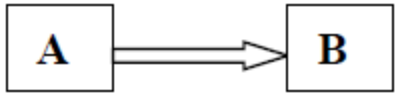
Last week

Principle security

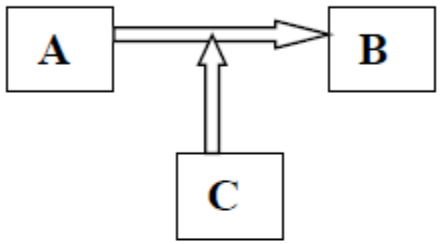
There are five principles of security. They are as follows:

- *Confidentiality:*
  The principle of confidentiality specifies that only the sender and the intended recipient should be able to access the content of the message.



Last week

- *Integrity:*
  The confidential information sent by A to B which is accessed by C without the permission or knowledge of A and B.



- *Authentication:*
  Authentication mechanism helps in establishing proof of identification.

- Non-repudiation:

- *Access control:*
  Access control specifies and control who can access what.
- *Availability:*
  It means that assets are accessible to authorized parties at appropriate times.

Last week

Attacks

We want our security system to make sure that no data are disclosed to unauthorized parties.

- Data should not be modified in illegitimate ways
- Legitimate user can access the data

Types of attacks

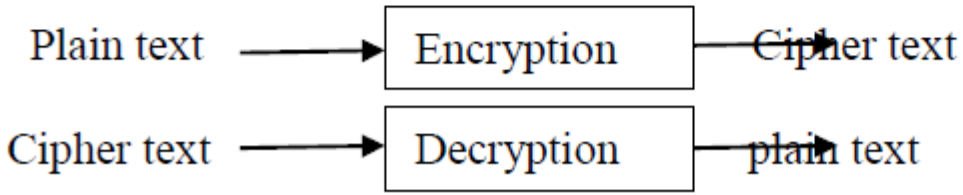
Attacks are grouped into two types:

- *Passive attacks:* does not involve any modification to the contents of an original message
- *Active attacks:* the contents of the original message are modified in some ways.

ELEMENTARY CRYPTOGRAPHY

Encryption is the process of encoding a message so that its meaning is not obvious; decryption is the reverse process, transforming an encrypted message back into its normal, original form. Alternatively, the terms encode and decode or encipher and decipher are used instead of encrypt and decrypt.That is, we say that we encode, encrypt, or encipher the original message to hide its meaning. Then, we decode, decrypt, or decipher it to reveal the original message. A system for encryption and decryption is called a cryptosystem.

The original form of a message is known as plaintext, and the encrypted form is called cipher text. For convenience, we denote a plaintext message P as a sequence of individual characters $P = <p1, p2, \ldots, pn>$. Similarly, cipher text is written as $C = <c1, c2, \ldots, cm>$.



