Cryptography

When people initially tried to communicate over distances, they tried to ensure the secrecy of their communications. **Cryptography** is a technique for securing the secrecy of communication .

Cryptography is a well-known method for securing the secrecy of communication in which the secret message is transformed to another form such that it does not make any sense to the intruder. The word Cryptography was evolved from two Greek words – Crypto (hidden, secret), and Graphein (writing). **Cryptography** is a techniques used for deciphering a message without any knowledge of the enciphering details fall into the area of **cryptanalysis**. Cryptanalysis is what the layperson calls "breaking the code." The areas of cryptography and cryptanalysis together are called **cryptology**.

Symmetric Cipher Model

A symmetric encryption scheme has five ingredients :

- **Plaintext(P):** This is the original intelligible message or data that is fed into the algorithm as input.
- **Encryption algorithm (E):** The encryption algorithm performs various substitutions and transformations on the plaintext.
- **Secret key(K) :** The secret key is also input to the encryption algorithm. The key is a value independent of the plaintext and of the algorithm. The algorithm will produce a different output depending on the specific key being used at the time. The exact substitutions and transformations performed by the algorithm depend on the key.

- **Ciphertext (C) :** This is the scrambled message produced as output. It depends on the plaintext and the secret key. For a given message, two different keys will produce two different ciphertexts.The ciphertext is an apparently random stream of data and, as it stands, is unintelligible.
- **Decryption algorithm (D) :** This is essentially the encryption algorithm run in reverse. It takes the ciphertext and the secret key and produces the original plaintext.

The security of the cryptosystem often depends on keeping the key secret to some set of parties.

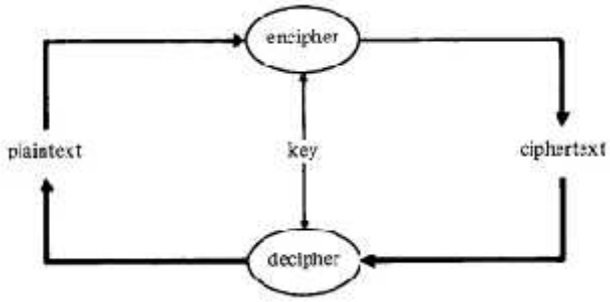


Figure (1) Secret writing (cryptography)

There are two requirements for secure use of conventional encryption:

a- A strong encryption algorithm.

b- Sender and receiver must have same secret key.

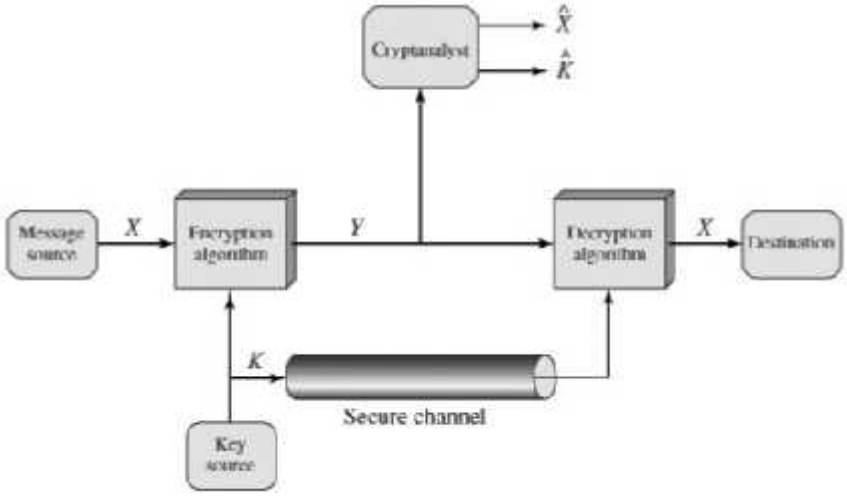


Figure (2) Model of Conventional Cryptosystem

If $X = [X1, X2, ..., XM]$ is a source produces a message in plaintext, and $K = [K1, K2, \ldots KJ]$ is the encryption key.

