Chapter 2

Cryptography?

Cryptography is derived from Greek words

Kryptos means hidden
graphien means to write

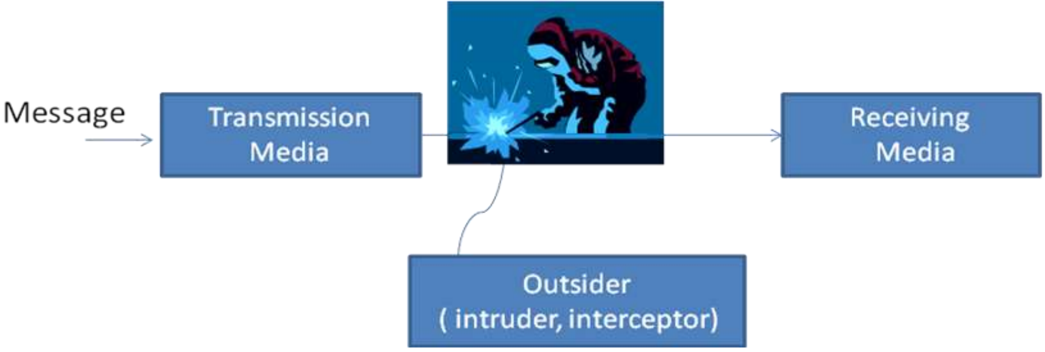
cryptography is the strongest tool for controlling against many kinds of security threats. Encrypted data cannot be read, modified, or fabricated easily.

Cryptography: is the art and science of writing in secret code

Cryptography is necessary when communicating over any untrusted telecommunication media

➔ **Cryptography** not only used to protect data from theft or alteration, but also be used for user authentication.

Steps of sending messages from a **sender**, S, to a **recipient**, R.

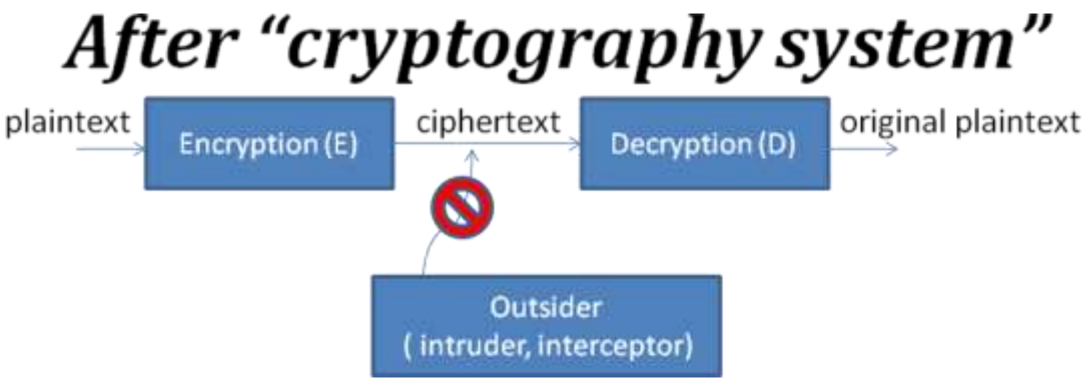


If S entrusts the message to T, who then delivers it to R, T then becomes the **transmission medium**. If an outsider, O, wants to access the message in the following ways, we call O an **interceptor** or **intruder**

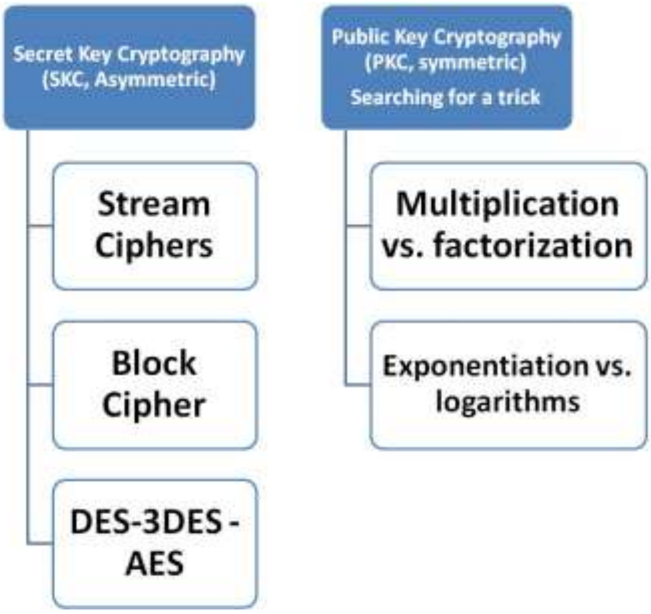
- **Block it,** by preventing its reaching R, thereby affecting the availability of the message.
- **Intercept it,** by reading or listening to the message, thereby affecting the confidentiality of the message.
- **Modify it,** by seizing the message and changing it in some way, affecting the message's integrity.
- **Fabricate** an authentic-looking message, arranging for it to be delivered as if it came from S, thereby also affecting the integrity of the message.