ELEMENTARY CRYPTOGRAPHY

CONVENTIONAL ENCRYPTION

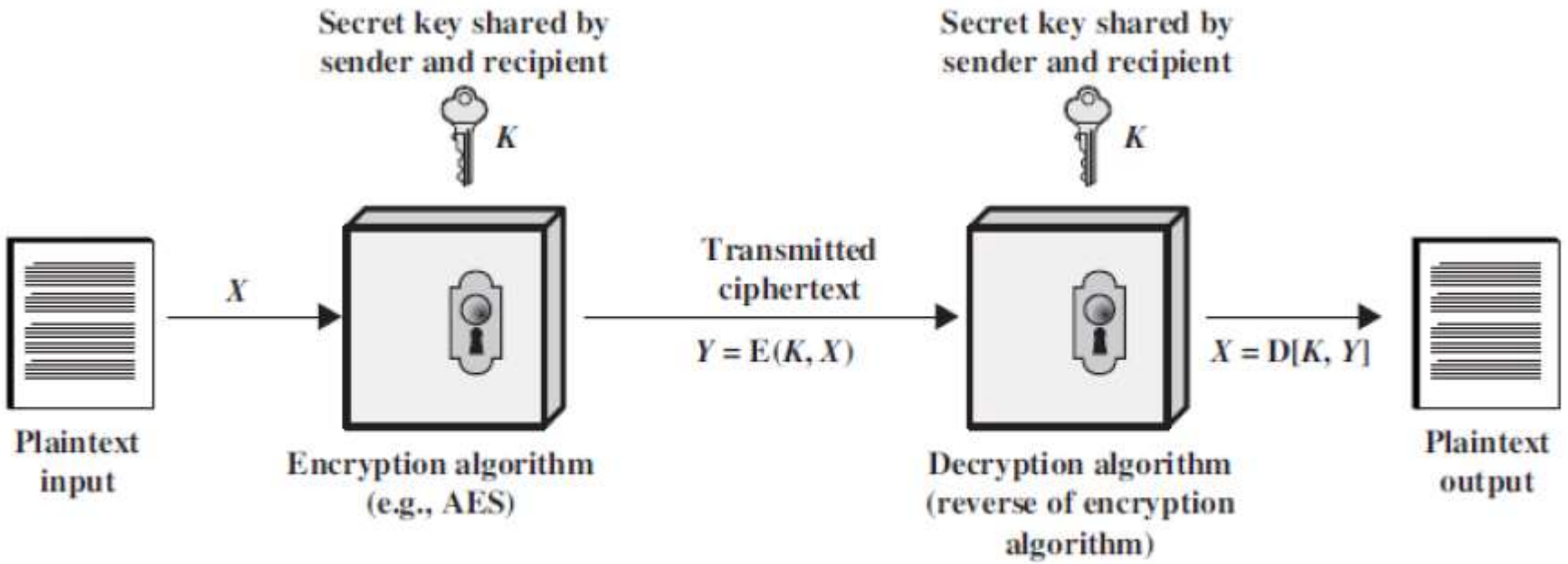
- Referred conventional / private-key / single-key
- Sender and recipient share a common key

All classical encryption algorithms are private-key was only type prior to invention of public-key in 1970"**plaintext** - the original message
Some basic terminologies used:

- **cipher text** - the coded message
- **Cipher** - algorithm for transforming plaintext to cipher text
- **Key -** info used in cipher known only to sender/receiver
- **encipher (encrypt)** - converting plaintext to cipher text
- **decipher (decrypt)** - recovering cipher text from plaintext
- **Cryptography** - study of encryption principles/methods

- **Cryptanalysis (code breaking)** - the study of principles/ methods of deciphering cipher text *without* knowing key
- **Cryptology** - the field of both cryptography and cryptanalysis

ELEMENTARY CRYPTOGRAPHY



ELEMENTARY CRYPTOGRAPHY

For instance, the plaintext message "I want cookies" can be denoted as the message string <*I, ,w,a,n,t,c,o,o,k,i,e,s*>. It can be transformed into cipher text<*c*1, *c*2, …,*c*14>, and the encryption algorithm tells us how the transformation is done.

We use this formal notation to describe the transformations between plaintext and cipher text. For example:

we write C = E (P) and P = D(C), where C represents the cipher text, E is the encryption rule, P is the plaintext, and D is the decryption rule.

P = D (E(P)).

In other words, we want to be able to convert the message to protect it from an intruder, but we also want to be able to get the original message back so that the receiver can read it properly.

The cryptosystem involves a set of rules for how to encrypt the plaintext and how to decrypt the cipher text. The encryption and decryption rules, called algorithms, often use a device called a key, denoted by *K*, so that the resulting cipher text depends on the original plaintext message, the algorithm, and the key value. We write this dependence as $C = E(K, P)$. Essentially, *E* is a *set* of encryption algorithms, and the key *K* selects one specific algorithm from the set.

There are many types of encryption. In the next 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.

ELEMENTARY CRYPTOGRAPHY

Substitutions Cipher: It basically consists of substituting every plaintext character for a different cipher text character.

It is of two types-

I. Mono alphabetic substitution cipher
II. Poly alphabetic substitution cipher

Mono alphabetic substitution cipher:

Relationship between cipher text symbol and plain text symbol is 1:1.

