AN ANALYSIS INTO THE EFFICIENCY OF SYMMETRIC CIPHERS

1Meera Rose Joseph, [2]Kukku George, [3]Mariya Raju,
[1]Assistant Professor, [2,3,4]Graduate Students,
[1]Mathematics Department,,
[1] Nirmala College, Muvattupuzha,Kerala,India

Abstract : Cryptography is about conducting and analysing protocols which prevent the third parties from reading private messages. In this paper we analyse different symmetric ciphers and make a comparison study and find out most efficient ciphers among them. The criteria used for comparison is the degree of security and difficulty in the procedure of encryption and decryption. By analysing the degree of security and difficulty in the procedure in cryptography we arrive at a conclusion by finding out the most efficient cipher among the once consider.

IndexTerms - **Cryptography, protocols, ciphers, symmetric ciphers, encryption, decryption**

I INTRODUCTION

Cryptography is the practice and study of technique for secure communication. With the advent of modern techniques, method in cryptography become more and more complex and has led to the invention of modern ciphers. Cipher means a secret writing for encryption and decryption.At present there is a misconception that any cipher is not permanent but it is a wrong notion. One time pad cipher is a cipher which could not be broken. Since continous efforts are made to break the cipher it could be sometimes broken in the future.

Here we are testing the efficiency of 6 different symmetric ciphers

1. Caesar cipher
2. Playfair cipher
3. Hill cipher
4. Ascii cipher
5. Binary cipher
6. One time pad cipher

II PRELIMINARIES

Plain text: The message that needs to be communicated privately.it could be a letter, number, words etc.
Cipher text: The coded text.We are blurred with the idea of codes. If we are considering a village, houses in that village can be represented by some codes and this code is different from cryptographic codes. In cryptography codes means replacement of linguistic groups (such as groups of words or phrases) with numbers,designated words or phrases.
Encryption: Process of converting plain text into cipher text.
Decryption: Transforming coded text into original message.
Cryptography: Combination of encryption and decryption.
Key: A secret parameter for encryption and decryption algorithm.
Transposition Cipher: A cipher in which encryption is done by rearranging the order of letters in the message.
Substitution cipher: Here,coding is done by replacing letter or a group of letters by other letters.

III CIPHERS AND GOALS

III.I (a) CIPHERS AND SECURE COMMUNICATION

Ciphers are generally classified into:
1. Symmetric cipher
2. Asymmetric cipher

1. .Asymmetric cipher

In cryptography, an asymmetric cipher uses a pair of different keys for encryption and decryption. These keys are related mathematically. The most common asymmetric key algorithm are in such a way that one key cannot be deduced with the knowledge of the other.

2. .Symmetric cipher

It is also known as single key cipher or traditional cipher. These are the oldest and most used cryptographic ciphers. Here the key that deciphers is same as the key that enciphers the plain text. It is further divided into:

2.1 Stream cipher

In a stream cipher, each plain text digit is encrypted one at a time with corresponding digit of the cipher text key stream

2.2 Block cipher

A block cipher is a method of encrypting text in which a cryptographic key and algorithm is applied to a block of data as a group than to one at a time.

III.I(b) GOALS OF CRYPYOGRAPHY

- Confidentiality: Hiding information from unauthorised access.
- Integrity: Preventing information from being modified by unauthorised persons.
- Availability: Should be easily available to the authorised user.

IV. WAYS OF ENCRYPTING

IV.I (a) TRANSPOSITION CIPHER

Spartans,are the great warriors of the Greek states. They used a transposition cipher device called a Skytale. This consists of a taperedwooden staff around which a strip of parchment was spirally wrapped, layer upon layer. The secret message was written on the parchment lengthwise down the staff. Then the parchment was unwrapped and sent. By themselves, the letters on the parchment were disconnected and made no sense until rewrapped around a staff of equal proportion, at which time the letters would realign to once again making sense.

IV.I (b) SUBSTITUTION CIPHER

MONOALPHABETIC AND POLYALPHABETIC SUBSTITUTION CIPHER

Multiple occurrence of the plain text character is replaced by same cipher text character in the encryption method of monoalphabetic substitution cipher. If the multiple occurrence are replaced by different cipher texts characters, it is called polyalphabetic substitution cipher.

An example of a polyalphabetic cipher, the first in history,is that invented by LEON BATTISTA ALBERTI. ALBERTI conceived of a disk with plain text letters and numbers on the outer ring and cipher text symbols on an inner movable circle. ALBERTI divided his ring and corresponding circle into twenty-four equal segments, called cells, each containing symbol. We have altered his original presentation since he had cipher text in lower case and plaintext in upper case, the reverse of what we have as a convention.

