Comparing Classical Encryption With Modern Techniques

Mohit Kumar[1*], Reena Mishra[2], Rakesh Kumar Pandey[3] and Poonam Singh[4]

ABSTRACT

This document reviews some of the classical encryption and modern techniques which are widely used to solve the problem in open networked systems, where information is being received and misused by adversaries by means of facilitating attacks at various levels in the communication. In this paper we propose building the basics of classical encryption and modern techniques and atleast section of paper comparison has been done between each of them.

***Keywords* :** *Network Security, Cipher text, Decryption, Encryption, Secret Key, Substitution, Transposition, Modern Encryption.*

I. INTRODUCTION

IN an open networked systems, information is being received and misused by adversaries by means of facilitating attacks at various levels in the communication [1].Data encryption is sought to be the most effective means to counteract the attacks [2].There are two classes of encryption in use, which are referred to as i) Symmetric-key encryption using secret keys and ii) Asymmetric-key encryption using public and private keys. Public-key algorithms are slow, whereas Symmetric-key algorithms generally run 1000 times faster [3]. Symmetric-Key cryptography has been - and - still is - extensively used to solve the traditional problem of communication over an insecure channel [4].In open network like the internet, data encryption has been widely used to ensure information security. Each type of data has its own inherent characteristics. Therefore, different encryption techniques should be used to protect the confidential data from unauthorized use. For text data, there are many encryption algorithms while the algorithm applicable to text data may not be applicable to image data. There are basically two goals i) To introduce the rudiments of encryption vocabulary and ii)To trace the history of some early approaches to cryptography and to show through this history a common failing of humans to get carried away by the technological and scientific hubris of the moment[5].

II. CLASSICAL ENCRYPTION TECHNIQUES

A. Building Blocks

i. Two building blocks of all classical encryption techniques are substitution and transposition.

ii. Substitution means replacing an element of the plaintext with an element of cipher text.

iii. Transposition means rearranging the order of appearance of the elements of the plaintext.

iv. Transposition is also referred to as permutation.

B. Caesar Cipher

This is the earliest known example of a substitution cipher.

Each character of a message is replaced by a character three position down in the alphabet.

i. Plaintext: are you ready

ii. Cipher text: DUH BRX UHDGB

If we represent each letter of the alphabet by an integer that corresponds to its position in the alphabet, the formula for replacing each character 'p' of the plaintext with a character 'C' of the cipher text can be expressed as

$$C = E(3, p) = (p + 3) \bmod 26$$

A more general version of this cipher that allows for any degree of shift would be expressed by

$$C = E(k, p) = (p + k) \bmod 26$$

The formula for decryption would be

[1*] Mohit Kumar is with the Dept. of Computer Science, Amity University Lucknow, Lucknow, E-mail: mohitandy007@gmail.com.

[2] Reena Mishra is with the Dept. of Computer Science, Amity University Lucknow, Lucknow.

[3] Rakesh Kr. Pandey is with the Dept. of Computer Science, Amity University Lucknow, Lucknow.

[4] Poonam Singh is with the Dept. of Computer Science, Amity University Lucknow.

p = D (k, C) = (C - k) mod 26

In these formulas, 'k' would be the secret key. The symbols 'E' and 'D' represent encryption and decryption.

C. Mono-alphabetic Ciphers

In a mono-alphabetic cipher, our substitution characters are a random permutation of the 26 letters of the alphabet:

i. Plaintext letters: a b c d e f.....

ii. Substitution letters: t h i j a b.....

The key now is the sequence of substitution letters. In other words, the key in this case is the actual random permutation of the alphabet used. Note that there are 26! permutations of the alphabet. That is a number larger than 4 × 10^26.

The All-Fearsome Statistical Attack: If you know the nature of plaintext, any substitution cipher, regardless of the size of the key space, can be broken easily with a statistical attack. When the plaintext is plain English, a simple form of statistical attack consists measuring the frequency distribution for single characters, for pairs of characters, for triples of characters, etc., and comparing those with similar statistics for English. Figure 1 shows the relative frequency of the letters in a sample of English text. Obviously, by comparing this distribution with a histogram for the characters in a piece of cipher text, you may be able to establish the true identities of the cipher text characters.