The encryption algorithm forms the ciphertext $Y = [Y1, Y2, ..., YN]$. We can write this as

$$Y = E(K, X)$$

The intended receiver, in possession of the key, is able to invert the transformation:

$$X = D(K, Y)$$

Cryptography systems are characterized along three independent dimensions :

1- The type of operations used for transforming plain text to cipher text:

a-Transposition algorithm: in which elements of the plain text are rearranged. The key is permutation of symbols , figure 3 explains the Transposition algorithm.

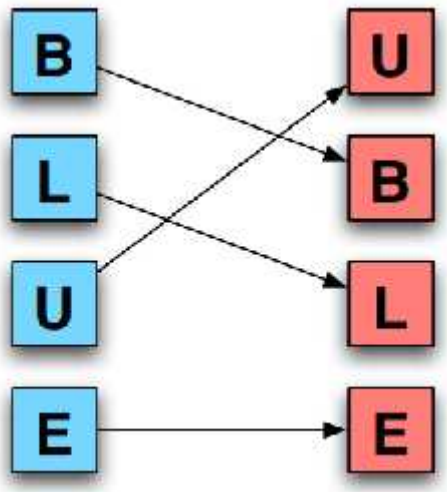


Figure (3)

b-Substitution algorithm: in which each element in the plain text (bit, letter, and group of bits or letters) is mapped into other element. The key is the permutation. Figure (4) explains the Substitution algorithm.

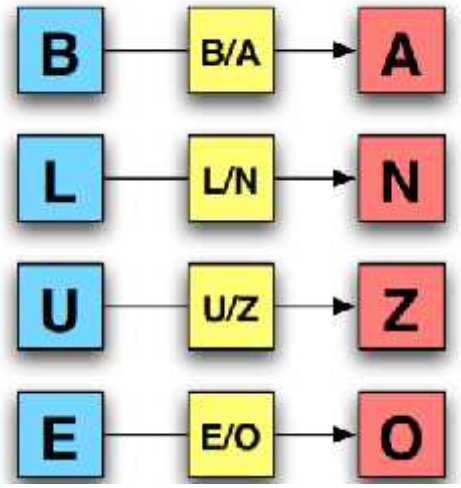


Figure (4)

c-Product system: in which multiple stages of substitution and transposition operations are done.

2- The number of key used:

a-Symmetric encryption: if both sender and receiver used the same key,the system is referred to as symmetric ,single-key, secret-key, or conventional encryption.

b-Asymmetric encryption : if the sender and receiver used different keys, the system is referred to as asymmetric, two-key, or public- key encryption.

3- the way in which the plain text is processed :

a-Block cipher : that process the input one block of elements at a time ,producing an output block for each input block.

b- Stream cipher: that process the input elements continuously, producing output elements at a time as it goes along.

Cryptanalysis

Is the science and study of methods of breaking ciphers. The whole point of cryptography is to keep the plaintext or the key or both secret from the eavesdroppers. There are two general approaches to attacking a conventional encryption scheme:

A- **Cryptanalysis:** Cryptanalytic attacks rely on the nature of the algorithm plus perhaps some knowledge of the general characteristics of the plaintext or even some sample plaintext - ciphertext pairs. This type of attack exploits the characteristics of the algorithm to attempt to deduce a specific plaintext or to deduce the key being used.

There are several types of **cryptanalytic attacks**, based on the amount of information known to the cryptanalyst.

1- **Ciphertext-only attack**, the cryptanalyst has the ciphertext of several messages, all of which have been encrypted using the same encryption algorithm.
2- **a known-plaintext attack**, a cryptanalyst has not only the ciphertext of several message, but also have the plaintext of those message
3- **chosen-plaintext attack**, it is same as know-plain text attack, but here the cryptanalyst choose the plain text that gets encrypted.
4- **Chosen-ciphertext attack**: the cryptanalyst can choose different ciphertexts to be decrypted and has access to the decrypted plain text .
5- **Chosen-key attack** : this attack does not mean that the cryptanalyst can choose the key ,but it mean that the cruptanalyst

has some knowledge about the characteristics of the key ,or the relationship between different keys.

