to Plaintext
Ciphertext: G ZGE WVG RNCP

CT	G	Z	G	E	W	V	G	R	N	C	P
PT	E		E				E				
PT	E		E			T	E				
PT	E		E			T	E			A	
PT	E		E			T	E		L	A	N
PT	E		E			T	E	P	L	A	N
PT	E	X	E	C	U	T	E	P	L	A	N

→ Advantages : Better Security than ceasar Cipher.

→ Disadvantages:
- Monoalphabetic cipher are easy to break because they reflect the frequency data of the original alphabet.
- Difficlt to guessing attack using the english letter frequency of occurance of letters.
- A co

* One time pad:

Improvement of the vernam Cipher

It yields the ultimate in security.

Random key is given that is as long as the message.

The key need not be repeated.

In addition, the key is to be used to encrypt and decrypt a single message and then is discarded.

Each new msg. requires a new key of same length as the new msg.

Such a scheme known as a One

time pad is unbreakable.

It produces random output.

No statistical relationship to the plain text.

Because the ciphertext contains no information whatever about the plaintext, there is simply no way to break the code.

The code is unbreakable. The security of the time pad is entirely due to the ~~rand~~ randomness of the key.

-> Two Fundamentals Difficulties:

The Practical problem of making large quantities of random keys.

Even more difficult to deal with the problem of key distribution and protection.

-> The Encryption Process:

One time pad keys are used in pairs.

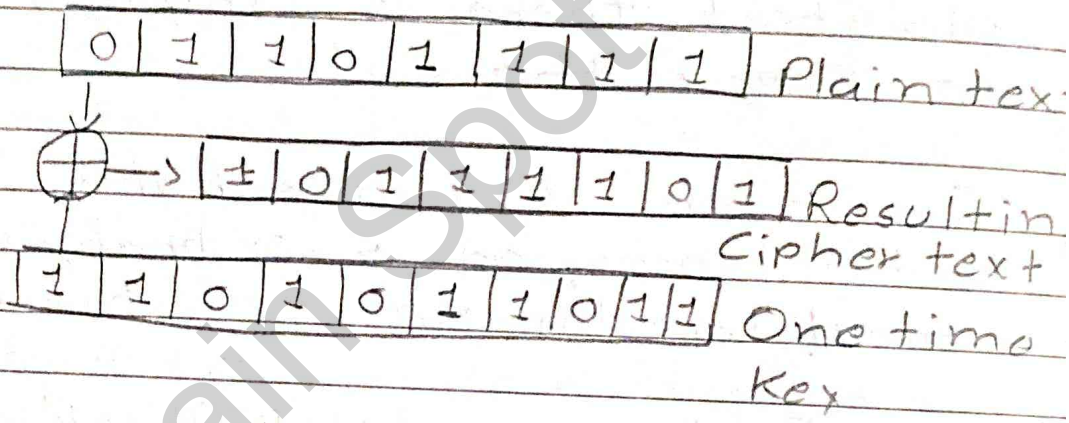
One copy of the key kept by each

Date : / /

user and the keys are distribute securely prior to encryption.

The confidentiality and authentia of the one time pad keys are assumed by continous protection during their distribution and stora

This quarentees that out sidess u not be able to misuse the key.



To encrypt plaintext data, the sender uses a key string equal in length to the plain text.

The key is used by mining (XOR) bit by bit, always a bit of the key with a bit of plaintext to create a bit of ciphertext.

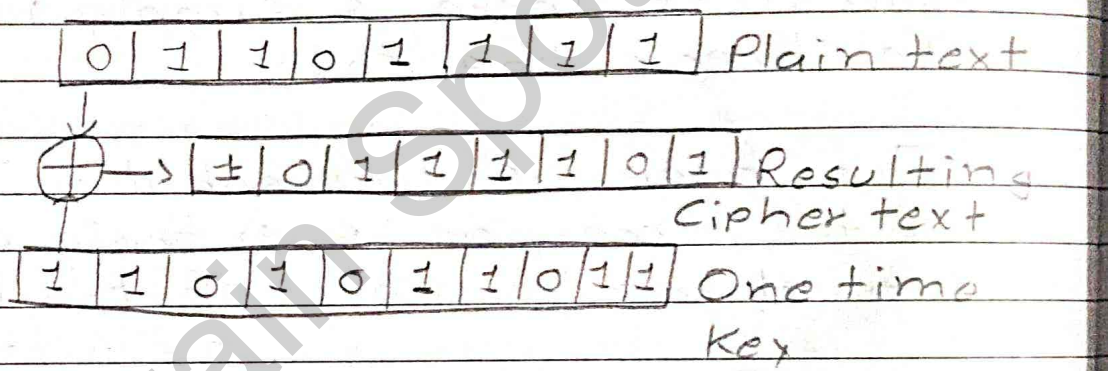
This cipher text is sent to the receiver.

At the receiver end, the encoded

user and the keys are distributed securely prior to encryption.

The confidentiality and authentialy of the one time pad keys are assumed by continous protection during their distribution and storage.

This quarentees that out sidess with not be able to misuse the key.



To encrypt plaintext data, the sender uses a key string equal in length to the plain text.

The key is used by mining (XOR) bit by bit, always a bit of the key with a bit of plaintext to create a bit of ciphertext.

This cipher text is sent to the receiver.

At the receiver end, the encoded

message is mixed with the duplicate copy of the one time key and the plaintext is restored.

Both senders and receivers keys are automatically destroyed after use to ensur re-applications of the same key is not possible.

Their message is represented as a binary string using a coding mechanism such as ASCII coding.

The key is tr a random sequence of 0's and 1's of the same length as the message.

