UNIT-1

Chapter 2 : Cryptography : Concepts and Techniques:

① Introduction

Cryptography :- Cryptography is the art and science of achieving security by encoding messages to make them non-readable.

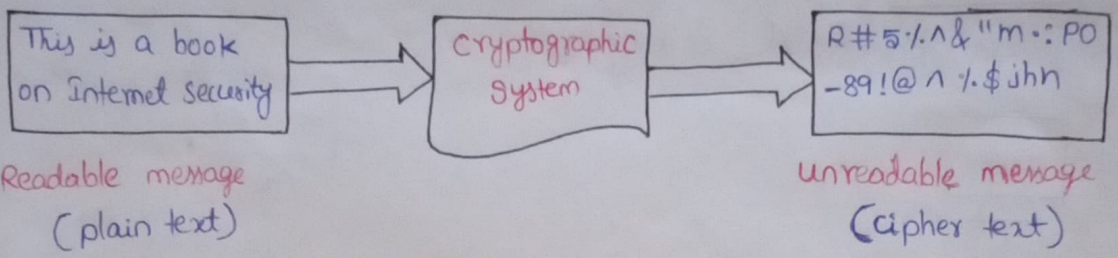


Fig:- Conceptual view of Cryptography

Cryptanalysis :- Cryptanalysis is the technique of decoding messages from a non-readable format to readable format

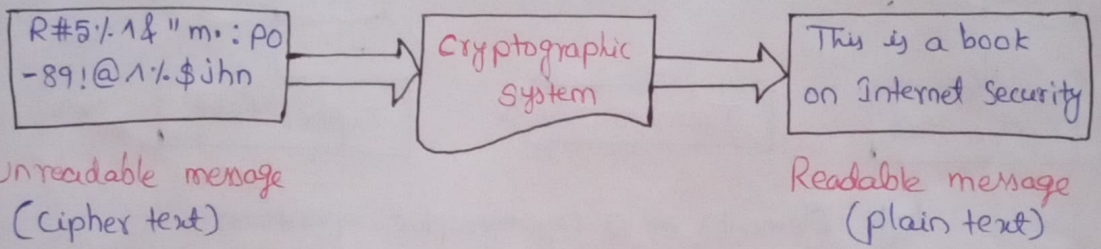
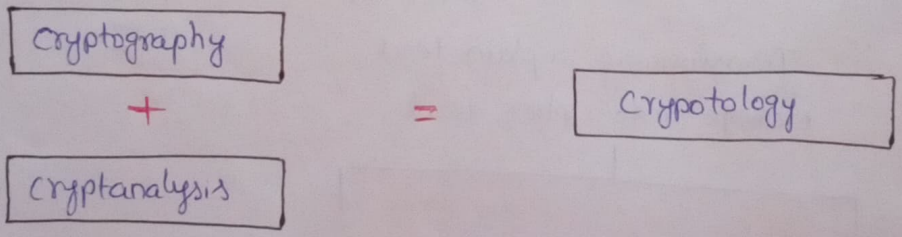


Fig:- cryptanalysis

Cryptology :- Cryptology is a combination of cryptography and cryptanalysis.



② plain Text and Cipher Text

* **plain Text** :- The original message. Any communication in the language that we speak - that is the human language.
Clear text or plain text signifies a message that can be understood by the sender and the receiver(s).

* **Cipher Text** :- When a plain text message is codified using any suitable scheme, the resulting message is called as cipher text.

→ Cipher :- An Algorithm for transforming plain text message into one that unintelligible by transposition and substitution methods.

→ Encipher (Encode) :- The process of converting plain text to cipher text using a cipher and a key.

→ Decipher (Decode) :- The process of converting cipher text to plain text using a cipher and a key.

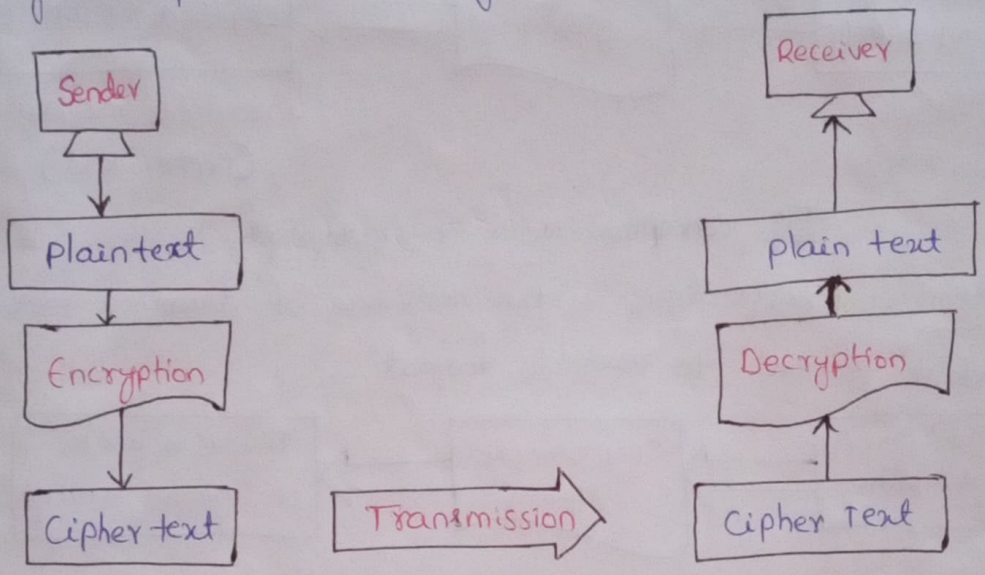


Fig:- Elements of a cryptographic operation.