ملخص الأربع نقط

- Interrupt (Blocking prevent from reaching R)
-Intercept (affect Confidentiality)
-Modify (affect integrity)
-Fabricate (affect authentication)



__Encryption (E):__ is the process of encoding a message so that its meaning is not obvious (encode, encipher)
__Decryption (D):__ is the reverse process (decode, decipher)
C=E(P)
P=D(C)=D(E)


Secret Key Cryptography (SKC, Asymmetric)
Stream Ciphers
Block Cipher
DES-3DES - AES
Public Key Cryptography (PKC, symmetric)
Searching for a trick
Multiplication vs. factorization
Exponentiation vs. logarithms

There are many types of encryption. In the next two sections we look at two simple forms of encryption: **substitutions**, in which one letter is exchanged for another, and **transpositions**, in which the order of the letters is rearranged.

[3] Cryptanalysis

A cryptanalyst's chore is to **break** an encryption. That is, the cryptanalyst attempts to deduce the original meaning of a ciphertext message. By determining which decrypting algorithm matches the encrypting algorithm so that other messages encoded in the same way can be broken.

Thus, a cryptanalyst can attempt to do any or all of six different things:

- break a single message
- recognize patterns in encrypted messages, to be able to break subsequent ones by applying a straightforward decryption algorithm
- infer some meaning without even breaking the encryption, such as noticing an unusual frequency of communication or determining something by whether the communication was short or long
- deduce the key, to break subsequent messages easily

- find weaknesses in the implementation or environment of use of encryption
- find general weaknesses in an encryption algorithm, without necessarily having intercepted any message

<u>Cryptanalyst can exploit:</u>

- ***Cipher text only***
- ***Known plaintext***
- ***Algorithm and cipher text***
- ***Cipher text and plaintext***

1-Substitution Ciphers:

1-1 Caesar Cipher:

Example: c=E(p)=p+3

Key:

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
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

Plaintext= MISSION IMPOSSIBLE

E(MISSION IMPOSSIBLE) = pivvirq ipsrvvleoh

Cipher= pivvirq ipsrvvleoh

Advantages and Disadvantages of the Caesar Cipher

Most ciphers, and especially the early ones, had to be easy to perform in the field. In particular, it was dangerous to have the cryptosystem algorithms written down for the soldiers or spies to follow. Any cipher that was so complicated that its algorithm had to be written out was at risk of being revealed if the interceptor caught a sender with the written instructions. Then, the interceptor could readily decode any ciphertext messages intercepted.

The Caesar cipher is quite simple.
Its obvious pattern is also the major weakness of the Caesar cipher. A secure encryption should not allow an interceptor to use a small piece of the ciphertext to predict the entire pattern of the encryption.

<u>Caesar Cipher drawbacks</u>

- ***Breaks between words are preserved***
- ***Double letters are preserved***
- ***Guessing the common English small words (am, is, to, be, and, she).***

Example:

wrr=too, see, odd, add, off.... you can guess more!!

Cryptanalysis of the Caesar Cipher

Let us take a closer look at the result of applying Caesar's encryption technique to "TREATY IMPOSSIBLE." If we did not know the plaintext and were trying to guess it, we would have many clues from the ciphertext. For example, the break between the two words is preserved in the ciphertext, and double letters are preserved: The SS is translated to vv. We might also notice that when a letter is repeated, it maps again to the same ciphertext as it did previously. So the letters T, I, and E always translate to w, l, and h. These clues make this cipher easy to break.