Ex. Message = IF

then its I F

ASCIT = 1 0 0 1 0 0 1 1 0 0 0 1 1 0

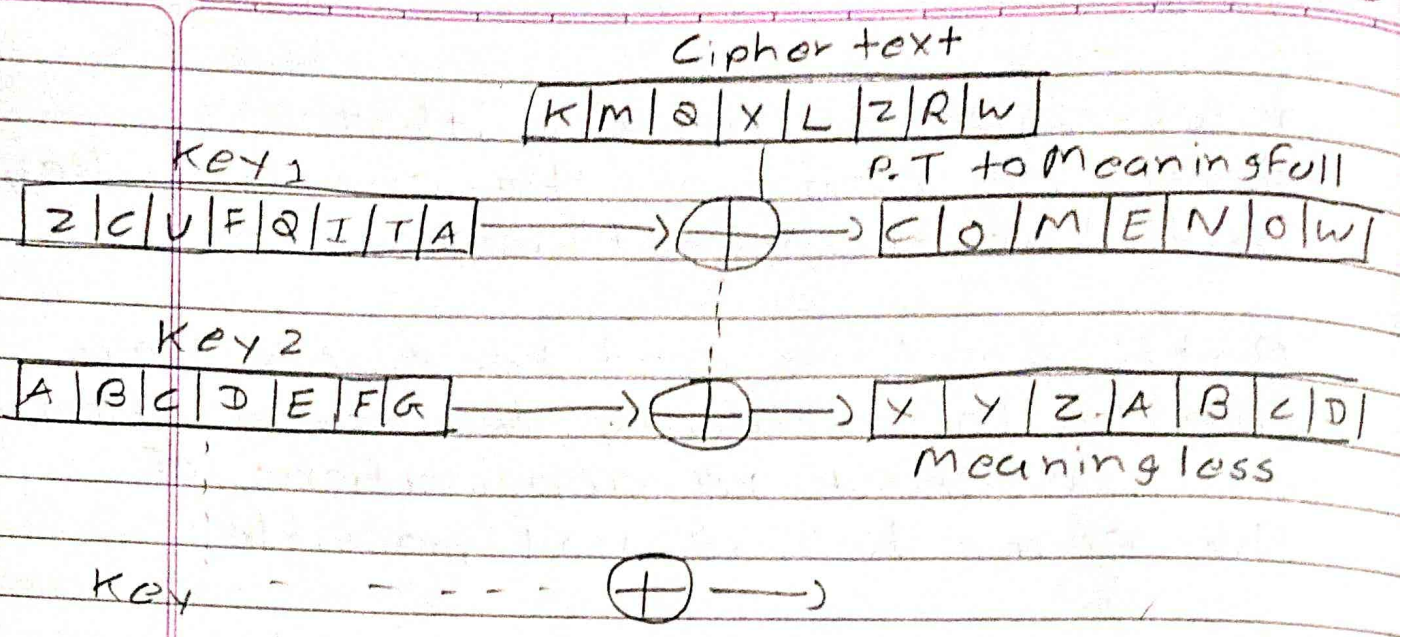
Key = 1 0 1 0 1 1 0 0 1 1 0 0 0 1

XOR

0 0 1 1 1 1 1 1 1 1 0 1 1 0

- Attack - Brute Force Attack.

Date : / /



Key - - - - ⊕ →

meaningless / meaningfull

* Transposition Method: A very different kind of mapping is achieved by performing some sort of permutation the plaintext letters.

Types → Rail Fence
→ Row Column Transposition

=> Rail Fence Method:

Ex. Plain text: Thank you very much
Depth / key : 3

T				K				V				m							
	H		N		y		U		e		y		U		H				
		A				O				r				C					

Ciphertext: TKVMHNYUEYUHAORC

⇒ Row Column Transposition : More Complex scheme.

- Recangle (works)
- key → Order of the ~~col~~ column
- ~~white~~ →
- Write → Row by Row
- Read → Column by Column
- Number of rows and no. of columns will be decided by sender and receiver.

Ex. Plain text = Kill Corona Virus at twelve am tomorrow.

Key = 4 3 1 2 5 6 7

4	3	1	2	5	6	7
K	I	L	L	C	O	R
O	N	A	V	I	R	U
S	a	T	T	W	E	L
V	E	A	M	T	O	M
O	R	R	O	W	Y	Z

Cipher text : LATARLUTMOINAERKOSVOCIWTWOREOYRULMZ

* Steganography:

It is an alternative to encrypt
In this we are not going to do encryption of the message rather, we are going to hides existance of message.

It is not encryption method may be other substitution or transposition technique.

It is not cryptography.

Cryptogroaphy renders the message elligible to outsiders by various transformations of the text.

Ex. Simply encrypt correct reading exactly twise, so, the msg which is hidden here is secret.

Only sender and receiver will understand the msg patterns.

=> Methods:
- Character Marking.
  - Invisible Ink
  - Pin
  - Typewriter Correction / color

(ii) Character Marking:

Selected letters of printed or typewritten text are over written in pencil.

The marks are Ordinarily not visible unless the paper hold at an angle to bright light.

Only sender and receiver knows the specific angle only the overwritten text will be shown in bright light.

(iii) Invisible Ink: A number of substances can be used for writting but leave no visible trace until heat or some chemical is applied to paper.

(iii) Pin puctures: Small pin puctures on selected letters ordinarily not visible unless the paper is hold in frount of light.

(iv) Typewritter Correction / ~~Color~~ ribbon:

There is a typed material and malty there is a some space b/w the lines.

Date : / /

That spaces are used b/w typed with black ribbon the result of typing with correction type.

=> Disadvantages:

(i) Lots of Overhead: It is happan on hiding the text because in encryption algorithm will be converting the plaintext.

(ii) One the system is discovered it becomes virtually worthless.