In figure the plaintext letter z is enciphered as V, so in this setting (one of the twenty -six possible cipher alphabets) the plaintext zebra for instance would be enciphered as VZLYD. However, there is nothing new at this juncture that is any different from say, the CAESAR CIPHER with the cipher alphabet having the letter C below the z. After a random number of plaintext words have been enciphered, usually three or four, ALBERTI would move the inner disk to new setting. Hence he would now be using a new cipher alphabet.Suppose that he moved the inner circle so that z sits over K . Then zebra would be enciphered as KADTR, a new cipher text for the same plaintext as above, since we have a new cipher alphabet. In fact with his cipher disk, ALBERTI invented the first polyalphabetic cipher in history.However he did even more.

ALBERTI had twenty-letters as depicted. This excludes the letters h, k and y deemed to be unnecessary, and since j, u and w were not part of his alphabet, this left twenty letters.The inner circle consists of the twenty- four letters of the Latin alphabet , put in the cells at random, including &. The disk also included the numbers 1 through 4 in the outer line of his original disk

V. TESTING THE EFFICIENCY OF DIFFERENT CIPHERS

V.I (a) CAESER CIPHER

What is being described here is a simple substitution cipher used by Julius Caesar.Caesar’s substitution cipher is even easier to use. With Caesar’s cipher there is merely a shift to the right of three places of each plaintext letter to achieve the cipher text letters. An example of a cryptogram made with the Caesar cipher is: brutus becomes EUXWXV. Also, this simple type of substitution cipher is called a shift cipher. Moreover, the mechanism for enciphering in the Caesar cipher is a shift to the right of three letters. So the value 3 is an example of a key, which we may regard, in general, as a shared secret between the sender and the recipient, which unlocks the cipher. So 3, in this case, is the enciphering key. Since shifting three units left unlocks the cipher, then 3 is also the deciphering key. This is an example of a symmetric-key cryptosystem.

If Caesar had anything confidential to say, he used to write it in a coded form, that is by changing the order of the letters of the alphabet.

E.g.: **‘hello’**

Encryption algorithm: $C \equiv E(P,3) \equiv (P+3) \pmod{26}$

‘HELLO’

** H→7

Cipher: (7+3)%26= 10%26=10

K’

Cipher text: KHOOR

Decryption Algorithm: P ≡ D (C,3) ≡ (C-3) (mod 26)
'KHOOR'
** K→10
Plain : (10-3)%26= 7%26 =7
'H'
** H→7
Plain: (7-3)%26=4%26=4
'E'
** O→14
Plain: 11%26=11
'L'
** R→17
14%26 =14
'O'
Therefore**, Plain text:** Hello

V.I (b) PLAYFAIR CIPHER

Play fair cipher was invented in 1854 by Charles Wheatstone, but bears the name of Lord Playfair who promoted the use of the cipher.

The Play fair cipher uses a 5*5 table containing a keyword. Memorization of the keyword and four simple rules that required to create the 5*5 table and use of cipher. To generate the table, one would first fill in the spaces in the table with the letters of the keyword (dropping any duplicate letters). Then fill the remaining spaces with the rest of the letters of the alphabet in order (usually omitting 'J' or 'Q' to reduce the alphabet to fit; other version put both 'I' and 'J' in the same space). The key can be written in the top of the table, from left to right. To encrypt a plain text , one would break it into diagrams (groups of two letters). Then apply the following rules in order, to each pair of letters in the plain text.

1. If both the letters are the same (or only one letter is left), add an 'X' after the first letter. Encrypt the new pair and continue.
2. If the letters appear on the same row of your table, replace them with the letters to their immediate right respectively.
3. If the letters appear on the same column of your table, replace them with the letters immediately below respectively.
4. If the letters are not on the same row or column, replace them with the letters on the same row respectively but at the other pair of corners of the rectangle defined by the original pair. The order is important; the first letter of the encrypted pair is one that lies on the same row as the first letter of the plain text.

To decrypt, use the inverse of the last three rules.

Consider the example, here 'MONARCHY' as the keyword and 'BALLOON' as the plain text. The 5*5 table is given below.