Suppose you are given the following ciphertext message, and you want to try to determine the original plaintext.
wklv phvvdjh lv qrw wrr kdug wr euhdn

The message has actually been enciphered with a 27-symbol alphabet: A through Z plus the "blank" character or separator between words. As a start, assume that the coder was lazy and has allowed the blank to be translated to itself. If your assumption is true, it is an exceptional piece of information; knowing where the spaces are allows us to see which are the small words. English has relatively few small words, such as am, is, to, be, he, we, and, are, you, she, and so on. Therefore, one way to attack this problem and break the encryption is to substitute known short words at appropriate places in the ciphertext until you have something that seems to be meaningful. Once the small words fall into place, you can try substituting for matching characters at other places in the ciphertext.
Look again at the ciphertext you are decrypting. There is a strong clue in the repeated r of the word wrr. You might use this text to guess at three-letter words that you know. For instance, two very common three-letter words having the pattern xyy are see and too; other less common possibilities are add, odd, and off. (Of course, there are also obscure possibilities like woo or gee, but it makes more sense to try the common cases first.) Moreover, the combination wr appears in the ciphertext, too, so you can determine whether the first two letters of the three-letter word also form a two-letter word.

For instance, if wrr is SEE, wr would have to be SE, which is unlikely. However, if wrr is TOO, wr would be TO, which is quite reasonable. Substituting T for w and O for r, the message becomes
wklv phvvdjh lv qrw wrr kdug wr euhdn
T--- ------- -- -OT TOO ---- TO -----

1-2 Using a key word to start from

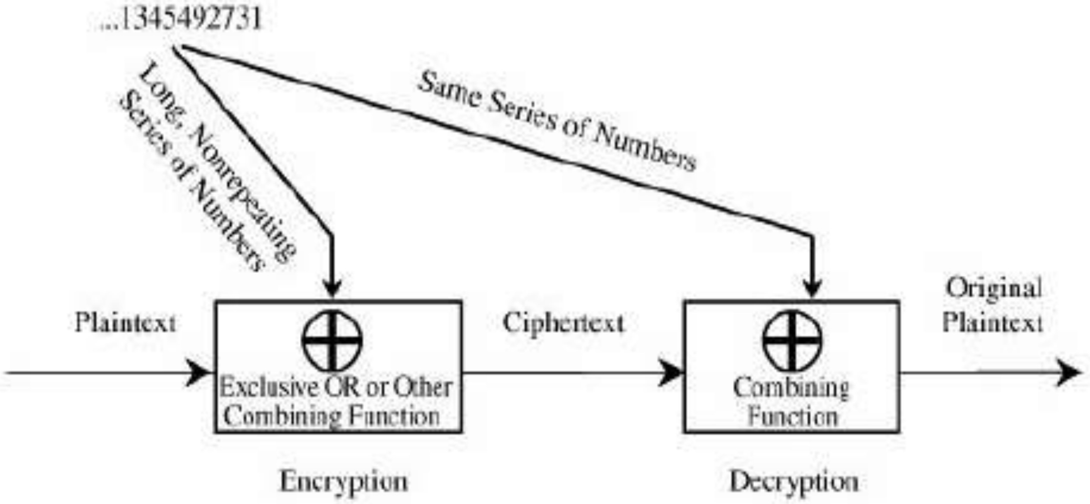
One way to scramble an alphabet is to use a key, a word that controls the permutation.

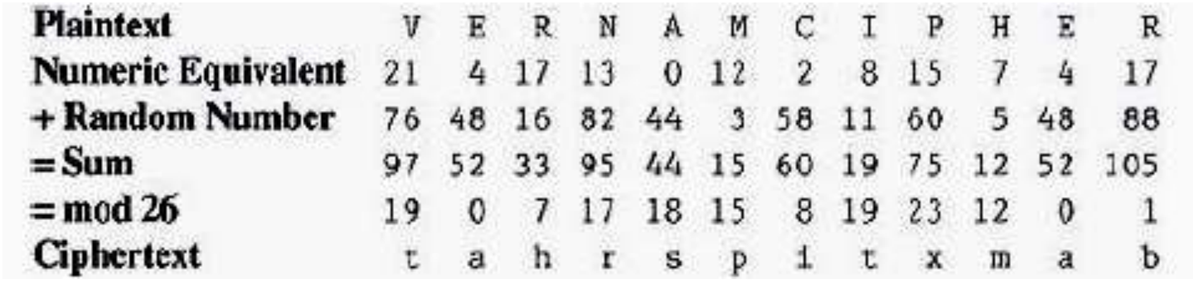
Example: *key= word*
A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
w o r d a b c e f g h I j k l m n p q s t u v x y z
Example: *key= professional*
A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
p r o f e s i o n a l a b c d g h j k m q t u v w x y z

1-3 Vernam cipher:

one-time pad is sometimes considered the perfect cipher.
A close approximation of a one-time pad for use on computers is a random number generator.