- Additive cipher:
  Key value is added to plain text and numeric value of key ranges from 0 – 25.

  Example:

  Plain text(P)- H E L LO (H=7,E=4,L=11,L=11,O=14)
  Key (K)=15
  Cipher text (C)= 7+15,4+15,11+15,11+15,14+15
  = 22,19, 26,26,(29%26)=3
  = W T A AD

ELEMENTARY CRYPTOGRAPHY

- Affine cipher:
  It is the combination c tive cipher

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

  Let K1 and K2 are two keys

  $C = [(P \times K1) + K2] \bmod 26$

  $P = [(C-K2) \times K1^{-1}] \bmod 26$

ELEMENTARY CRYPTOGRAPHY

Polyalphabetic substitution cipher

In polyalphabetic cipher each occurrence of a character may have different substitution. The relationship between characters in plain text and cipher text is 1 to many.

- Auto key cipher
- Playfair cipher
- Vigegeire cipher
- Hill cipher

Auto key cipher:

- In this cipher, key is stream of subkeys in which subkey is used to encrypt the corresponding character in the plain text.
- Here 1st subkey is predefined and 2nd subkey is the value of the 1st character of the plain text 3rd subkey is the value of the 2nd plain text and so on.

Example:

	A	T	T	A	C	K
	0	19	19	0	2	10
Key=12	↘	↘	↘	↘	↘	
	12	0	19	19	0	2

Cipher text(C)= (12,19,38 19,2 12)%26 ⟶ M T M T C M

ELEMENTARY CRYPTOGRAPHY

TYPES OF AUTOKEY CHIPER

There are two forms of autokey cipher: *key-autokey* and *text-autokey* ciphers. A key-autokey cipher uses previous members of the keystream to determine the next element in the keystream. A text-autokey uses the previous message text to determine the next element in the keystream.

More popular autokeys use a tabula recta, a square with 26 copies of the alphabet, the first line starting with 'A', the next line starting with 'B' etc. Instead of a single letter, a short agreed-upon keyword is used, and the key is generated by writing down the primer and then the rest of the message, as in Vigenère's version.

To encrypt a plaintext, the row with the first letter of the message and the column with the first letter of the key are located. The letter in which the row and the column cross is the ciphertext letter.

https://en.wikipedia.org/wiki/Autokey_cipher

ELEMENTARY CRYPTOGRAPHY

TYPES OF AUTOKEY CHIPER

Method
The autokey cipher, as used by members of the American Cryptogram Association, starts with a relatively-short keyword, the primer, and appends the message to it.

For example, if the keyword is QUEENLY and
the message is attack at dawn,
then the key would be QUEENLYATTACKATDAWN

Plaintext: attackatdawn
Key: QUEENLYATTACKATDAWN
Ciphertext: QNXEPVYTWTWP

The ciphertext message would thus be "QNXEPVYTWTWP".

https://en.wikipedia.org/wiki/Autokey_cipher

ELEMENTARY CRYPTOGRAPHY

TYPES OF AUTOKEY CHIPER

To decrypt the message, the recipient would start by writing down the agreed-upon keyword.

QNXEPVYTWTWP
QUEENLY

The first letter of the key, Q, would then be taken, and that row would be found in a tabula recta.
That column for the first letter of the ciphertext would be looked across, also Q in this case, and the letter to the top would be retrieved, A.
Now, that letter would be added to the end of the key:

QNXEPVYTWTWP
QUEENLYA

[a] https://en.wikipedia.org/wiki/Autokey_cipher

ELEMENTARY CRYPTOGRAPHY

TYPES OF AUTOKEY CHIPER

Then, since the next letter in the key is U and the next letter in the ciphertext is N, the U row is looked across to find the N to retrieve T:

QNXEPVYTWTWP

QUEENLYAT

At

That continues until the entire key is reconstructed, when the primer can be removed from the start.

With Vigenère's autokey cipher, a single mistake in encryption renders the rest of the message unintelligible

https://en.wikipedia.org/wiki/Autokey_cipher

	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

ELEMENTARY CRYPTOGRAPHY

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 cipher text digrams. The playfair algorithm is based on the use of 5x5 matrix of letters constructed using a keyword. Let the keyword be „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 alphabetical order.