* There are two primary ways in which plain text message can be codified to obtain the corresponding cipher text:

(i) Substitution (ii) Transposition

Transforming a plain text message into cipher text

Substitution Techniques | Transposition Techniques

Note that when the two approaches are used together, we call the technique as product cipher.

(3) Substitution Techniques

Substitution technique is a classical encryption technique where the characters present in the original message are replaced by the other characters or numbers or by symbols.

⇒ Types of substitution techniques are

i) Caesar Cipher
ii) Mono-alphabetic Cipher
iii) Homophonic Substitution Cipher
iv) polygram Substitution Cipher
v) polyalphabetic Substitution Cipher
vi) playfair Cipher
vii) Hill Cipher

i) Caesar cipher :- In this technique, the characters of a plain text message are replaced by other characters, numbers.

→ Caesar Cipher is a special case of substitution techniques wherein each alphabet in a message is replaced by an alphabet three places down the line

* The caesar cipher scheme is shown in figure. The first row shows the original alphabets and second row shows replaced alphabets.

Plain : 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 : 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

* Numerical equivalent to each letter given below.

Plain:	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:	0	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

Example :- plain text : Helloworld
cipher text : KHOORZRUOG
(or)
7411111422141717113

clearly, the caesar cipher is a very weak scheme of hiding plain text messages.

⇒ Modified Version of Caesar Cipher :- In this the cipher text alphabets corresponding to the original plain text alphabets may not necessarily be three places down the line, can be any places down the line.

It means each letter of a given text is replaced by a letter some fixed number of positions down the alphabet.

→ The algorithm can be expressed as follows. For each plaintext letter P, substitute the cipher letter C:

$$C = E(k, P) = (P + k) \bmod 26$$

where k takes on a value in the range 1 to 25.

The decryption algorithm is simply

$$P = D(k, C) = (C - k) \bmod 26$$

- Demerits:

1. The encryption and decryption algorithms are known.
2. There are only 25 keys to try.
3. The language of the plaintext is known and easily recognizable.
4. Brute-force attack

ii) Mono-alphabetic cipher:-

A mono-alphabetic cipher is a substitution cipher where each letter of the plain text is replaced with another letter of the alphabet.

→ In this we are using random substitution. This means that in a given plain text message, each A can be replaced by any other alphabet (B through Z), each B can also be replaced by any other random alphabet (A or C through Z).

→ To put it mathematically, we can now have any permutation or combination of the 26 alphabets. This is extremely hard to crack.

permutation or combination of the 26 alphabets, which means ($26 \times 25 \times 24 \times 23 \ldots$ ... 2) or 4×10^6 possibilities!

Frequency Analysis :- one approach used to help decrypt a monoaphabetic substitution cipher is to use a frequency analysis based on counting the number of occurrence of each letter to help identify the most recurrent letters. Some alphabets in the English language occur more frequently than others (e.g., In the English language letters E, T and A).

The cryptanalyst can try different attacks based on her knowledge of the English language.

∴ The process of trying to break any cipher text message to obtain the original plain text message itself is called as Cryptanalysis and the person attempting a cryptanalysis is called as a cryptanalyst.

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

* Example :- Hello how are you

cipher text : zcggh zhr mac why

(iii) Homophonic Substitution Cipher :- Homophonic substitution cipher also involves substitution of one plain text character with a cipher text character at a time, however the cipher text character can be any one of the chosen set.

→ The Homophonic substition cipher is very similar to Mono-alphabetic cipher. We replace one alphabet with another in this scheme.

→ In Homophonic substitution cipher, one plain text alphabet can map to more than one cipher text alphabet.

→ For instance, A can be replaced by D, H, P, R
B can be replaced by E, I, Q, S

(iv) polygram Substitution Cipher :- polygram substitution cipher technique replaces one block of plain text with a block of cipher text - it does not work a character-by-character basis.

* Example :-

HELLO → polygram substitution → YUQQW

HELL → polygram substitution → TEUI

(v) polyalphabetic Substitution Cipher :- In this substitution, each occurrence of a character can have a different substitute.

→ The vigenere cipher is example of polyalphabetic substitution cipher

→ This cipher uses multiple - one character keys. Each of the keys encrypts one plain text character.

→ The below table shows the vigenere tableau.

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

Method 2 :- When the vigenere table is not given, the encryption and decryption are done by using formula.

* Formula of encryption is $C_i = (P_i + k_i) \bmod 26$

* Formula of decryption is $P_i = (C_i - k_i) \bmod 26$

Example: Let the message is THE BOY HAS THE BAG and key is VIG

key = VIG VIG VIG VIG VIG
plain text = THE BOY HAS THE BAG
Cipher text = OPK WNE CIY OPK WIH

(vi) play fair cipher :- The play fair cipher is also called as playfair square, is a cryptographic technique that is used for manual encryption of data.

→ The playfair encryption scheme uses two main processes:

step 1 :- Creation and population of matrix
step 2 :- Encryption Process

Step 1 : Creation and population of matrix : The playfair cipher make use of 5 x 5 matrix, which is used to store a keyword.