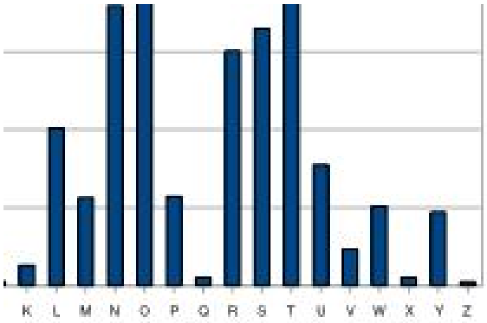


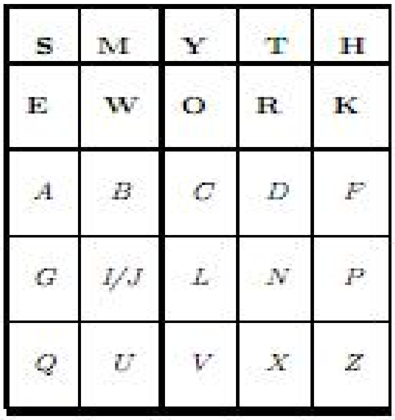
Fig. 1: This Figure is from Lecture 2 of "Computer and Network Security" by Avi Kak. [5]

D. Multiple Character Encryption to Mask Plain Text Structure

One character at a time substitution obviously leaves too much of the plaintext structure in cipher text. So how about destroying some of that structure by mapping multiple characters at a time to cipher text characters? The best known approach that carries out multiple-character substitution is known as Playfair Cipher.

i. Constructing the Matrix for Pair Wise Substitutions in PlayFair Cipher:

In Playfair cipher, you ?rst choose an encryption key. You then enter the letters of the key in the cells of a 5 × 5 matrix in a left to right fashion starting with the ?rst cell at the top-left corner. You ?ll the rest of the cells of the matrix with the remaining letters in alphabetic order. The letters I and J are assigned the same cell. In the following example, the key is "smythework".



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

ii. Substitution Rules for Pairs of Characters in Playfair Cipher: Two plaintext letters that fall in the same row of the 5 × 5 matrix are replaced by letters to the right of each in the row. The "rightness" property is to be interpreted circularly in each row, meaning that the first entry in each row is to the right of the last entry. Therefore, the pair of letters "bf" in plaintext will get replaced by "CA" in cipher text.

a. Two plaintext letters that fall in the same column are replaced by the letters just below them in the column. The "belowness" property is to be considered circular, in the sense that the topmost entry in a column is below the bottommost entry. Therefore, the pair "ol" of plaintext will get replaced by "CV" in cipher text.

b. Otherwise, for each plaintext letter in a pair, replace it with the letter that is in the same row but in the column of the other letter. Consider the pair "gf" of the plaintext. We have 'g' in the fourth row and the first column; and 'f' in the third row and the ?fth column. So we replace 'g' by the letter in the same row as 'g' but in the column that contains 'f'. This given us 'P' as a replacement for 'g'. And we replace 'f' by the letter in the same row as 'f' but in the column that contains 'g'. That gives us 'A' as replacement for 'f'. Therefore, 'gf' gets replaced by 'PA'.

E. Dealing with Duplicate Letters in a Key and Repeating Letters in Plaintext

You must drop any duplicates in a key. Before the substitution rules are applied, you must insert a chosen "?ller" letter (let's say it is 'x') between any repeating letters in the plaintext. So a plaintext word such as "hurray" becomes "hurxray"

F. How Secure Is the Play FAIR?

i. Playfair was thought to be unbreakable for many decades.

ii. It was used as the encryption system by the British Army in World War 1. It was also used by the U.S. Army and other Allied forces in World War 2.

iii. But, as it turned out, Playfair was extremely easy to break.