The **Vernam cipher** is a type of one-time pad devised by Gilbert Vernam for AT&T. The Vernam cipher is immune to most cryptanalytic attacks. The basic encryption involves an arbitrarily long nonrepeating sequence of numbers that are combined with the plaintext. Vernam's invention used an arbitrarily long punched paper tape that fed into a teletype machine. The tape contained random numbers that were combined with characters typed into the teletype.

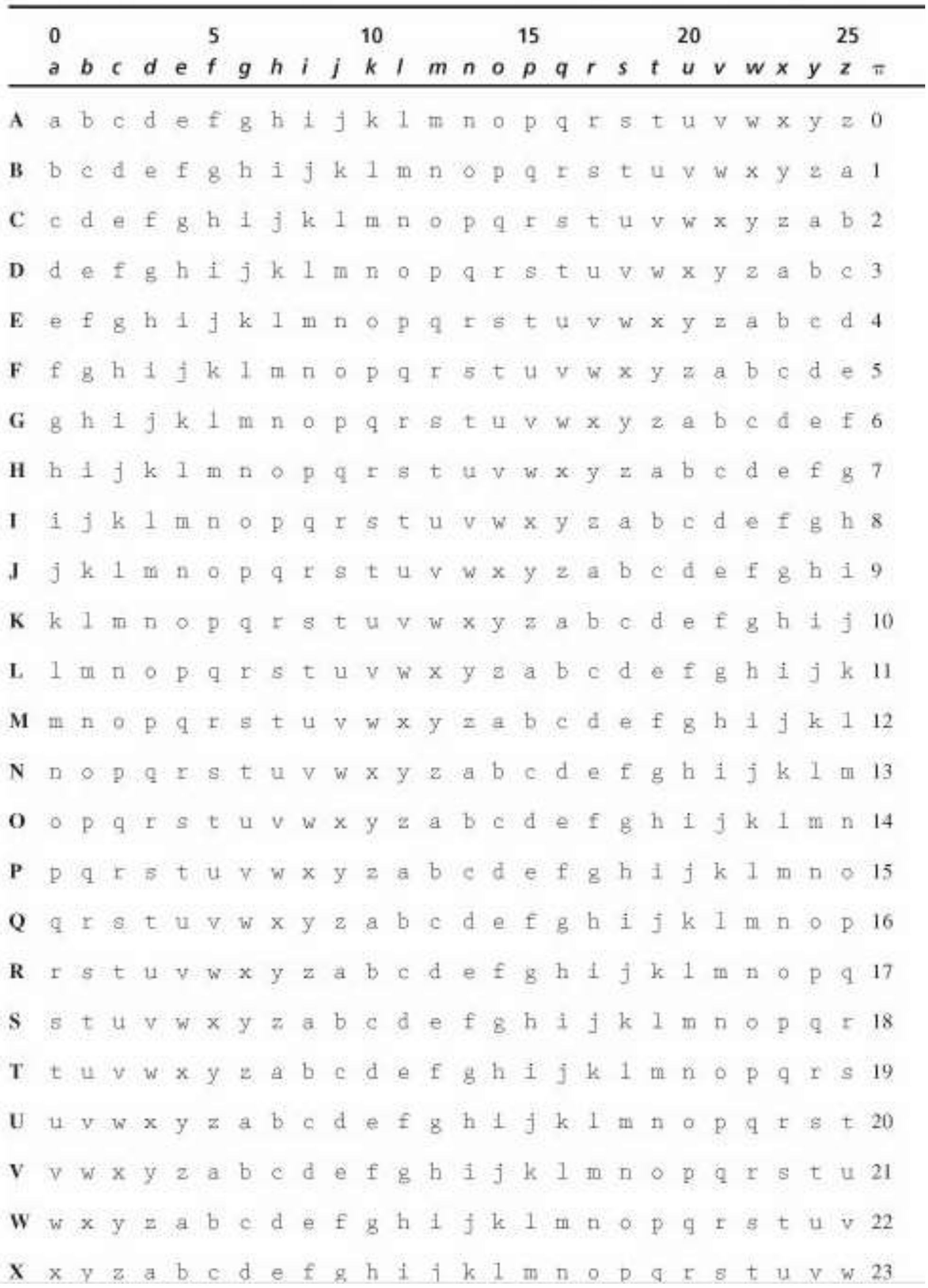




Plaintext	V	E	R	N	A	M	C	I	P	H	E	R
Numeric Equivalent	21	4	17	13	0	12	2	8	15	7	4	17
+ Random Number	76	48	16	82	44	3	58	11	60	5	48	88
= Sum	97	52	33	95	44	15	60	19	75	12	52	105
= mod 26	19	0	7	17	18	15	8	19	23	12	0	1
Ciphertext	t	a	h	r	s	p	i	t	x	m	a	b

2- Book Cipher

Another source of supposedly "random" numbers is any book, piece of music, or other object of which the structure can be analyzed. Both the sender and receiver need access to identical objects. For example, a possible one-time pad can be based on a telephone book. The sender and receiver might agree to start at page 35 and use two middle digits (ddd-DDdd) of each seven-digit phone number, mod 26, as a key letter for a substitution cipher. They use an already agreed-on table (a Vigenère tableau)



	0					5					10					15					20					25	
	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*	π
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	0
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	1
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	2
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	3
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	4
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	5
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	6
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	7
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	8
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	9
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	10
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	11
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	12
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	13
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	14
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	15
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	16
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	17
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	18
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	19
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	20
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	21
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	22
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	23