⇒ Matrix is created based on some simple rules:

1. Enter the keyword in the matrix row-wise : left-to-right, and then top-to-bottom.
2. Drop duplicate letters.
3. Fill the remaining spaces in the matrix with the rest of the English alphabets (A-Z) that were not a part of our keyword. While doing so, combine I and J in the same cell of the table.

Step 2 :- Encryption process : The encryption process consists of five steps:

1. The plaintext message that we want to encrypt needs to be broken down into groups of two alphabets.
2. If both alphabets are the same (or only one is left), add an X after the first alphabet. Encrypt the new pair and continue.
3. If both the alphabets in the pair appear in the same row of our matrix, replace them with alphabets to their immediate right respectively. If the original pair is on the right side of the row, then wrapping around to the left side of the row.
4. If both the alphabets in the pair appear in the same column of our matrix, replace them with alphabets immediately below them respectively.

If the original pair is on the bottom side of the row, then wrapping around to the top side of the row happens.

5. If the alphabets are not in the same row or column, replace them with the alphabets in the same row respectively but at the other pair of corners of the rectangle defined by the original pair.

Example :- original text : attack
Keyword : MONARCHY

Step 1: Creation of matrix

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

Step 2 :- Encryption process

Original text : attack

at	ta	ck
RS	SR	DE

→ The first pair of alphabets is AT. The alphabets A & T do not occur in the same row or column.

In this case, the text RS is our first cipher text block.

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

→ our next text block to be encrypted is TA.

our second block of cipher text SR.

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

→ now take the third block of plain text, which is CK.

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

The cipher text block is DE

Thus outplain text blocks attack becomes RS SR DE.

(vii) Hill cipher :- Hill cipher is works on multiple letters at the same time. It is a polygraphic substitution cipher based on linear algebra. Each letter is represented by a number modulo 26. It means A=0, B=1, C=2, ..., Z=25.

→ To encrypt a message, each block of n letters is multiplied by an invertible n x n matrix, against modulus 26.

→ To decrypt the message, each block is multiplied by the inverse of the matrix used for encryption.

- Example:- plaintext : ACT
  Key : GYBNQKURP

Encryption:- We have to encrypt the message ACT (n=3). The key is GYB NQKURP which can be written as the n x n matrix:

$$\begin{bmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{bmatrix}$$

The plain text ACT is written as:

$$\begin{bmatrix} 0 \\ 2 \\ 19 \end{bmatrix}$$

The encrypted vector is given as:

$$\begin{bmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{bmatrix} \times \begin{bmatrix} 0 \\ 2 \\ 19 \end{bmatrix} = \begin{bmatrix} 67 \\ 222 \\ 319 \end{bmatrix}$$

Now compute a mod 26 of the above matrix

$$\begin{bmatrix} 67 \\ 222 \\ 319 \end{bmatrix} \bmod 26 = \begin{bmatrix} 15 \\ 14 \\ 7 \end{bmatrix}$$

Now, translating the numbers to alphabets, 15 = P, 14 = O, and 7 = H.

Therefore, our cipher text is 'POH'

Decryption :- To decrypt the message, the cipher text matrix multiply by the inverse matrix of the key matrix.

$$\begin{bmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{bmatrix}^{-1} \equiv \begin{bmatrix} 8 & 5 & 10 \\ 21 & 8 & 21 \\ 21 & 12 & 8 \end{bmatrix}$$

$$\begin{bmatrix} 8 & 5 & 10 \\ 21 & 8 & 21 \\ 21 & 12 & 8 \end{bmatrix} \times \begin{bmatrix} 15 \\ 14 \\ 7 \end{bmatrix} = \begin{bmatrix} 260 \\ 574 \\ 539 \end{bmatrix} \bmod 26 = \begin{bmatrix} 0 \\ 2 \\ 19 \end{bmatrix}$$

0 = A, 2 = C, and 19 = T, This gives is the original plain text ACT

* Vernam cipher (One-Time pad) :- The vernam cipher also called as one-Time pad. It is implemented using a random set of non-repeating characters as the input cipher text.

→ The most significant point here is that once an input cipher text for Substitution is used, it is never used again for any other message.

→ The length of the input key is equal to the length of the original plain text.

- The algorithm used in Vernam Cipher is:

1. Treate each plain text alphabet as a number in an increasing sequence, i.e., A=0, B=1, ---, Z=25.
2. Do the same for each character of the input cipher text (key).
3. Add each number corresponding to the plain text alphabet to the corresponding input cipher text alphabet number.
4. If the sum thus produced is greater than 26, subtract 26 from it.
5. Translate each number of the sum back to the corresponding alphabet. This gives the output cipher text.

Example :- plain text message : How ARE YOU

one-time pad (key): NCBTZQARX

1. plain text	H	O	W	A	R	E	Y	O	U
	7	14	22	0	17	4	24	14	20
	+								
2. one-Time pad	13	2	1	19	25	16	0	17	23
	N	C	B	T	Z	Q	A	R	X
3. Initial Total	20	16	23	19	42	20	24	31	43
4. Subtract 26, if >25	20	16	23	19	16	20	24	5	17
5. Cipher text	U	Q	X	T	Q	U	Y	F	R

Cipher text message : UQXTQUYFR

Vernam cipher uses a one-time pad, which is discarded after a single use.