iv. As expected, the cipher does alter the relative frequencies associated with the individual letters and with diagrams and with trigrams, but not su?ciently.

v. The ?gure shows the single-letter relative frequencies in descending order (and normalized to the relative frequency of the letter 'e') for di?erent ciphers. There is still considerable information left in the distribution for good guesses.

vi. The cryptanalysis of the Playfair cipher is also aided by the fact that a diagram and its reverse will encrypt in a similar fashion. That is, if AB encrypts to XY, then BA will encrypt to YX. So by looking for words that begin and end in reversed diagrams, one can try to compare then with plaintext words that are similar. Example of words that begin and end in reversed diagrams: receiver, departed, repairer, redder, denuded, etc.

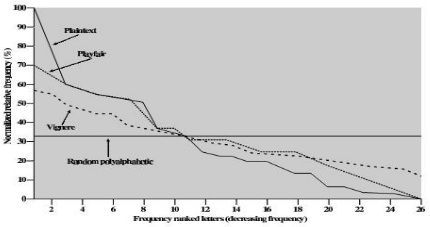


Figure 2.6 Relative Frequency of Occurrence of Letters

This figure is from Chapter 2 (page no.42) of William Stallings: "Cryptography and Network Security", Fourth Edition, Prentice-Hall.[6]

G. Multi-Letter Cipher: The Hill Cipher

The Hill cipher takes a very di?erent (more mathematical) approach to multi-letter substitution:

i. You assign an integer to each letter of the alphabet. For the sake of discussion, let's say that you have assigned the integers 0 through 25 to the letters 'a' through 'z' of the plaintext.

ii. The encryption key, call it K, consists of a 3×3 matrix of integers:

$$\mathbf{K} = \begin{bmatrix} k_{11} & k_{12} & k_{13} \\ k_{21} & k_{22} & k_{23} \\ k_{31} & k_{32} & k_{33} \end{bmatrix}$$

Now we can transform three letters at a time from plaintext, the letters being represented by the numbers p1, p2, and p3, into three cipher text letters c1, c2, and c3 in their numerical representations by

$$\begin{aligned} c_1 &= (k_{11}p_1 + k_{12}p_2 + k_{13}p_3) \; mod \; 26 \\ c_2 &= (k_{21}p_1 + k_{22}p_2 + k_{23}p_3) \; mod \; 26 \\ c_3 &= (k_{31}p_1 + k_{32}p_2 + k_{33}p_3) \; mod \; 26 \end{aligned}$$

The above set of linear equations can be written more compactly in the following vector-matrix form:

$$\vec{\mathbf{C}} = [\mathbf{K}] \, \vec{\mathbf{P}} \; mod \; 26$$

Obviously, the decryption would require the inverse of K matrix.

$$\vec{\mathbf{P}} = \left[\mathbf{K}^{-1}\right] \vec{\mathbf{C}} \; mod \; 26$$

This works because

$$\vec{\mathbf{P}} = \left[\mathbf{K}^{-1}\right] [\mathbf{K}] \, \vec{\mathbf{P}} \; mod \; 26 = \vec{\mathbf{P}}$$

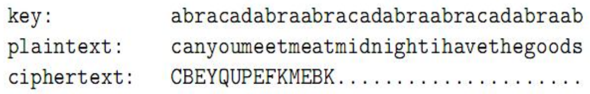
How Secure is the Hill Cipher?

It is extremely secure against cipher text attacks only. That is because the key space can be made extremely large by choosing the matrix elements from a large set of integers (The key space can be made even large by generalizing the technique to larger-sized matrices). But it has zero security when the plaintext-cipher text pairs are known. The key matrix can be calculated easily from a set of known pairs.

H. Poly-alphabetic Cipher: The Vigenere Cipher

In a mono-alphabetic cipher, the same substitution rule is used for every substitution. In a poly-alphabetic cipher, the substitution rule changes continuously from letter to letter according to the elements of the encryption key. Let each letter of the encryption key denote a shifted Caesar cipher, the shift corresponding to the key. This is illustrated with the help of the table on the next page.

