International Journal of Computer Architecture and Mobility
(ISSN 2319-9229) Volume 2-Issue 4, February 2014

Overview of Conventional Encryption Techniques

Shadab Pasha
CDGI,Indore
shadabpasha@gmail.com

Abstract: *Symmetric Encryption or Single-key Encryption or* ***Conventional Encryption*** *was only the type of encryption before the development of the public key encryption. In Symmetric encryption sender and receiver both uses the same key. In this paper, first I will discuss the generalized conventional Cryptosystem model and then the main focus will be shifted on various Symmetric Encryption Techniques.*

1. Introduction

Cryptographic Systems are generally categorized by one of the following three criteria:

(1) The types of operations (substitution or transposition) which are used to get cipher-text from the plain-text. In *Substitution* Technique, each element in the plain-text is transformed into its corresponding cipher-text letter whereas in *Transposition* Technique all the elements of the plain-text letters are rearranged to get the cipher-text.

(2) The numbers of keys are used. If the sender and the receiver use the same key, the system is referred to as *Symmetric Encryption* and if the sender and the receiver each uses a different key, the system is referred to as *Asymmetric Encryption*.

(3) The way in which the plain-text is processed. A *Block Cipher* processes the input block of elements at a time and produces the same sized cipher-text block. A *Stream Cipher*processes the input elements continuously, producing output one element at a time.

2. Model of Conventional Cryptosystem :

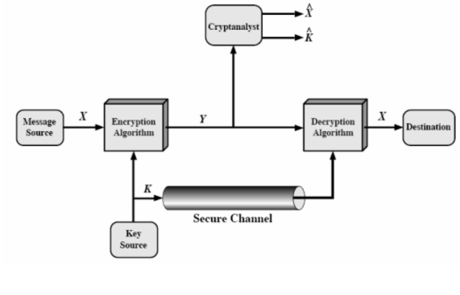


Figure – 1 Conventional Cryptosystem Model

Figure-1 shows the essential elements of the symmetric encryption scheme.

A source produces the message in plain-text,

$X = [\ x_1, x_2, x_3, \ldots\ldots\ldots\ldots, X_M\ ]$

Where, M elements of the message x are the letters in some finite alphabet.

For Encryption, the key of the form,

$K = [\ k_1, k_2, k_3, \ldots., k_J\ ]$ is generated.

With the message X and the Encryption Key K as input, the Encryption algorithm produces the corresponding Cipher-text,

$Y = [\ y_1, y_2, y_3, \ldots\ldots\ldots\ldots.., y_N]$.

So, at the sender-side we can easily write, the cipher-text, $\mathbf{Y = E_K(\ X\ )}$.

The receiver is able to retrieve the plain-text message by inverting this transformation using the same key K, So we can write, $\mathbf{X = D_K(\ Y\ )}$.

3. Substitution Techniques :

A Substitution Technique is one in which the letters of plaintext are replaced by other letters or by numbersor by symbols. The various Substitution Techniques are as follows :

- Caesar Cipher
- Monoalphabetic Ciphers
- Playfair Cipher
- Polyalphabetic Ciphers

(1) CaeserCipher :

The Caeser Cipher involves replacing of each letter of the alphabet with the letter standing three places further down the alphabet.

The alphabet is wrapped around, so that the letter following Z is A.

Example :

plain-text : meet me behind the lab
cipher-text : PHHW PH EHKLQG WKH ODE

If we will assign numerical equivalent to each letter i.e. a = 0, b = 1, …., z = 25, then this method can be expressed as follows :

The cipher-text C for the plain-text letter p is,

C = (p + 3) mod 26.

In general, the shift can be any amount so we can write,

C = (p + k) mod 26

where k is the key value ranges from 1 to 25.

Similarly, in general we can write, the plain-text,

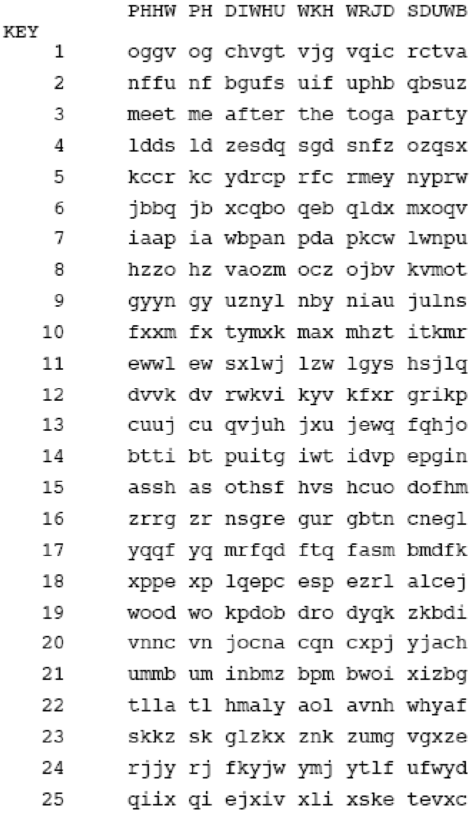
p = (C - k) mod 26.