The letter „i" and „j" count as one letter. Plaintext is encrypted two letters at a time

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

ELEMENTARY CRYPTOGRAPHY

According to the following rules:

Repeating plaintext letters that would fall in the same pair are separated with a Filler letter such as „x".

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 following the last.

Plaintext letters that fall in the same column are replaced by the letter beneath, with the top element of the column following the last.

Otherwise, each plaintext letter is replaced by the letter that lies in its own row And the column occupied by the other plaintext 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

Plaintext = meet me at the school house

Splitting two letters as a unit => me et me at th es ch o x ol ho us ex

Corresponding cipher text => CL KL CL RS PD IL HY AV MP HF XL IU

ELEMENTARY CRYPTOGRAPHY

Strength of playfair cipher

Playfair cipher is a great advance over simple mono alphabetic ciphers.

Since there are 26 letters, 26x26 = 676 diagrams are possible, so identification of individual diagram is more difficult.

ELEMENTARY CRYPTOGRAPHY

Vigener cipher:

The key stream is the repetition of the initial secret key stream of length m. (1<=m<=26)

Example:

Plaintext- A B C D E F G H

Ks= 0, 5, 8

A	B	C	D	E	F	G	H	(B=1 =>1+5=6=>G)
0	5	8	0	5	8	0	5	
0	**6**	**10**	**3**	**9**	**13**	**6**	**12**	
A	**G**	**K**	**D**	**J**	**N**	**G**	**M**	<= ciphertext

ELEMENTARY CRYPTOGRAPHY

Vigener cipher:

The key stream is the repetition of the initial secret key stream of length m. (1<=m<=26)

Example:

Plaintext- A B C D E F G H

Ks= 0, 5, 8

A	B	C	D	E	F	G	H	(B=1 =>1+5=6=>G)
0	5	8	0	5	8	0	5	
0	**6**	**10**	**3**	**9**	**13**	**6**	**12**	
A	**G**	**K**	**D**	**J**	**N**	**G**	**M**	<= ciphertext

ELEMENTARY CRYPTOGRAPHY

TYPES OF Vigenère's CHIPER

Encryption is simple: Given a key letter X and a plaintext letter y, the cipher text is at the intersection of the row labeled x and the column labeled y; in this case, the ciphertext is V.

To encrypt a message, a key is needed that is as long as the message. Usually, the key is a repeating keyword.

e.g., key = d e c e p t i v e d e c e p t i v e d e c e p t i v e PT = w e a r e d i s c o v e r e d s a v e y o u r s e l f CT = ZICVTWQNGRZGVTWAVZHCQYGLMGJ

Decryption is equally simple. The key letter again identifies the row. The position of the cipher text letter in that row determines the column, and the plaintext letter is at the top of that column.

	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

Strength of Vigenere cipher

- There are multiple cipher text letters for each plaintext letter.
- Letter frequency information is obscured.

ELEMENTARY CRYPTOGRAPHY

Transposition cipher:

A transposition cipher is a method of encryption by which the positions held by units of plaintext (which are commonly characters or groups of characters) are shifted according to a regular system, so that the ciphertext constitutes a permutation of the plaintext. That is, the order of the units is changed.

The goal of substitution is confusion; the transposition method is an attempt to make it difficult i.e diffusion.

1. Keyless transposition cipher

   There are two methods for permutation of characters

   - Text is written into a table column by column and transmitted row by row

     Example: plaintext- meet me at the park

     m e m a t e a k
     e t e t h p r

     ciphertext- memateaketethpr

   - Text is written into the table row by row and then transmitted column by column.