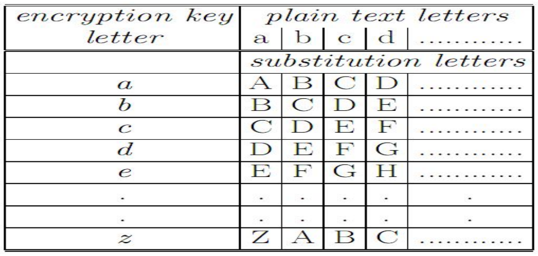
Now a plaintext message may be encrypted as follows key:



```
key:          abracadabraabracadabraabracadabraab
plaintext:    canyoumeetmeatmidnightihavethegoods
ciphertext:   CBEYQUPEFKMEBK.....................
```

The Vigenere cipher is an example of a poly alphabetic cipher.

Since, in general, the encryption key will be shorter than the message to be encrypted, for the Vigenere cipher the key is repeated, as illustrated in the above example where the key is the string "abracadabra".



encryption key letter	plain text letters				
	a	b	c	d	....
	substitution letters				
a	A	B	C	D	....
b	B	C	D	E	....
c	C	D	E	F	....
d	D	E	F	G	....
e	E	F	G	H	....
.	.	.	.	.	.
.	.	.	.	.	.
z	Z	A	B	C	....

How Secure is the Vigenere Cipher?

Since there exist in the output multiple cipher text letters for each plaintext letter, you would expect that the relative frequency distribution would be e?ectively destroyed. But as can be seen in the plots on page 22, a great deal of the input statistical distribution still shows up in the output. (The plot shown for Vigenere cipher is for an encryption key that is 9 letters long.)

Obviously, the longer the encryption key, the greater the masking of the structure of the plaintext. The best possible key is as long as the plaintext message and consists of a purely random permutation of the 26 letters of the alphabet. This would yield the ideal plot shown in the ?gure on page 22 of these notes. The ideal plot is labeled "Random poly alphabetic" in the ?gure.

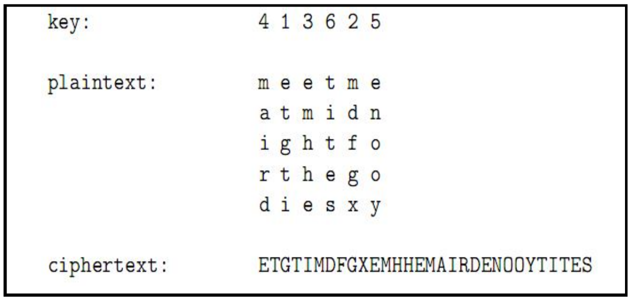
In general, to break the Vigenere cipher, you ?rst try to estimate the length of the encryption key. This length can be estimated by using the logic that plaintext words separated by multiples of the length of the key will get encoded in the same way.

If the estimated length of the key is N, then the cipher consists of N mono alphabetic substitution ciphers and the plaintext letters at positions 1, N, 2N, 3N, etc., will be encoded by the same mono alphabetic cipher. This insight can be useful in the decoding of the mono alphabetic ciphers involved.

I. TRANSPOSITION TECHNIQUES

All of our discussion so far has dealt with substitution ciphers. We have talked about mono alphabetic substitutions, poly alphabetic substitutions, etc. We will now talk about a di?erent notion in classical cryptography; permuting the plaintext.

This is how a pure permutation cipher could work: You write your plaintext message along the rows of a matrix of some size. You generate cipher text by reading along the columns. The order in which you read the columns is determined by the encryption key:



```
key:              4 1 3 6 2 5

plaintext:        m e e t m e
                  a t m i d n
                  i g h t f o
                  r t h e g o
                  d i e s x y


ciphertext:       ETGTIMDFGXEMHHEMAIRDENOOYTITES
```

The cipher can be made more secure by performing multiple rounds of such permutations.