Types of Attacks on Encrypted Messages

Type of Attack	**Known to Cryptanalyst**
1- Ciphertext only	● Encryption algorithm ● Ciphertext
2- Known plaintext	● Encryption algorithm ● Ciphertext ● One or more plaintext-ciphertext pairs formed with the secret key.
3- Chosen plaintext	● Encryption algorithm ● Ciphertext ● Plaintext message chosen by cryptanalyst, together with its corresponding ciphertext generated with the secret key.
4- Chosen ciphertext	● Encryption algorithm ● Ciphertext ● Purported ciphertext chosen by cryptanalyst, together with its corresponding decrypted plaintext generated with the secret key.
5- Chosen text	● Encryption algorithm ● Ciphertext ● Plaintext message chosen by cryptanalyst, together with its corresponding ciphertext generated with the secret key.

- Purported ciphertext chosen by cryptanalyst, together with its corresponding decrypted plaintext generated with the secret key.

B- brute-force attack involves trying every possible key until an intelligible translation of the ciphertext into plaintext is obtained. On average, half of all possible keys must be tried to achieve success.

Table 1. Average Time Required for Exhaustive Key Search

Key size (bits)	Number of alternative keys		Time required at 1 decryption/*ms*		Time required at 10^6 decryption/*ms*
32	2^{32}	= 4.3 x 10^9	2^{31} *ms*	= 35.8 minutes	2.15 milliseconds
56	2^{56}	= 7.2 x 10^{16}	2^{55} *ms*	= 1142 years	10.01 hours
128	2^{128}	= 3.4 x 10^{38}	2^{127} *ms*	= 5.4 x 10^{24} years	5.4 x 10^{18} years
168	2^{168}	= 3.7 x 10^{50}	2^{167} *ms*	= 5.9 x 10^{36} years	5.9 x 10^{30} years
26 characters (permutation)	26!	= 4 x 10^{26}	2 x 10^{26} *ms*	= 6.4 x 10^{12} years	6.4 x 10^6 years

Substitution Techniques

A substitution technique is one in which the letters of plaintext are replaced by other letters or by numbers or symbols. If the plaintext is viewed as a sequence of bits, then substitution involves replacing plaintext bit patterns with ciphertext bit patterns.

Some type of substitution cipher:

1. **Caesar cipher:**

   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 three places further down the alphabet. For example,

```
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
```

So, K=3 and E = small later ⇒ Capital letters

Example :

Plain = meet me later ,key=3

Cipher=PHHW PH ODWHU

The assign a numerical equivalent to each letter:

a	b	c	d	e	f	g	h	i	j	k	l	m
0	1	2	3	4	5	6	7	8	9	10	11	12

n	o	p	q	r	s	t	u	v	w	x	y	z
13	14	15	16	17	18	19	20	21	22	23	24	25

Then the algorithm can be expressed as follows. For each plaintext letter *p*, substitute the ciphertext letter *C*:

$C = E(3, p) = (p + 3) \bmod 26$

A shift may be of any amount, so that the general Caesar algorithm is

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

where *k* takes on a value in the range 1 to 25. The decryption algorithm is simply

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

A brute-force attack is easly performed with Caesar cipher because:

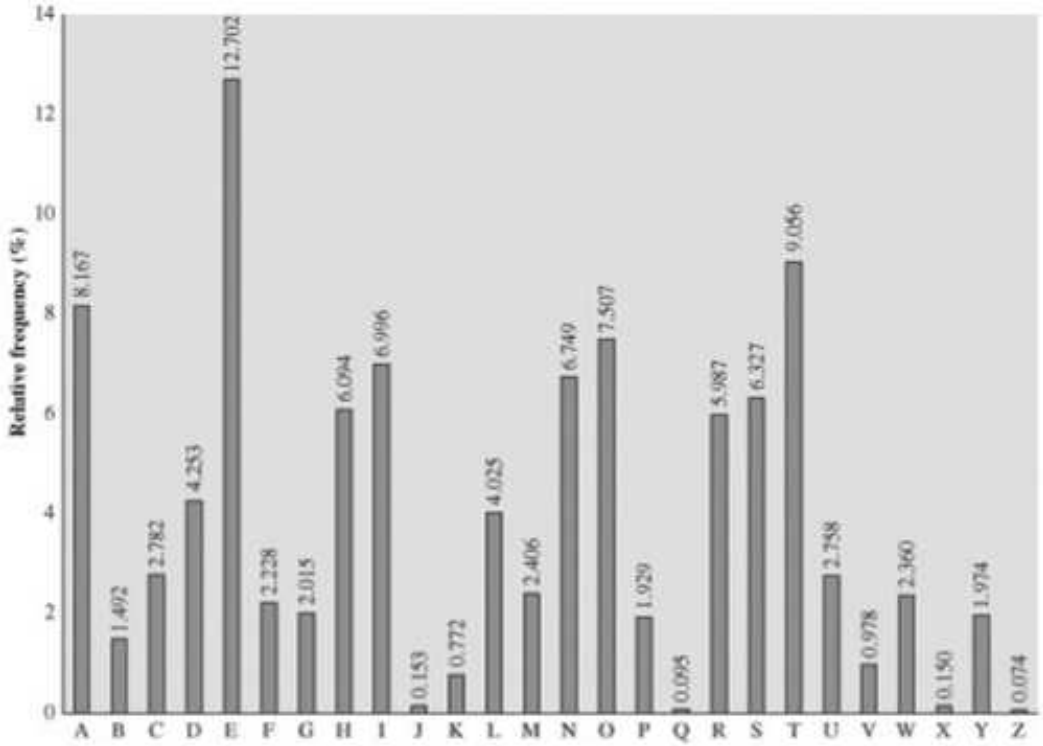
1. The encryption and decryption algorithms are known.
2. There are only 25 keys to try.
3. The language of the plaintext is known and easily recognizable.

2- **Monoalphabetic Ciphers**:

With only 25 possible keys, the Caesar cipher is far from secure.A dramatic increase in the key space can be achieved by allowing an arbitrary substitution. The "cipher" line can be any permutation of the 26 alphabetic characters, then there are 26! possible keys.

If the cryptanalyst knows the nature of the plaintext (e.g.,noncompressed English text), then the analyst can exploit the regularities of the language.

As a first step, the relative frequency of the letters can be determined and compared to a standard frequency distribution for English, such as is shown in below:



Relative Frequency of Letters in English Text

Example:

Cipher text= F W Z EZ W Q Z F Z I F

Total no. of elements=12

Z=4/12 , F=3/12 ,W=2/12

Z > F > W > E >Q >I Compare with the previous figure

Z=e , F=t , W=a ,

From the above analysis we can conclude that:

F W Z …. =t a e …. But it will be only estimation not certain and may by wrong

3- Playfair Cipher:

The best-known multiple-letter encryption cipher is the Playfair, which treats digrams in the plaintext as single units and translates these units into ciphertext digrams.

The Playfair algorithm is based on the use of a 5 x 5 matrix of letters constructed using a keyword.

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

In this case, the keyword is *monarchy*. The matrix is constructed by filling in the letters of the keyword (minus duplicates) from left to right and from top to bottom, and then filling in the remainder of the matrix with the remaining letters in alphabetic order. The letters I and J count as one letter.

Plaintext is encrypted two letters at a time, according to the following rules:

1. Repeating plaintext letters that are in the same pair are separated with a filler letter, such as x, so that balloon would be treated as ba lx lo on.
2. Two plaintext letters that fall in the same row of the matrix are each replaced by the letter to the right, with the first element of the row circularly following the last. For example, ar is encrypted as RM.
3. Two plaintext letters that fall in the same column are each replaced by the letter beneath, with the top element of the column circularly following the last. For example, mu is encrypted as CM.
4. Otherwise, each plaintext letter in a pair is replaced by the letter that lies in its own row and the column occupied by the other plaintext letter. Thus, hs becomes BP and ea becomes IM (or JM, as the encipherer wishes).