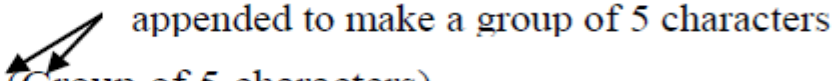
     Example: **m e e t**
     m e a t
     t h e p
     a r k

     ciphertext- mmtaeehreaekttp

ELEMENTARY CRYPTOGRAPHY

2. Keyed transposition cipher
   Plaintext is divided into groups and permutes the character in each group.
   Example: plaintext- "enemy attack at night"

   keys:



e n e m y a t t a c k a t n i g h t y z (Group of 5 characters)

encryption: e e m y n t a a c t t k n i k t g y z h

decryption: e n e m y a t t a c k a t n i g h t y z

the characters exceeding the length of plaintext are discarded.
Like y and z two characters are discarded

3. Combining the two approaches:
   Encryption and decryption is done in three steps.
   - Text is written into a table row by row.
   - Permutation is done by reordering the column.
   - New table is read column by column

1.5 MAKING GOOD ENCRYPTION ALGORITHM

So far, the encryption algorithms we have seen are trivial, intended primarily to demonstrate the concepts of substitution and permutation. At the same time, we have examined several approaches cryptanalysts use to attack encryption algorithms. Now we examine algorithms that are widely used in the commercial world.

For each type of encryption we considered, has the advantages and disadvantages. But there is a broader question: What does it mean for a cipher to be "good"? The meaning of good depends on the intended use of the cipher. A cipher to be used by military personnel in the field has different requirements from one to be used in a secure installation with substantial computer support. In this section, we look more closely at the different characteristics of ciphers.

Shannon's Characteristics of "Good" Ciphers

In 1949, Claude Shannon [SHA49] proposed several characteristics that identify a good cipher.

1. The amount of secrecy needed should determine the amount of labor appropriate for the encryption and decryption.

2. The set of keys and the enciphering algorithm should be free from complexity.

This principle implies that we should restrict neither the choice of keys nor the types of plaintext on which the algorithm can work. For instance, an algorithm that works only on plaintext having an equal number of A's and E's is useless. Similarly, it would be difficult to select keys such that the sum of the values of the letters of the key is a prime number.

Restrictions such as these make the use of the encipherment prohibitively complex. If the process is too complex, it will not be used. Furthermore, the key must be transmitted, stored, and remembered, so it must be short.

3. The implementation of the process should be as simple as possible.

Principle 3 was formulated with hand implementation in mind: A complicated algorithm is prone to error or likely to be forgotten. With the development and popularity of digital computers, algorithms far too complex for hand implementation became feasible. Still, the issue of complexity is important. People will avoid an encryption algorithm whose implementation process severely hinders message transmission, thereby undermining security. And a complex algorithm is more likely to be programmed incorrectly.

4. Errors in ciphering should not propagate and cause corruption of further information in the message.

Principle 4 acknowledges that humans make errors in their use of enciphering algorithms. One error early in the process should not throw off the entire remaining ciphertext. For example, dropping one letter in a columnar transposition throws off the entire remaining encipherment. Unless the receiver can guess where the letter was dropped, the remainder of the message will be unintelligible. By contrast, reading the wrong row or column for a polyalphabetic substitution affects only one character and remaining characters are unaffected.

5. The size of the enciphered text should be no larger than the text of the original message.

The idea behind principle 5 is that a ciphertext that expands dramatically in size cannotpossibly carry more information than the plaintext, yet it gives the cryptanalyst more datafrom which to infer a pattern. Furthermore, a longer ciphertext implies more space for storage and more time to communicate.

Properties of "Trustworthy" Encryption Systems

Commercial users have several requirements that must be satisfied when they select an encryption algorithm. Thus, when we say that encryption is "commercial grade," or "trustworthy," we mean that it meets these constraints:

- It is based on sound mathematics. Good cryptographic algorithms are not just invented; they are derived from solid principles.
- It has been analyzed by competent experts and found to be sound. Even the best cryptographic experts can think of only so many possible attacks, and the developers may become too convinced of the strength of their own algorithm. Thus, a review by critical outside experts is essential.
- It has stood the atest of time.a As a new algorithm gains popularity, people continue to review both its mathematical foundations and the way it builds on those foundations. Although a long period of successful use and analysis is not a guarantee of a good algorithm, the flaws in many algorithms are discovered relatively soon after their release.

