2.3 SUBTITUTION CIPHERS.

2.3.1 SIMPLE SUBTTTUION CIPHERS:

In simple substitution (or monoalphabetic) ciphers, each character of the plaintext is replaced with a corresponding character of ciphertext. A single one-to-one mapping function (f) from plaintext to ciphertext character is used to encrypt the entire message using the same key (k); such that

Ek(M)=f(m1)f(m2)….. f(mN)=C

Where N: is the length of the message.

M: is plaintext message given by M= (m 1, m2 ...... mN).

C: is ciphertext message given by C=(c1, c2,….,cN)

Simple substitution ciphers are often called monoalphabetic ciphers, figure (2-2) represents two concentric rings of which the outer is free to rotate and represent the ciphertext while the inner one represent the plaintext. If the outer one is moved to a certain position then the plaintext letters could be enciphered by replacing each letter by the one out side it. The letter frequency distribution is preserved in the ciphertext. Several forms of f can be used in simple substitution, such as:

- **Shifted alphabet (Caesar cipher):**

f(mi) - (mi + k) mod n

Where **k** is the number of positions to be shifted, mi is a single character of the

alphabet, and **n** is the size of the alphabet.

If k = 3 then we can encrypt the following message as:

M: R E N A I S S A N C E

Ek(M): U H Q D L V V D Q F H

- **Multiplication based (decimation):**

$$f(mi) = mi * k \bmod n$$

where **k** and **n** are relatively prime in order to produce a complete set of residues.

Example: k = 9; then the above message can encrypted as:

M: R E N A I S S A N C E

Ek(M): X K N A U G G A N S K

If k and n are not prime, several letters will encipher to the same ciphertext letter, and not all letters will appear in the ciphertext.

<u>Home work:</u> try it when k = 13

- **Addition and multiplication (affine) :**

$$f(mi)= (mi * k1+k0) \bmod n$$

Where **k1** and **n** are relatively prime.

Simple substitution ciphers does not hide the underlying frequencies of the different letters of the plaintext, and hence it can be easily broken.

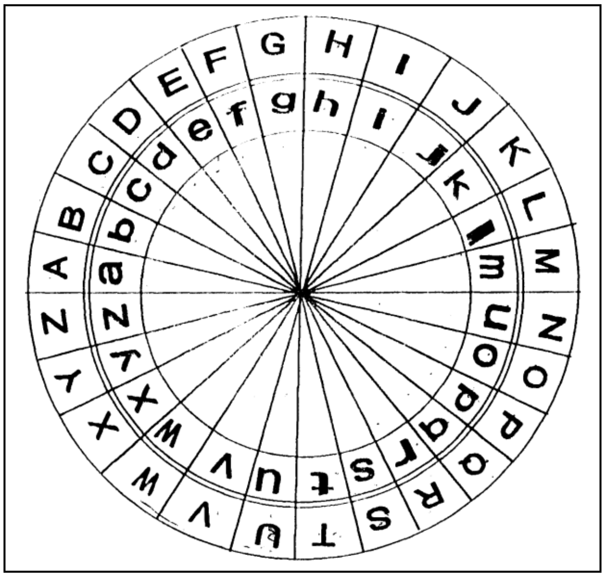

Figure (2-2) simple substitution dis

2.3.2 POLYALPHABETIC SUBSTITUTION CIPHER:

A Polyalphabetic cipher means a sequence of monoalphabetic ciphers, which are often referred to as its substitution alphabets or just alphabet. In another meaning; it is made of multiple simple substitutions. The sequence of the substituting alphabet may have fixed length (d) and is denoted as its period.

Given a period d, cipher alphabet (C1, ..., C2, and $fi : A \longrightarrow Ci$ be a mapping from a plaintext A to its ciphertext C, and M =m1,…,md,md+1,…,m2d,... is enciphered by repeating the sequence of mapping f1,…,fd every d characters.

Ek(M)=f1(m1),…,fd(md) , f1(md+1),….,fd(m2d)

For d=1 ,the cipher is monoalphabetic

A popular form of periodic substitution ciphers is the **Vigenere cipher**. The key is specified by a sequence of letters, K= k1,k2,…,kd , then Vigenere cipher system is defined as:

fi (mi) = (mi +ki) mod n for i=1,2, ..., d

Example:

M: C O D E B R E A K I N G

K: r a d i o r a d i o r a

C: T O G M P I E D S W E G

Another periodic cipher, is **Beaufort cipher**, which is similar to Vigenere but using subtraction instead of addition, and defined as :

fi (mi) = (ki - mi) mod n

2.3.3 HOMOPHONIC SUBSTITUTION CIPHER:

Homophonic substitution ciphers maps each character (a) of the plaintext alphabet into a set of ciphertext elements f(a) called homophone. Thus the mapping function f from plaintext to ciphertext is of the form: $f:A \longrightarrow 2^{c}$. Example of such ciphers are **Beale** , and **High order homophonic ciphers.**

- **BEALE CIPHERS:**

A plaintext message M=m1 m2... .... is encrypted as C = c1 c1 ... . where ci is picked at random from the set of homophones f(mi).