An important issue in using any cryptosystem is the time it takes to turn plaintext into ciphertext, and vice versa. Especially in the field (when encryption is used by spies or decryption is attempted by soldiers), it is essential that the scrambling and unscrambling not deter the authorized parties from completing their missions. The timing is directly related to the complexity of the encryption algorithm. For example, encryption and decryption with substitution ciphers can be performed by direct lookup in a table illustrating the correspondence, like the ones shown in our examples. Transforming a single character can be done in a constant amount of time, so we express the complexity of the algorithm by saying that the time to encrypt a message of n characters is proportional to n. One way of thinking of this expression is that if one message is twice as long as another, it will take twice as long to encrypt.

Cryptanalysis of Substitution Ciphers

The techniques described for breaking the Caesar cipher can also be used on other substitution ciphers. Short words, words with repeated patterns, and common initial and final letters all give clues for guessing the permutation.

Of course, breaking the code is a lot like working a crossword puzzle: You try a guess and continue to work to substantiate that guess until you have all the words in place or until you reach a contradiction. For a long message, this process can be extremely tedious. Fortunately, there are other approaches to breaking an encryption. In fact, analysts apply every technique at their disposal, using a combination of guess, strategy, and mathematical skill.

Cryptanalysts may attempt to decipher a particular message at hand, or they may try to determine the encryption algorithm that generated the ciphertext in the first place (so that future messages can be broken easily). One approach is to try to reverse the difficulty introduced by the encryption. To see why, consider the difficulty of breaking a substitution cipher. At face value, such encryption techniques seem secure because there are 26! possible different encipherments. We know this because we have 26 choices of letter to substitute for the a, then 25 (all but the one chosen for a) for b, 24 (all but the ones chosen for a and b) for c, and so on, to yield 26 * 25 * 24 *…* 2 * 1 = 26! possibilities. By using a brute force attack, the cryptanalyst could try all 26! permutations of a particular ciphertext message. Working at one permutation per microsecond (assuming the cryptanalyst had the patience to review the probable-looking plaintexts produced by some of the permutations), it would still take over a thousand years to test all 26! possibilities.

We can use our knowledge of language to simplify this problem. For example, in English, some letters are used more often than others. The letters E, T, O, and A occur far more often than J, Q, X, and Z, for example. Thus, the frequency with which certain letters are used can help us to break the code more quickly. We can also recognize that the nature and context of the text being analyzed affect the distribution. For instance, in a medical article in which the term x-ray was used often, the letter x would have an uncommonly high frequency.

When messages are long enough, the frequency distribution analysis quickly betrays many of the letters of the plaintext. In this and other ways, a good cryptanalyst finds approaches for bypassing hard problems. An encryption based on a hard problem is not secure just because of the difficulty of the problem.