(4) Transposition Techniques

Transposition techniques is a cryptographic algorithm where the order of alphabets in the plaintext is rearranged to form a cipher text.

→ Transposition technique also perform some permutation over the plain text alphabets.

There are two types of transposition techniques:

(i) Rail Fence Technique

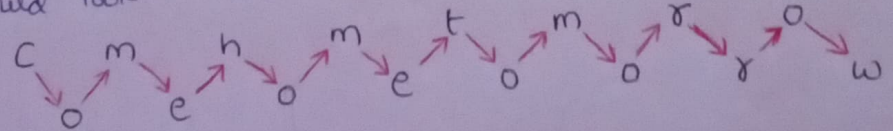
(ii) Simple Columnar Transposition Technique

(i) Rail Fence Technique :- The rail fence cipher also called a zigzag cipher. It is a classical type of transposition cipher.

Encryption :- 1. Write down the plain text message as a sequence of diagonals.
2. Read the plain text written in step 1 as a sequence of rows.

Example :- Come home tomorrow

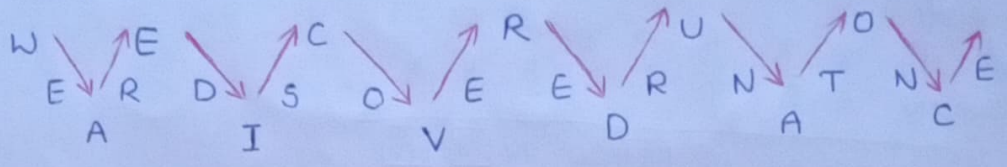
1. After we arrange the plain text message as a sequence of diagonals, it would look as follows.



2 Now read the text row-by-row, and write it sequentially. Thus, we have

Cmhmtmrooeoorw as the cipher text.

Example 2 :- To encrypt the message 'WE ARE DISCOVERED. RUN AT ONCE' with 3 rails, write the text as:



Cipher text : WECRUO ERDSOEERNTNE AIVDAC

Rail fence technique involves writing plain text as sequence of diagonals and then reading it row-by-row to produce cipher text.

(ii) Simple columnar Transposition Technique :- The Simple columnar Transposition technique simply arranges the plain text as a sequence of rows of a rectangle that are read in columns randomly.

Encryption :- 1. Write the plaintext message row-by-row in a rectangle of a pre-defined size

2. Read the message column-by-column. It need not be in the order of Columns 1, 2, 3 etc, It can be any random order such as 2, 3, 1, etc,

3. The message thus obtained is the cipher text message.

Example :- original plain text message: Come home tomorrow

1. Let us consider a rectangle with six columns. Write the message in the rectangle row-by-row.

Column 1	Column 2	Column 3	Column 4	Column 5	Column 6
c	o	m	e	h	o
m	e	t	o	m	o
r	r	o	w		

2. Now, let us decide the order of column as some random order 4, 6, 1, 2, 5 and 3.

3. The cipher text would be : eowoocmroerhmmto

To make matters complex for a cryptanalyst, we can modify the simple Columnar Transposition technique to add another twist: perform more than one round of transposition using the same technique.

* Simple Columnar Transposition Technique with Multiple Rounds: The idea is to use the same basic procedure as used by the simple columnar Transposition Technique, but do it more than once.

Cipher text produced by the simple columnar Transposition Technique with multiple rounds is much more complex to crack as compared to the basic technique.

Example:- original plain text messg: Come home tomorrow

1)

Column 1	Column 2	Column 3	Column 4	Column 5	Column 6
C	o	m	e	h	o
m	e	t	o	m	o
r	r	o	w		

2) Now, let us decide the order of columns as some random order 4, 6, 1, 2, 5, 3.

3) The ciphertext message is: eowoocmroethmmto

4) Let us perform 1 through 3 once more.

Column 1	Column 2	Column 3	Column 4	Column 5	Column 6
e	o	w	o	o	c
m	r	o	e	r	h
m	m	t	o		

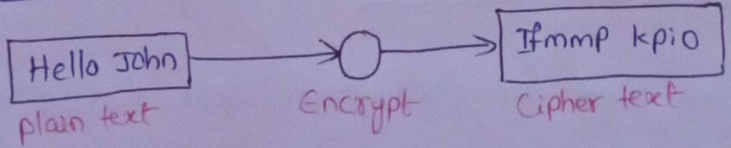
Now let us use the same order of columns, as before, that is 4, 6, 1, 2, 5, 3.

The cipher text is: oeochemmormorwot

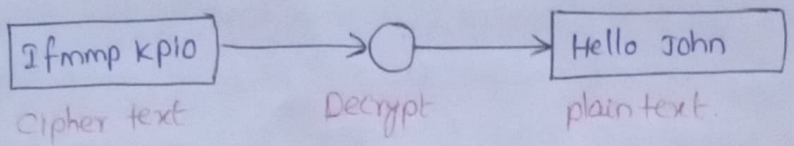
→ continue like this if more number of iterations is desired, otherwise stop.

