Information Security

- ## Important concepts :

  - Protocol : is a system of **rules** about the correct way to act in formal situations.
  - TCP/IP : TCP/IP stands for **Transmission Control Protocol/Internet Protocol** and is a suite of communication protocols used to **interconnect network devices** on the internet.
  - Information = data + processing
  - Plain text : نص واضح
  - Cypher text : نص مشفر
  - Traphic : حجم هائل من البيانات المنقولة من المرسل إلى المستقبل
  - Cables :
    - UTP(unshielded twisted pair)
    - STP(shielded twisted pair)
    - fiber
  - Cypher text by
    - Algorithms
    - Key
  - Symmetric encryption: is a type of encryption where only one key (a secret key) is used to both encrypt and decrypt electronic data.
  - Asymmetric encryption: uses a mathematically related pair of keys for encryption and decryption: a public key and a private key.

- ## Security Requirements Services :

  1. Confidentiality : We use algorithms to cypher text the message.
  2. Integrity : The message should be received without any changes.
  3. Authentication : Check the sender identity be **Ip Address**.
  4. Availability : It should be all time available.
  5. Non-Repudiation : Denial of service.
  6. Access Control : To give access to certain people.

- ## Levels of impact :
  - Low
  - Moderate

    - High

- Threat : a potential for violation of security.
- Attack : an assault on system security, a deliberate attempt to evade security services :
    - Passive attack : an attacker observes the messages and copies them.
    - Active attack : an attacker tries to modify the content of the messages.

- Ciphertext = Encryption(Message , Single key)
- Message = Decryption (Ciphertext , Key)

- Classical approach:

    - Substitution cipher method:

        - Monoalphabetic

            - Caesar
            - Simple keyword monoalphabetic
            - Simple keyword with columnar
            - Mixed alphabetic with coulmnanal and numeric digits

        - Polygraphic cipher method

            - PLayFair
            - Hill
        - Transposition cipher method

            - Rail Fence
            - One Time Pad

Caesar

Example :

plainText = ammar
Key = 4

CipherText = eqqev
cipher letter = key + index

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

Simple keyword monoalphabetic

Example :

keyword = ammar = amr
plainText = ammar
CipherText = akkaq

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

Simple keyword with columnar

Example :

keyword = ammar = amr
plainText = ammar

اخر صف → اول صف

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

CipherText = aiiaz

Mixed alphabetic with coulmnanal and numeric digits

Example :

keyword = ammar (غير مسموح التكرار) = amr
plainText = ammar

الترتيب يكون حسب رقم العامود (توزيع ارقام الاعمدة يكون عشوائي)

2	1	3
a	m	r
b	c	d
e	f	g
h	i	j
k	l	n
o	p	q
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	s	t	y	v	w	x	y	z
m	c	f	i	l	p	t	w	z	a	b	e	h	k	o	s	v	y	r	d	g	j	n	q	u	x

CipherText = mhhmy

Play Fair

Example :

keyword = ammar (غير مسموح التكرار) = amr
plainText = hello (الحرف المكرر نضع بعد الحرف الاول اكس ومع الحرف الاخير اكس)

	1	2	3	4	5
1	a	m	r	b	c
2	d	e	f	g	h
3	i / j	k	l	n	o
4	p	q	s	t	u
5	v	w	x	y	z

- We gather each two letters in one word, and if there are two letters beside each other we take the first letter + x and put the last letter x.

he	lx	lo	x
df	sr	ijn	x

- Notes:
  - If the letters are in the same column but not the same row:
    - CipherLetter = <u>the one under it.</u>
  - If the letters neither in same column nor row:
    - CipherLetter = <u>same letter rowe & other letter column</u>.
  - If the letters are in same row
    - CipherLetter = the letter beside the plain letter.

Hill cipher method

Example:

PlainText: eg

$$K = \begin{matrix} 3 & 2 \\ 3 & 5 \end{matrix} \rightarrow (dcdf)$$

$$K = \begin{matrix} d & c \\ d & f \end{matrix} \cdot \begin{matrix} e \\ g \end{matrix} \quad \text{mod } 26$$

$$K = \begin{matrix} 3 & 2 \\ 3 & 5 \end{matrix} \cdot \begin{matrix} 4 \\ 6 \end{matrix} \quad \text{mod } 26$$

e = ((3 * 4) + (2 * 6)) mod 26 = 24 = y
g = ((3 * 4) + (5 * 6)) mod 26 = 16 = q

- Decryption: $K = \begin{matrix} d & c \\ d & f \end{matrix} \cdot \begin{matrix} y \\ q \end{matrix} \quad \text{mod } 26$

Rail Fence

It's a simple transposition method in which the plaintext is written down as a sequence of diagrams (columns) and then read off as a sequence of rows.

Example:

Cipher the M = meet me after class using rail fence with depth 2

Row 1:   e t e f e t e l s
Row 2: m e m a t r h c a s

C = etefetelsmematrhcas

One Time Pad

Malicious Software

Is an algorithm written by a coder in order to harm others.

RSA

Generate key :

- Choose two primes p, q
- Compute n = p * q
- Compute euler φ = (p-1)(q-1)
- Choose e, 1<e<euler and must be comprime with euler (لا يوجد قواسم مشتركة بينهم)

K is (n,e)

Encryption = $M^{e}\ mod\ n$

Decryption = $C^{d}\ mod\ n$

D = $(d + \varphi(n))$ / e * until integer result d will be accepted.