3-Transpositions (Permutations)

The goal of substitution is confusion; the encryption method is an attempt to make it difficult for a cryptanalyst or intruder to determine how a message and key were transformed into ciphertext. In this section, we look at a different kind of scrambling with the similar goal. A **transposition** is an encryption in which the letters of the message are rearranged. With transposition, the cryptography aims for diffusion, widely spreading the information from the message or the key across the ciphertext. Transpositions try to break established patterns. Because a transposition is a rearrangement of the symbols of a message, it is also known as a permutation.

Columnar Transpositions

Transposition (permutation), Substitution drawbacks

- It depends on mathematical function = easier predictable.
- Even using a keyword, the last letters is usually less used.
- These method are characterized by being vulnerability

4- block cipher
5- stream cipher } مقارنة

Ceasar is stream
One time pad is stream
Stream cipher can function as block cipher. There is a buffer to fill up data to be encrypted as a block.

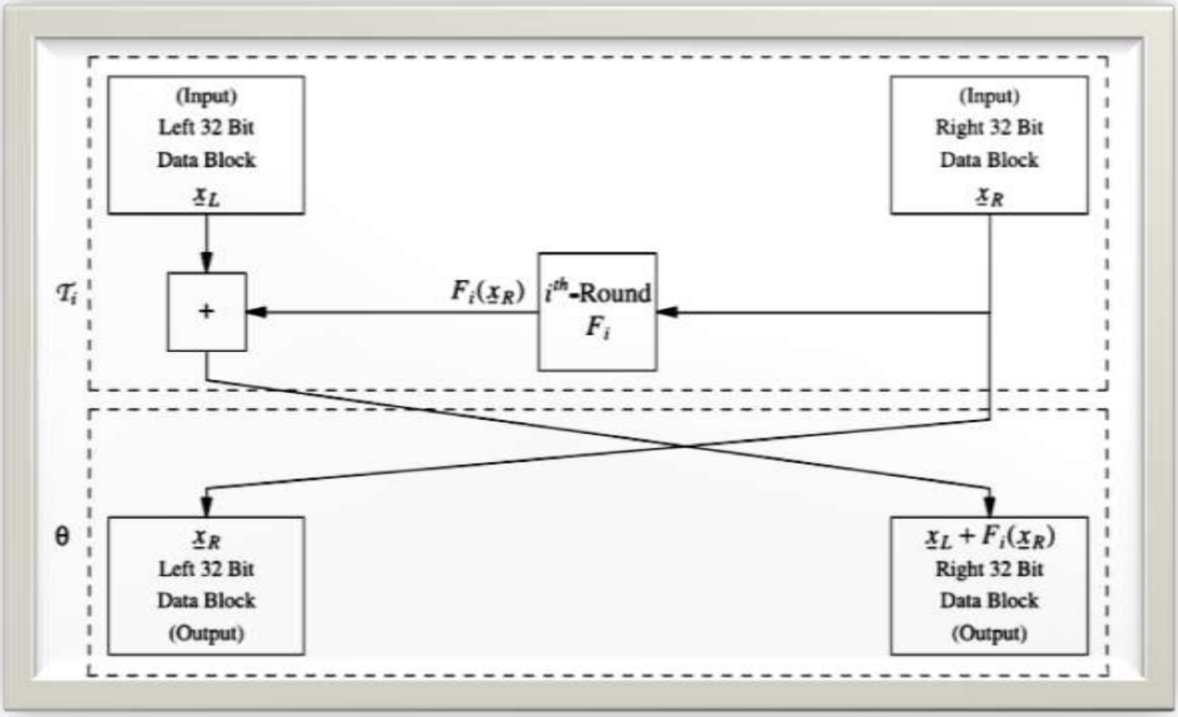
Three algorithms are popular in the commercial world:

DES (data encryption standard),

RSA (Rivest Shamir Adelman)

AES (advanced encryption standard

Data Encryption Standard



<u>*DES advantages:*</u>

- Able to provide high level of security.
- Specified and easy to understand
- Available to user
- Adaptable to different applications
- Efficient
- Economical
- Many more ……

Properties of "Trustworthy" Encryption Systems:

- **It must be based on sound mathematics*.***

not invented; derived from solid principles.

- **It has been analyzed by competent experts and found to be sound*.***
- ***It has stood the "test of time"***