Analysis :

- The encryption and decryption algorithms are known.
- There are only 25 possibilities to try. So brute-force analysis is easily applicable.
- Following is the example that shows how the brute-force is applicable on this cipher.

Preventive Measures :

- If the language of the plain-text is unknown, the plain-text output may not be easily recognized by cryptanalyst. So the language used should be unknown to cryptanalyst.



```
            PHHW PH DIWHU WKH WRJD SDUWB
KEY
   1        oggv og chvgt vjg vqic rctva
   2        nffu nf bgufs uif uphb qbsuz
   3        meet me after the toga party
   4        ldds ld zesdq sgd snfz ozqsx
   5        kccr kc ydrcp rfc rmey nyprw
   6        jbbq jb xcqbo qeb qldx mxoqv
   7        iaap ia wbpan pda pkcw lwnpu
   8        hzzo hz vaozm ocz ojbv kvmot
   9        gyyn gy uznyl nby niau julns
  10        fxxm fx tymxk max mhzt itkmr
  11        ewwl ew sxlwj lzw lgys hsjlq
  12        dvvk dv rwkvi kyv kfxr grikp
  13        cuuj cu qvjuh jxu jewq fqhjo
  14        btti bt puitg iwt idvp epgin
  15        assh as othsf hvs hcuo dofhm
  16        zrrg zr nsgre gur gbtn cnegl
  17        yqqf yq mrfqd ftq fasm bmdfk
  18        xppe xp lqepc esp ezrl alcej
  19        wood wo kpdob dro dyqk zkbdi
  20        vnnc vn jocna cqn cxpj yjach
  21        ummb um inbmz bpm bwoi xizbg
  22        tlla tl hmaly aol avnh whyaf
  23        skkz sk glzkx znk zumg vgxze
  24        rjjy rj fkyjw ymj ytlf ufwyd
  25        qiix qi ejxiv xli xske tevxc
```

(2) MonoalphabeticCiphers :

With only 25 possible keys, the Ceaser Cipher is very far from secure. This security can be increased by allowing the arbitrary substitution.

For Example, mapping of plain-text message and cipher-text message is defined as follows :

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

Example :

plain-text :ifwewishtoreplaceletters
cipher-text:WIRFRWAJUHYFTSD
VFSFUUFYA

Analysis :

- The plain-text letter is any permutation of the 26 alphabetic characters, then there are total 26! or greater than 4 X 1026 possible keys. So, this system is more secure than Caeser Cipher.
- The problem with this cipher is the language characteristics.This cipher is easy to break because they reflect the frequency data of the original alphabet.
- The most powerful cryptanalysis is possible with the use of digram(two-letter combination) and trigram(three-letter combination) frequencies.

Preventive Measures :

- The more security can be provided by using the multiple substitutes, known as homophones, for a single letter. If the number of symbols assigned to each letter is proportional to the relative frequency of that letter, then the single-letter frequency information is completely obliterated.

(3) Playfair Cipher :

The best-known multi-letter encryption technique is Playfair Cipher, in which digrams in the plain-text letters are treated as single units and translates these units into cipher-text digrams.

The Playfair cipher is based on the use of 5 X 5 matrix of letters constructed using the predefined keyword compromised by both sender and receiver.