Example: English letters are enciphered as integers (0 - 99), a group of integers are assigned to a letter proportional to the relative frequency of the letter, as follows:

Letter	Homophones
A	17 19 34 4 56 60 67 83
I	08 22 53 65 88 90
L	03 44 76
N	02 09 15 27 32 40 59

0	01 11 23 28 42 54 70 80
P	33 91
T	05 10 20 29 45 58 64 78 99

M= P L A I N P I L 0 T

C= 91 44 56 65 59 33 08 76 28 78

Homophonic substitution ciphers are more complicated than simple substitution ciphers, but still do not obscure all of the statistical properties of the plaintext language.

- **HIGER-ORDER HOMOPHONICS:**

It is possible to construct higher-order homophonic ciphers such that an intercepted ciphertext will decipher into more than one meaningful message under different keys. To construct 2nd - order homophonic cipher, (lie number (1 - n2) are randomly inserted into (n * n) matrix K, whereas columns and rows correspond to the characters of the plaintext alphabet (A). For each character a , row a defines one set of homophones f1(a), and column a defines another set of homophones f2(a). There are two keys (mapping) f1, and f2. The ciphertext is selected from the intersection f1(mi),and f2(xi).

Ci = [mi , xi].

Where M = ml m2 ... ... Message,

X = xl x2 ... . Dummy message.

Example : if n= 5, 5 *5 matrix for the alphabet [E, I, L, M, S]:

	E	**I**	**L**	**M**	**S**
E	10	22	18	02	11
I	12	01	25	05	20
L	19	06	23	13	07
M	03	16	08	24	15
S	17	09	21	14	04

Then the message (**smile**) is enciphered as:

M: S M I L E

X: L I M E S

C: 21 16 05 19 11

2.3.4 POLYGRAM SUBSTITUTION CIPHER:

Polygram cipher systems are ciphers in which group of letters are encrypted together, and includes enciphering large blocks of letters. Therefore, permits arbitrary substitution for groups of characters. For example the plaintext group "ABC" could be encrypted to "RTQ", "ABB" could be encrypted to "SLL", and so on. In another meaning, encryption includes substitution of a block of multiple letters from plaintext with the corresponding group of ciphertext. Example of such ciphers are **Playfair**, and **Hill ciphers.**

- **PLAYFA1R CIPHER:**

playfair cipher is a digram substitution cipher, the key is given by a 5*5 matrix of 25 letters (j was not used), as described in figure 2-3.

Each pair of plaintext letters are encrypted according to the following rules:

l. if m1 and m2 are in the same row, then c1 and c2 are to the right of m1 and m2 , respectively. The first column is considered to the right of the last column.

2. if m1 and m2 are in the same column, then c1 and c2 are below m1 and m2 respectively. the first row is considered to be below the last row.

3. if m1 and m2 are in different rows and columns, then c1 and c2 are the other two corners of the rectangle.

4. If m1=m2 a null letter is inserted into the plaintext between m1 and m2 to eliminate the double.

5. If the plaintext has an odd number of characters, a null letter is appended to the end of the plaintext.

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

Figure 2-3 Key for Playfair cipher

Example:

M = RE NA IS SA NC EX

Ek(M) = HG WC BH HR WF GV

- **HILL CIPHER:**

Hill cipher performs linear transformation on d plaintext characters to get d cipher text characters. If d = 2, M= m1 m2 , then C = Ek(M) = C1 C2 where:

C1 =(k11 m1 + k12 m2) mod n

C2 =(k21 m1 + k22 m2) mod n

Expressing M and C as column vectors:

C = Ek(M) = KM where K is matrix of coefficients:

$$\begin{pmatrix} K11 & k12 \\ K21 & k22 \end{pmatrix} \quad \text{that is} \quad \begin{pmatrix} c1 \\ c2 \end{pmatrix} = \begin{pmatrix} k11 & k12 \\ k21 & k22 \end{pmatrix} \begin{pmatrix} m1 \\ m2 \end{pmatrix} \text{ mod n}$$

Deciphering is done using the inverse matrix K^{-1}

Dk =(C)= K^{-1C} mod n = K^{-1} K M mod n =M

Where K K^{-1} mod n = I , I is 2*2 identity matrix.

Example : To encipher the message **EG** :

$$\text{Let k} = \begin{pmatrix} 3 & 2 \\ 3 & 5 \end{pmatrix}$$

$$\text{Where} \quad k * k^{-1} \text{ mod } 26 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

$$\text{Then} \quad k^{-1} = \begin{pmatrix} 15 & 20 \\ 17 & 9 \end{pmatrix}$$ " by using Gauss elimination "

$$C = k * M \text{ mod } 26 = \begin{pmatrix} 4 & 2 \\ 3 & 5 \end{pmatrix} * \begin{pmatrix} 3 \\ 6 \end{pmatrix} \text{ mod } 26 = \begin{pmatrix} 24 \\ 16 \end{pmatrix}$$

Then the C = YQ

To decipher :

$$K^{-1} * C \bmod 26 = M$$

$$\begin{pmatrix} 16 & 20 \\ 17 & 9 \end{pmatrix} * \begin{pmatrix} 24 \\ 16 \end{pmatrix} \bmod 26 = \begin{pmatrix} 4 \\ 6 \end{pmatrix} = \begin{pmatrix} E \\ G \end{pmatrix}$$