III. MODERN TECHNIQUES

A. S-DES:

Simplified DES has a process of key generation instead of using key as it is for encryption and the key generation process of S-DES generates 2 sub keys after processing the initial 10 bit input, it has 8 bit plaintext input the two sub keys are generated at both transmission and receiving ends the two keys are applied to 2 complex functions respectively, with the inclusion of initial permutation, expansion permutations expansions and s-boxes the security is substantial when compared with the classical techniques, S-des gave some structure and formation to encryption techniques with step to step procedures for both encryption and decryption. [7]

B. DES:

DES enhances the structure of S-DES by increasing the key size from 10-bits to 64-bits out of which its affective length is 56-bits [8].16 rounds are introduced with each round containing XOR, substitutions and permutations for 16 rounds 16 keys are generated each of 48-bits which strengthens the security of this algorithm further, in terms of processing DES is 3 times faster than 3 DES [9].DES takes plain text in 64-bits of block these 64-bits are divided in to 32-bits each the right half of 32-bits goes through the expansion block which increase the bit count from 32 to 48-bits by reusing some bits after expansion block comes XOR operation with sub-key which is also of 48-bits result of this operation is again of 48-bits, these 48-bits now goes in to 8 S-boxes the 48-bits are divided into 8 parts of 6-bits each going in to S-box1 to S-box8, the overall result of S-box substitution is reduced from 48 to 32-bits which is then XOR with the left half of the initial plaintext block to give a 32-bit result which is placed on right and the initial right half of the block is placed at left to get the 64-bit output of its round similarly this output of 1st round becomes input of the 2nd round and same procedure is pursued till the 16th round, after 16th round there is a 32 bit swap and finally the bits are placed in inverse permutation table to get the encrypted message, reverse method is applied to yield the result [7].

IV. AVALANCHE EFFECT

A desirable property of any encryption algorithm is that a small change in either the plain text or the key should produce a significant change in the cipher text [6].Avalanche effect is the phenomenon that describes the effect in the output cipher text if a single or few bits are changed in the plain text, whereas this change that occurs at the output should be sufficient if we want to create a secure algorithm [7].In next section comparison will be made with other techniques on the basis of avalanche effect.

V. COMPARISON

In this section we will make comparison between SDES, DES, Playfair, and Vigenere on the basis of avalanche effect with same key and plaintext.

KEY: **FAUZANCE**

010001100100000101010101010110100100

0001011010010 [7].

PLAINTEXT: **DISASTER**

010001000100100101010011010000010101001101101000100010
0010101010010

CIPHER:

00010000 0100 0001010101110100 0111
111100111011 0011100011011110101 0 [7].

Now we will keep the key same and will introduce 1 character change in plaintext our plaintext will become "DISCSTER" [7].

KEY: **FAUZANCE**

PLAINTEXT: **DISCSTER**

CIPHER:

1 1 0 0 0 1 1 1 1 1 1 1 0 1 1 0
1 1 0 1 1 1 0 0 1 1 1 1 1 1 0 0 0 0 1 0 1 1 0 1
00001101000010110101 1111 [7].

A. SDES

As SDES takes 8bit data and 10bit key we will divide our text in to bits we took F's 8 bits and 2bits of A to constitute our key in DISASTER and DISCSTER the only difference is in the letter A and C so we made the calculations of these two letters rest will be the same [7].

0100011001 key F and 2 bits of A

A 01000001 of "DISASTER"

Result: 01110011

Now change in plaintext from "DISASTER" to "DISCSTER".

C=01000011

Result: 11001110

Avalanche effect: 01000001
11001110

5-bit difference was noted when one character was changed from "A" to "C" [7].

B. DES

Key: **FAUZANCE**

010001100100000101010101010110100100000101001110010000110100010.

Plaintext: **DISASTER**

010001000100100101010011010000010101001101010101000100010101010100010.

Cipher: **DISASTER**

0101011101001010000010011011011101100010101110110011100001 01011.