We can divide all the cryptography algorithms (ciphers) into two groups: symmetric key cryptography algorithms and asymmetric cryptography algorithms. Figure shows the taxonomy.

1. *Symmetric-Key Cryptography*

In symmetric-key cryptography, the same key is used by both parties. The sender uses this key and an encryption algorithm to encrypt data; the receiver uses the same key and the corresponding decryption algorithm to decrypt the data.

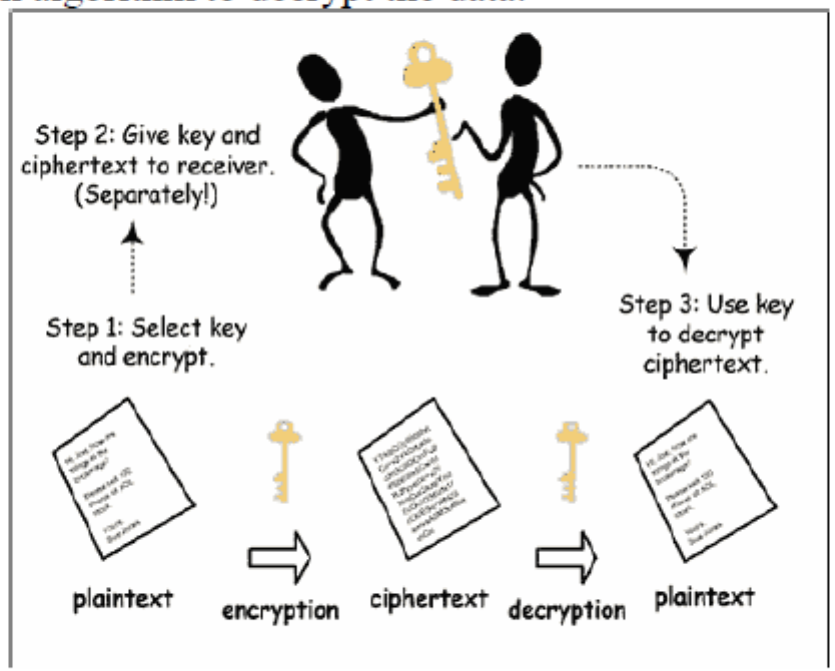
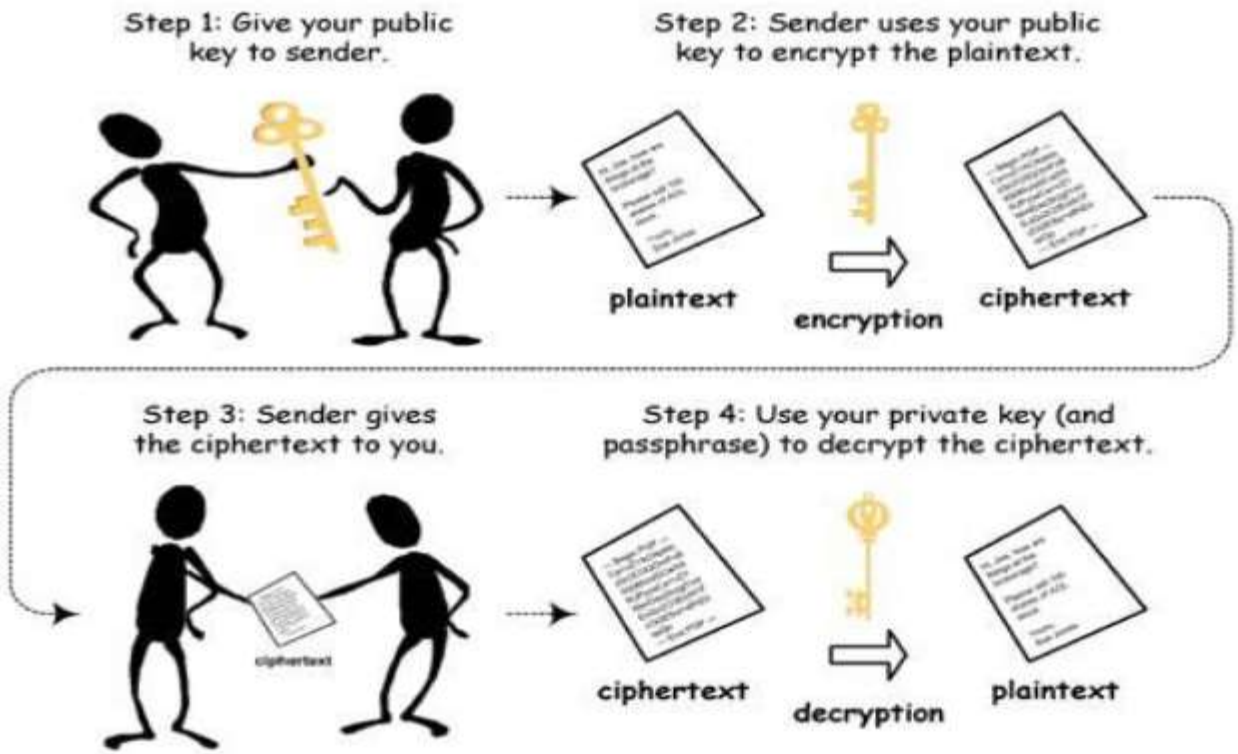