⑤ Encryption and Decryption

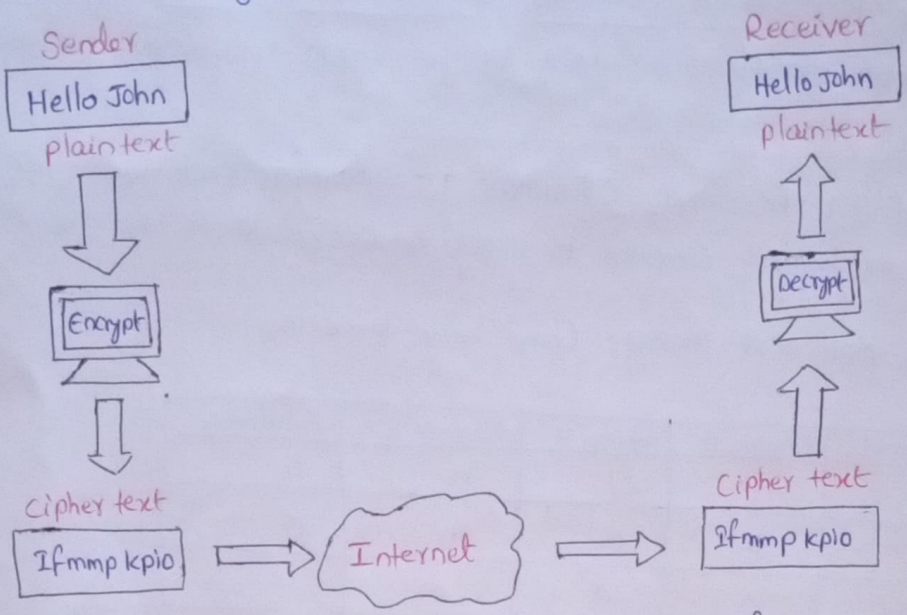
The process of encoding plain text message into cipher text message is called as encryption.



The reverse process of transforming cipher text message back to plain text message is called as decryption.



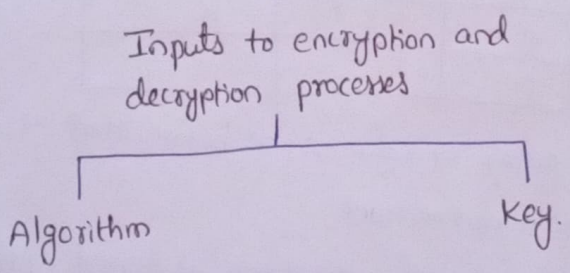
Encryption and Decryption in the real world.



→ To encrypt a plain text message, the sender perform encryption, i.e., applies the encryption algorithm. To decrypt a received encrypted message, the receiver perform decryption, i.e., applies the decryption algorithm.

→ Clearly, the decryption algorithm must be same as the encryption algorithm.

→ The second aspect of performing encryption & decryption of message is the key.



In general, the algorithm used for encryption and decryption processes is usually known to everybody. However, the key used for encryption & decryption that makes the process of cryptography secure.

⇒ There are two cryptographic mechanisms, depending on what keys are used.

(i) If the same key is used for encryption and decryption, we call the mechanism as Symmetric key Cryptography.

(ii) If two different keys are used ~~for~~ in a cryptographic mechanism, wherein one key is used for encryption and another (different) key used for decryption; we call the ~~mechanism~~ mechanism as Asymmetric key Cryptography.

Cryptography techniques

Symmetric key cryptography Asymmetric key cryptography

(6) Symmetric and Asymmetric Key Cryptography

* Symmetric key cryptography and the problem of key Distribution

Symmetric key cryptography involves the usage of the same key for encryption and decryption.

→ For symmetric encryption to work, the two parties ~~an~~ to an exchange must share the same key, and that key must be protected from access by others.

→ Distribution of secret key has been problematic, because it involved face-to-face meeting, use of a trusted courier, or sending the key through an existing encryption channel.

~~→~~ In ~~public key~~ ~~cry~~

→ If A wants to communicate with two persons, B and C securely. 'A' must use a different lock-and-key pair for B and C.

parties involved	No. of lock-and-key pairs required
2 (A, B)	1 (A-B)
3 (A, B, C)	3 (A-B, A-C, B-C)
4 (A, B, C, D)	6 (A-B, A-C, A-D, B-C, B-D, C-D)

In general for 'n' persons, the no. of lock-and-key pairs is $n * (n-1)/2$.

→ We must keep in mind that a record of which lock-and-key pair was issued to which communicating pair must be maintained by somebody.

Let us call this somebody as T. T must be highly trustworthy and accessible to everybody. Each communicating pair has to approach T to obtain the lock-and-key pair. This is quite a tedious & time consuming process.

* **Diffie-Hellman Key Exchange / Agreement Algorithm** :- It is a method of securely exchanging cryptographic keys over a public channel.

→ It is a solution to the problem of key agreement or key exchange.

- **Description of the Algorithm** :- Let us Assume that Alice & Bob want to agree upon a key to be used for encryption / decryption of messages that would be exchanged b/w them. Then, the Diffie-Hellman key exchange algorithm works as shown in fig:

1. Firstly, Alice & Bob agree on two large prime numbers, n and g. These two prime numbers (integers) need not be kept secret. Alice & Bob can use an insecure channel to agree on them.
2. Alice chooses another large random number x, and calculates A such that: $A = g^x \bmod n$
3. Alice sends the number A to Bob.
4. Bob independently chooses another large random integer y and calculates B such that: $B = g^y \bmod n$
5. Bob sends the number B to Alice
6. A now computes the secret key K1 as follows:

$$K1 = B^x \bmod n$$

7. B now computes the secret key K2 as follows:

$$K2 = A^y \bmod n$$

- **Example of the Algorithm** :-

1. Alice & Bob agree on two large prime numbers, n and g.

Let $n=11$, $g=7$

2. Alice chooses another large random number x. & Calculates A

Let $x=3$.