Cipher: **DISCSTER**

11110110101010001001001001011111101110100001101001110101110111

Avalanche effect: When we encrypted our message using DES and changed the same character "A" to "C" the change avalanche effect we got was spread over 35 bits which is quite significant if we compare it with SDES [7].

C. Playfair

KEY: **FAUZANCE**

PLAINTEXT: **DISASTER**

CIPHER: **ELPNOYDP**

CHANGE PLAINTEXT: **DISCSTER**

CIPHER: **ELOGOYDP**

We compared the two ciphers in bits to calculate the difference and found out that there was a change in 7-bits [7].

D. Vigenere

KEY: **FAUZANCE**
PLAINTEXT: **DISASTER**
CIPHER: **IIMZSGGV**
CHANGE PLAINTEXT: **DISCSTER**
CIPHER: **IIMBSGGV**

We compared the two cipher texts in bits and found the difference to be 2-bits [7].

VI. RESULTS AND DISCUSSION

After comparison the results that were obtained can be well represented in form of table that describes the avalanche effect in the above discussed algorithms [7].

Table 2: Indicating effect of Avalanche in various Algorithms

ENCRYPTION TECHNIQUE	AVALANCHE EFFECT	%
DES	35 bits	54.6
SDES	5 bits	7.8
PLAYFAIR	7 bits	10.9
VIGENERE	2 bits	3.1

Above results clearly shows the comparison of Playfair, Vigenere, SDES and DES in terms of avalanche effect.

VII. CONCLUSIONS

This paper reviews some of the encryption and modern techniques that are demanded in several fields nowadays. These techniques had already been applied in fields related to security in message communication, key management problem remote sensing satellite, video encryptions etc. The encryption algorithm presented above, is a simple, direct mapping algorithm using matrix and arrays. The poly alphabetic cipher text generation provides a good strength to this encryption algorithm, while the combination of poly alphabetic substitution, translation and transposition makes the decryption extremely difficult in absence of a secret key. With the increasing importance of video security more enhanced better methods are required to improve security in a broad way. As such it is quite essential to improve our algorithms performance in future.

ACKNOWLEDGMENT

The authors would like to thank Mr. Fauzan Saeed, Mustafa Rashid and Avi Kak whose papers helped us a lot in making good theory with suitable examples. I would also like to thank Dr. Deepak Arora and Dr. Ganga Ram Mishra for their moral support.

REFERENCES

[1] William Stallings, "Network Security Essentials (Applications and Standards)" Pearson Education, 2004, pp.2-80.

[2] Charles P. Pfleeger, Shari Lawrence Pfleeger. "Security in computing" Pearson Education 2004 -pp. 642-666.

[3] Jose J. Amador, Robert W. Green, "Symmetric-key Block Ciphers for Image and Text Cryptography" , International Journal of imaging System Technology, Vol. 15 - pp. 178-188,2005.

[4] Dragos Trinica, "Sequential and Parallel Cascaded Convolution Encryption with Local Propagation: Toward future Directions in Cryptography", Proceedings of The third International Conference on information Technology-New Generations. (ITNG'06), 0-7695-2497- 4 / 2006, IEEE Computer Society.

[5] Lecture Notes on "Computer and Network Security" by Avi Kak.Pdf http://junicholl.org/Cryptanalysis/Data/EnglishData.php

[6] William Stallings, "Cryptography and Network Security", Fourth Edition, Prentice-Hall -pp.80-81.

[7] Fauzan Saeed 1, Mustafa Rashid 2, "Integrating Classical Encryption with Modern Technique", International Journal of Computer Science and Network Security, VOL. 10 No.5, {May 2010}.

[8] V. Umakanta Sastry 1, N.Ravi Shankar2, and S.Durga Bhavan "A Modified Hill Cipher Involving Interweaving and Iteration" International Journal of Network Security, Vol. 11, No. 1, PP.11 {16, July 2010}.

[9] Results of Comparing Tens of Encryption Algorithms Using Different Settings- Crypto++ Benchmark, Retrieved Oct.1, 2008, (http://www.eskimo.com/ wei-Dai/benchmarks.html).