Fig :Symmetric-key Cryptography

2. *Asymmetric-Key Cryptography:*

In asymmetric or public-key cryptography, there are two keys: a private key and a public key. The private key is kept by the receiver. The public key is announced to the public.



1.6 PRIVATE KEY CRYPTO SYSTEM

Symmetric encryption (also called *private-key encryption* or *secret-key encryption*) involves using the same key for encryption and decryption.

Encryption involves applying an operation (an algorithm) to the data to be encrypted using the private key to make them unintelligible. The slightest algorithm (such as an exclusive OR) can make the system nearly tamper proof (there being so such thing as absolute security).

However, in the 1940s, *Claude Shannon* proved that to be completely secure, private-key systems need to use keys that are at least as long as the message to be encrypted. Moreover, symmetric encryption requires that a secure channel be used to exchange the key, which seriously diminishes the usefulness of this kind of encryption system.

The main disadvantage of a secret-key cryptosystem is related to the exchange of keys. Symmetric encryption is based on the exchange of a secret (keys). The problem of key distribution therefore arises:

Moreover, a user wanting to communicate with several people while ensuring separate confidentiality levels has to use as many private keys as there are people. For a group of *N* people using a secret-key cryptosystem, it is necessary to distribute a number of keys equal to *N * (N-1) / 2*.
In the 1920s, Gilbert Vernam and Joseph Mauborgne developed the *One-Time Pad* method (sometimes called "One-Time Password" and abbreviated *OTP*), based on a randomly generated private key that is used only once and is then destroyed. During the same period, the Kremlin and the White House were connected by the famous **red telephone**, that is, a

telephone where calls were encrypted thanks to a private key according tothe *one-time pad* method. The private key was exchanged thanks to the diplomatic bag (playing the role ofsecure channel).

An important distinction in symmetric cryptographic algorithms is between stream and block ciphers.

Stream cipher: Stream ciphers convert one symbol of plaintext directly into a symbol of ciphertext.

Advantages:

- Speed of transformation: algorithms are linear in time and constant in space.
- Low error propogation: an error in encrypting one symbol likely will not affect subsequent symbols.

Disadvantages:

- Low diffusion: all information of a plaintext symbol is contained in a single ciphertext symbol.
- Susceptibility to insertions/ modifications: an active interceptor who breaks the algorithm might insert spurious text that looks authentic.

Block ciphers: It encrypt a group of plaintext symbols as one block.

Advantages:

- High diffusion: information from one plaintext symbol is diffused into several ciphertext symbols.
- Immunity to tampering: difficult to insert symbols without detection.

Disadvantages:

- Slowness of encryption: an entire block must be accumulated before encryption / decryption can begin.
- Error propagation: An error in one symbol may corrupt the entire block.

Simple substitution is an example of a stream cipher. Columnar transposition is a block cipher.