Plain text in diagram format 'BA LX LO ON'

Corresponding cipher text is 'IB SU PM NA 'or 'JB SU PM NA '

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

V.I (c) HILL CIPHER

The method was devised in 1929 by Lester Hill, an assistant professor of Mathematics at Hunter College. Briefly, Hill's approach is to divide the plain text into blocks of 'n' letters and to encrypt block by block using a system of 'n' linear congruence in 'n' variables. In the simplest form, when 'n=2', the procedure takes two successive letters and transform their numerical equivalents P_1, P_2 into a block C_1 C_2 of cipher text numbers by the pair of congruence $C_1 \equiv aP_1+bP2 (\text{mod } 26)$ and $C_2 \equiv cP_1+dP_2 (\text{mod } 26)$, the four coefficients a,b,c,d must be selected so that gcd(ad-bc,26)=1.

Consider the example:

$C_1 \equiv 4P_1+11P_2 (\text{mod } 26)$ and $C_2 \equiv 3P_1+8P_2 (\text{mod } 26)$
Plain text: OX
In encryption, cipher text: XS
For decryption, solving the two congruence relations we get:
$P_1 \equiv -8C_1+11C_2$ (mod 26) and $P_2 \equiv 3C_1-4C_2$ (mod 26)
Then we get the plain text: OX.

V.I (d) ASCII CIPHRER

Here encryption and decryption are done by computer programming.

Ascii codefor each letter is given as follows **a=097 , b=098 ,…….. , z=122, A=065, B=066,….., Z=090 .**
For example ,cat can be encrypted as 099097116

V.I (e) BINARY CIPHER

Here also encryption and decryption are done by computer programming.
Binary code for each letter is given as follows **a=01100001, b=01100010,…,z=01111010, A=01000001,B=01000010,……, Z=01011010**
For example,cat can be encrypted as 011000110110000101110100

V.I (f) ONE TIME PAD CIPHER

One time pad cipher is also known as Perfect cipher. Here pain text is combined with a random key. It cannot be cracked but requires the use of a one time preshared key of same size as the message being sent. Here each bit of character of the plain text is encrypted by combining it with the corresponding bit or character from the pad using modular addition. Each new message requires a new key of the same length as the new message. Such a scheme is known as One-time pad and is considered as unbreakeable.
Eg: Let the plain text be 'HELLO'
Key: XMCKL
Plain text Value: 7 14 11 11 14
Key stream: 23 12 2 10 11
Cipher text Value:4 16 13 21 25 which corresponds to 'EQNVZ'
The security of OTP is due to the randomness of the key. If the stream of characters that constitute the key is truly random. Then the stream of characters that constitute the cipher text will be truly random. Thus there are no patterns or regularities that a cryptanalyst can use to attack the cipher text.

VI. APPLICATIONS

- ATM Machines :
  According to current standard, clear pin which is entered into ATM Should be converted to encrypted format before sending it over network. Every ATM has encrypted PIN Pads which encrypt the PIN on ATM. Keys for this are manually added or come from the system to which ATMs are connected.
- Whatsapp Messages:
  The Whatsapp messages are encrypted in such a way that the third party couldnot receive it.
- Fingerprint scanner system:
  In this system cryptography is used where our fingerprints are scanned , analysed and then stored in a coded form. This is known as enrolment. Second stage is known as verification .Anyone who wants to acess ha to put their fingers on the scanner, the scanner takes it,checks it against the stored data and identifies the person.
- Cryptography is also used for safe and secure communication in several fields like defense,online transferring etc.

VII. CONCLUSION

We have discussed about various ciphers and their efficiencies. Of the ciphers we have considered,Ceaser cipher is the least secure one, because of its simplicity and the ease with which an encrypted text can be broken. Playfair cipher was better when compared with the Caeser cipher. But with the knowledge of the plane text and cipher text, key is relatively straight forward. In playfair cipher the could be found easily. Then we came across the Hill cipher. It is secure when compared with Caeser and playfair cipher. Hill cipher also can be broken if we could find numbers a,b,c,d such that g.c.d (ad-bc)=1. But it is difficult to find as compared to Caeser and playfair cipher. In ASCII and Binary cipher, enciphering and deciphering is done by computer programming. Therefore, it cannot be broken as easily as compared to playfair and Hill cipher. But there is no compromise with the security of one time pad cipher. Hence one time pad cipher is the best among thses ciphers due to random selection of keys.

VIII.REFERENCE

[1] Chapman and Hall /CRC Introduction to cryptography – 2nd edition Kenneth H.Rosen

[2] International Journal of Scientific & Engineering Research on efficiency of ciphers Volume 8, Issue 7, July-2017 1303 ISSN 2229-5518 by Alka Benny and Mesly Mathews

[3] B. Schnieir, Applied Cryptography John Wiley

[4] D.R Stinson, Cryptography- theory and practice, CRS press