Then, $A = 7^3 \bmod 11 \Rightarrow 343 \bmod 11$

$\Rightarrow 2$

3. Alice sends the number A to Bob

Alice sends 2 to Bob

4. Bob chooses another large random integer y and calculates B

Let $y = 6$

Then, $B = 7^6 \bmod 11 \Rightarrow 117649 \bmod 11$

$\Rightarrow 4$

5. Bob sends the number B to Alice.

Bob sends 4 to Alice

6. A now computes the secret key K1 as follows:

$K1 = B^x \bmod n$

$K1 = 4^3 \bmod 11 \Rightarrow 64 \bmod 11$

$\Rightarrow 9$

7. B now computes the secret key K2 as follows:

$K2 = A^y \bmod n$

$K_2 = 2^6 \bmod 11 \Rightarrow 64 \bmod 11$

$\Rightarrow 9$

- Problem with the Algorithm :- Diffie-Hellman key exchange algorithm has a problem that is man-in-the-middle attack, also called as bucket brigade attack.

The way this happens is as follows:-

1. Alice wants to communicate with Bob securely. For this purpose, she sends the values of n and g to Bob.

Let $n = 11$, $g = 7$

2. Alice does not ~~realize~~ realize that the attacker Tom is listening quietly to the conversation b/w Alice & Bob.

Tom simply picks up the values of n & g and also forwards them to Bob.

Alice	Tom	Bob
$n=11, g=7$	$n=11, g=7$	$n=11, g=7$

3. Alice, Tom, & Bob select random numbers x and y as shown in fig:

Alice	Tom	Bob
$x=3$	$x=8, y=6$	$y=9$

4. Now, Based on these values, all the three persons calculate the values of A and B as show in fig:

Alice & Bob calculates A & B respectively. Tom calculates both A & B.

Alice

$A = g^x \bmod n$
$= 7^3 \bmod 11$
$= 343 \bmod 11$
$= 2$

Tom

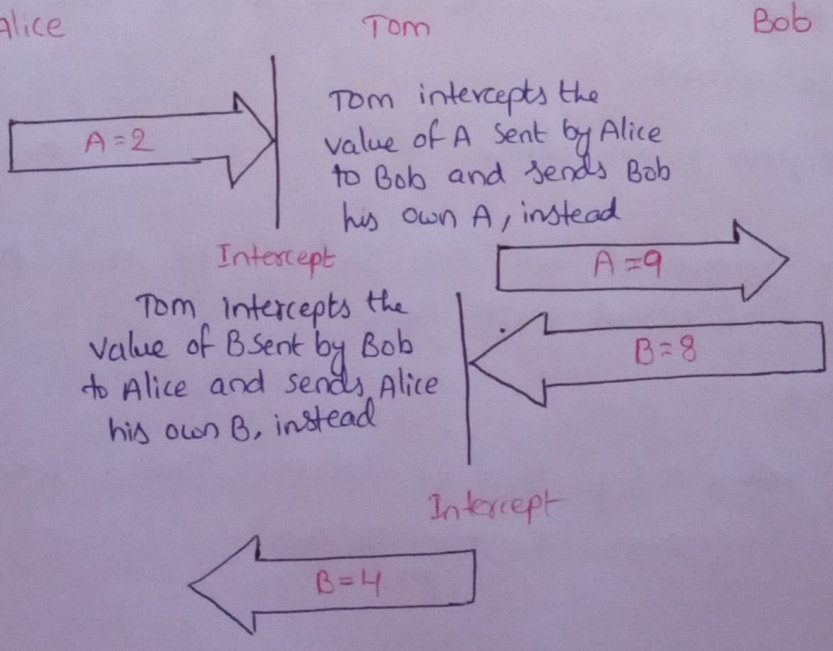
$A = g^x \bmod n$
$= 7^8 \bmod 11$
$= 5764801 \bmod 11$
$= 9$

$B = g^y \bmod n$
$= 7^6 \bmod 11$
$= 117649 \bmod 11$
$= 4$

Bob

$B = g^y \bmod n$
$= 7^9 \bmod 11$
$= 40353607 \bmod 11$
$= 8$

5. Now, the real problem begins, as shown in fig:



Alice, Tom & Bob have the values of A & B as shown in fig:

Alice	Tom	Bob
A=2, B=4*	A=2, B=8	A=9*, B=8

(Note: * indicates the these are the values after Tom hijacked & changed them)

6. Based on these values, all the three persons now calculate their keys as shown in fig:

Alice

$K1 = B^x \bmod n$
$= 4^3 \bmod 11$
$= 64 \bmod 11$
$= 9$

Tom

$K1 = B^x \bmod n$
$= 8^8 \bmod 11$
$= 16777216 \bmod 11$
$= 5$

$K2 = A^y \bmod n$
$= 2^6 \bmod 11$
$= 64 \bmod 11$
$= 9$

Bob

$K2 = A^y \bmod n$
$= 9^9 \bmod 11$
$= 387420489 \bmod 11$
$= 5$

Tom has two keys: This is because at one side, Tom wants to communicate with Alice securely using a shared symmetric key (9) and on the other hand, he wants to communicate with Bob securely using a different shared symmetric key (5).