Example:

If the keyword is INFORMATION, then the matrix is constructed by filling in the letters of the keyword from left to right and from top to bottom, and then filling in the remainder of the matrix with remaining letters in the alphabetical order. In this case, the matrix will be as follows:

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

The letters J and K are treated as one letter. Two plain-text letters are encrypted at a time according to the following rules:

(1) if a pair is a repeated letter, insert a filler like ‘ X ' ,
eg. “ balloon " encrypts as “ ba lx lo on "

(2) if both letters fall in the same row, replace each with letter to right (wrapping back to start from end)
eg. “ at " encrypts as “ TB "

(3) if both letters fall in the same column, replace each with the letter below it (again wrapping to top from bottom),
eg. “ ep " encrypts to “ PW "

(4) otherwise each letter is replaced by the one in its row in the column of the other letter of the pair,
eg. “ hf " encrypts to “ GO "

Analysis :

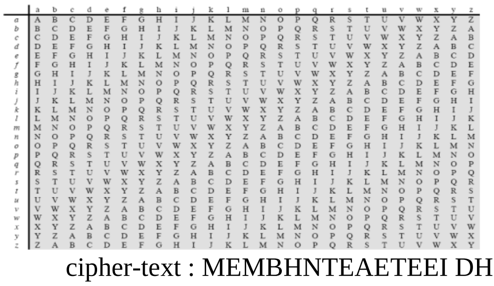
- The playfair cipher is the great advance over simple monoalphabetic cipher because in monoalphabetic cipher mapping is based on frequency letters whereas in this mapping does not depend upon frequency calculation.
- If the keyword is compromised then the whole communication is fetched by the cryptanalyst.

Preventive Measures :

- The keyword must be chosen such that the cryptanalyst can not easily guess.
- The playfair cipher security can also be increased by using 6 X 6 matrix instead of 5 X 5 matrix. In this matrix can be filled by total of 26 alphabetic characters and 10 numbers from 0 to 9.

(4) Polyalphabetic Cipher :

The improvement on the simple Monoalaphabtic technique is to use different monoalphabetic substitutions. This approach is known as Polyalphabetic Substitution 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

Figure – 2 Vignere Table

The best known Polyalphabetic Cipher is **Vignere Cipher**. This method is based on the use of vignere tableau as shown in the figure above. The encryption can be done as follows : Given a key letter x and a plain-text letter y, the cipher-text letter is at the intersection of the row labeled x and the column labeled y.

Example:
if the keyword is DECEPTIVE then the plain-text message “wearediscoveredsaveyourself” is encrypted as “ZICVTW QNGRZGVTWAVZHCQYGLMGJ”.

Analysis :

- The strength of this cipher is that there are multiple cipher-text letter for each plain-text letter, one for each unique letter of the keyword. So, the single letter frequency is obscured.
- The problem with this method is the use repetition of key letters for the encryption process. That is if the cryptanalyst will be able to determine the keyword length then using trial and error will enable him/her to decrypt the cipher-text successfully.

Preventive Measures :

- The keyword length must be as long as the plain-text message such that the cryptanalyst will not be able to determine the exact keyword length. This concept is popularly known as “One-Time Pad”.

4. Transposition Techniques :

A very different kind of mapping is achieved by performing some sort of permutation on the plain-text letters. This technique is referred to as Transposition Cipher. The various Substitution Techniques are as follows :

- Rail Fence
- Row Transposition Cipher
- Rotor Machines

(1) Rail Fence :

In this technique, the plain-text letters are written down as a sequence of diagonals and then read off as a sequence of rows. Suppose for the following example rail fence depth is 2.

Example :
plain-text : meet me behind the lab

cipher-text : MEMBHNTEAETEEI DHLB

Analysis :

- If the depth value is small then the cryptanalyst can decrypt the given cipher-text and retrieve the plain-text message very easily.

Preventive Measures :

- The depth value to be chosen should be very big so that the cryptanalysis is difficult.

(2) Row Transposition Cipher :

In Row Transposition Cipher, the letters of message are written out in rows over a specified number of columns and the columns are reordered according to some key before reading off the rows.

Example :

Key :	4	3	1	2	5	6	7
P.T. :	m	e	e	t	m	e	B
	e	h	i	n	d	t	H
	e	g	a	r	d	e	N

C.T.: EIATNREHGMEEMDDE
TEBHH

Analysis :

- The security of this system basically depends on the key value so if the key is compromised then the cryptanalyst can easily retrieve the plain-text message.

Preventive Measures :

- The security can be increased by performing more than one stage of transposition. The resulting cipher-text will be more complex permutation which is impossible to break.

5. Conclusion :

This paper clearly discusses the working of conventional cryptosystem and also focuses on the various conventional encryption techniques with their analysis and Preventive Measures . These techniques can be used to provide the security of the sensitive information. But each and every technique has its own lacking point so we can’t ignore the possibility of the cryptanalysis totally.

6. References :

[1] Cryptography and Network Security,
Principles and Practices by William Stallings.

[2] Cryptography : A primer by Konheim