Al-Mustaqbal University

College of Sciences

Intelligent Medical System Department

جامـــــعة المــــستــقبــل
AL MUSTAQBAL UNIVERSITY

كلية العلوم

قســـم الانظمة الطبية الذكية

Lecture: (6)

Information Security in Healthcare

Subject: Homophonic substitution cipher Vegene'r cipher,
Bearfut cipher,

Level: Fourth

Lecturer: Prof. Dr. Mehdi Ebady Manaa

Homophonic Substitution Cipher

Homophonic substitution ciphers maps each character (a) of the plaintext alphabet into a set of ciphertext elements f(a) called **homophone**. **Beale**, and **High order** are example of homophonic ciphers.

In a **homophonic substitution cipher**, a single plaintext symbol is mapped to **multiple possible ciphertext symbols**.

Instead of the classical substitution:

$$a \rightarrow x$$

where each plaintext letter corresponds to exactly one ciphertext symbol, the homophonic model defines a **set of possible symbols**:

$$a \rightarrow \{x1, x2, x3, ..., xk\}$$

During encryption, one element from this set is **selected randomly**.

Thus, for a plaintext message

$M = m1, m2, ..., mn$

the ciphertext becomes

$C = c1, c2, ..., cn$

where each ciphertext symbol c_i is chosen randomly from the set of homophones assigned to the plaintext character m_i

$$ci \in f(mi)$$

The mapping function

$f:A \to P(S)$

assigns each plaintext symbol in alphabet A to a **subset of ciphertext symbols** taken from the symbol space S.

This structure distributes the statistical frequency of common letters across several ciphertext symbols, thereby weakening traditional **frequency analysis attacks** used against simple substitution 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= PLAIN PIL0T

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.

Higher-Order Homophonic

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, (i.e., number (1 ➔ n^2) 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]:

$$\begin{array}{cccccc}
 & \mathbf{E} & \mathbf{I} & \mathbf{L} & \mathbf{M} & \mathbf{S} \\
\mathbf{E} & 10 & 22 & 18 & 02 & 11 \\
\mathbf{I} & 12 & 01 & 25 & 05 & 20 \\
\mathbf{L} & 19 & 06 & 23 & 13 & 07 \\
\mathbf{M} & 03 & 16 & 08 & 24 & 15 \\
\mathbf{S} & 17 & 09 & 21 & 14 & 04
\end{array}$$

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**

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. Examples of such ciphers are **Playfair** and **Hill ciphers.**

PlayFair Cipher:

Playfair cipher is a diagram 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:

1. 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:

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

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

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

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