→ only then can he receive message from Alice, view/ manipulate them and forward them to Bob and vice versa.

* Asymmetric key operation

Asymmetric key cryptography involves the usage of one key for encryption and another, different key for decryption.

In this scheme, A and B do not jointly approach for a lock-and-key pair.

→ B alone approaches to obtain a lock and key (K1) that can seal the lock and sends the lock and key K1 to A.

→ B possesses a different but related key (K2), which is obtained by B along with the lock and key K1, only which can open the lock.

→ one key (K1) is used for locking and another different key (K2) is used for unlocking; we will call this scheme as asymmetric key operation.

→ Both A & B approaches T for a lock-and-key pair. T is clearly defined as a "trusted third party".

→ This means that B posseses a key pair (i.e, two keys K1 and K2). one key (K1) can be used for locking and the corresponding other key (K2) from the key pair can be used for unlocking.

→ B can send the lock and key K1 to anybody (eg. A) who wants to send anything securely to B. B would request the sender (e.g. A) to use that lock and key K1 to seal the contents. B can open the seal using the key K2.

→ Since the key K1 is meant for locking and is available to the general public, we shall call K1 as public key.

→ The other key K2 is meant for unlocking and is strictly held secret/ private by A. Therefore, we shall call it as private key (or) secret key.

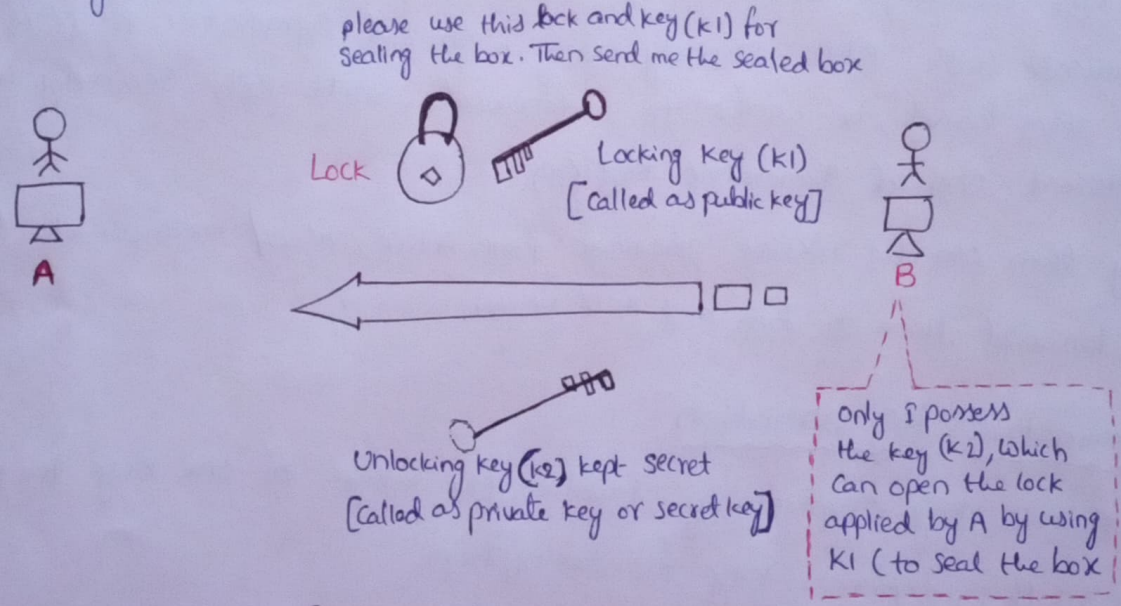


Fig:- Use of key pair

⑦ Steganography

Steganography is a technique that facilitates hiding of a message that is to be kept secret inside other messages. This results in the concealment of the secret message itself.

Historically, the sender used methods such as invisible ink, tiny pin punctures on specific characters, minute variation b/w handwritten characters, pencil marks on handwritten characters, etc.

→ Now, people hide secret messages within graphic images. For instance, suppose that we have a secret message to send. We can take another image file, and we can replace the last two rightmost bits of each byte of that image with (the next) two bits of our secret message.

→ The resulting image would not look too different & yet carry a secret message inside.

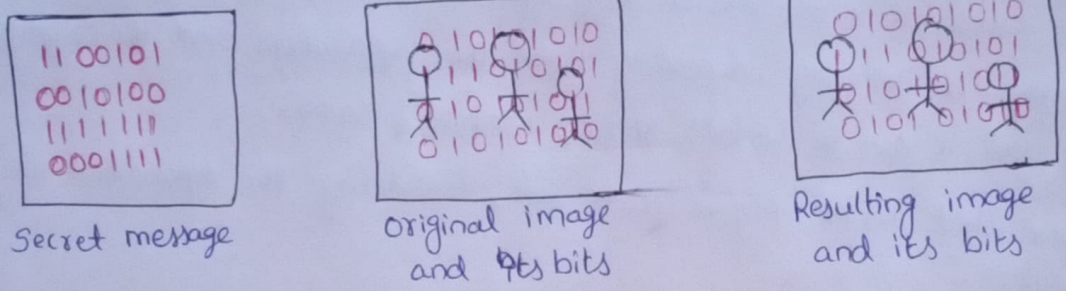


Fig:- Steganography example

(8) Key Range and key size

The concept of key range and key-size are related to each other. Key Range is total no. 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 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 expanding the key range to a large extent, longer it will take 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 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 8 bits then the key range 0 to 256. From a practical viewpoint, a 40-bit key takes about 3 hours to crack. However, a 41-bit key would take 6 hours, a 42-bit key takes 12 hours and so on.

→ This means that every additional bit doubles the amount of time required to crack the key.

→ with every incremental bit, the attacker has to perform double the no of operations as compared to the previous key size.

→ 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.

→ we can assume that 128 bit key is quite safe, considering the capabilities of todays computers.

(9) possible Types of attacks

When the sender of a message encrypts a plain text message into its corresponding cipher text, there are five possibilities for an attacker on this message.

(i) cipher text only attack
(ii) known plain text attack
(iii) chosen plain text attack
(iv) chosen cipher text attack
(v) chosen text attack.

(i) Cipher text only attack :- In this type of attack, the attacker does not have any clue about the plain text. Attacker has some or all of the cipher text.

→ The attacker analyzes the cipher text at leisure to try and figure out the original plain text.

→ Based on the frequency of letters the attacker makes an attempt to guess the plain text. Obviously, the more cipher text available to the attacker, more are the chances of a successful attack.

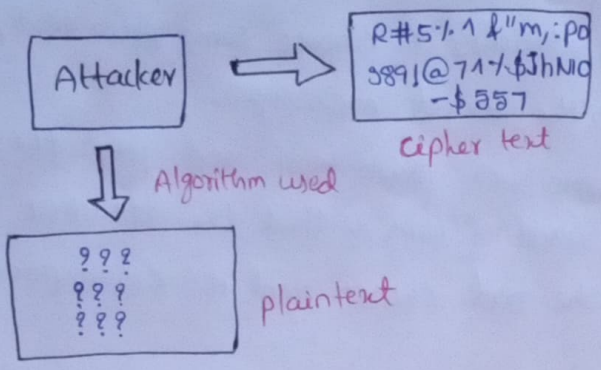


Fig:- cipher text only attack

(ii) Known plain text attack:- In this case, the attacker knows about some pairs of plain text and corresponding cipher text for those pairs. Using this information, the attacker tries to find other pairs and therefore, know more and more of the plain text.

Example:- Example of such known plaintexts are Company banners, file headers etc. which are found commonly in all documents of a particular company.

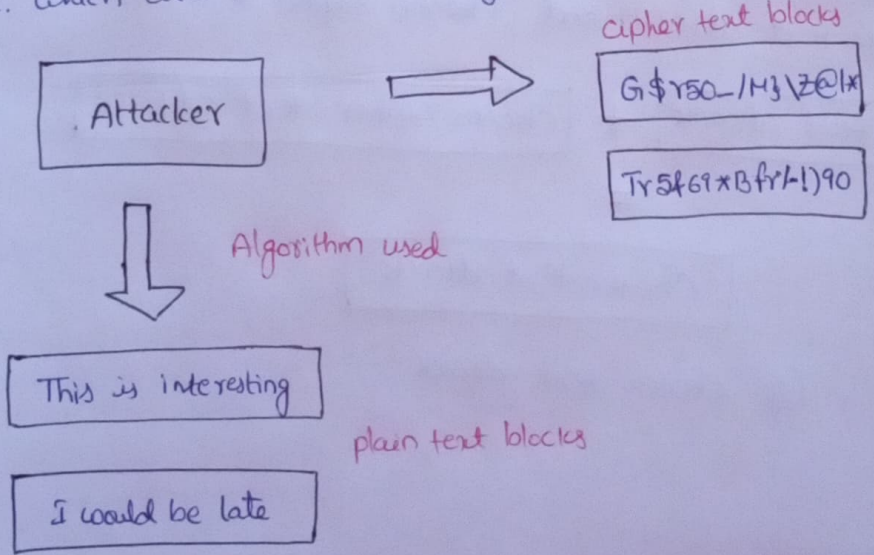


Fig:- known plain text attack

(iii) Chosen plain text attack:- Here, the attacker selects a plain text block and tries to look for the encryption of the same in the cipher text.

→ Here, the attacker is able to choose the messages to encrypt. Based on this, the attacker intentionally picks patterns of cipher text that result in obtaining more information about the key.

For example:- a telegraph company may offer a paid service where they encrypt people's messages and send them to the desired recipient. The telegraph company on the other side would decrypt the message and give the original message to the recipient.

→ Therefore, it is quite possible for the attacker to choose some plain text, which she thinks is quite commonly used in the secret messages.

→ Therefore, the attacker chooses some such plain text and pays the telegraph company to encrypt it. The result of this is that the attacker now has access to some plain text that she had chosen and its corresponding cipher text.

(iv) chosen cipher text attack :- In the case, the attacker knows the cipher text to be decrypted, the encryption algorithm that was used to produce this cipher text and the corresponding plain text block.

→ The attacker's job is to discover the key used for encryption. However, this type of attack is not very commonly used.

(v) chosen text attack :- The chosen text attack is essentially a combination of chosen plain text attack and chosen cipher text attack.

chosen plain text attack + chosen cipher text attack

=

chosen text attack

Fig:- chosen text attack