An Analysis into the Efficiency of Ciphers

*Alka Benny, **Mesly Mathews

Abstract— Cryptography is the branch of science which deals wth secure communication using codes. It is a part of cryptology whch includes both cryptography and cryptanalysis where we analyse the degree of security of a particular coded text (cipher). In this paper, we analyse different ciphers and make a comparison study on them and find out the most efficient cipher discovered till now. The criterion used for comparison is the degree of security and the ease in the process of key generation. We also consider different attacks to which each cipher is prone to and thus, be able to analyse each cipher from the corresponding perspective. By analyzing the advantages and disadvantages, we arrive at a concusion by finding out the most efficient cipher among the ones considered.

Index Terms— Ciphers, Cryptography Cryptanalysis, key, Attacks, Cryptology, Plain text.

1 INTRODUCTION

Cryptography, the practise and study of techniques for secure communications, is about conducting and analysing protocols which prevent the third parties from reading private messages. Applications of cryptography involve ATMs, Computer passwords and e-commerce.
The cryptography literature often uses "Alice (A)" for the sender and "Bob (B) for the intended recipient and eve for the advisory. With the development of technology, the methods used to carry out cryptography have become increasingly complex and applications more widespread.
The earliest known use of cryptography is some carved cipher text on stone in Egypt. As time passed, various classical ciphers came into existence. Some of them are the Caesar cipher, Scytale cipher, e.t.c. With the advent of modern techniques, a method in cryptology has become more complex and hassled to the development of modern ciphers. This gave rise to the symmetric cryptography and Public key Cryptography.
Cryptology is the branch of science which deals with cryptography and cryptanalysis. The goal of cryptanalysis is to find some weakness or loophole in a cryptographic scheme. There is a misconception that every method in cryptography can be broken. One time pad is a cipher which is unbreakable but it is generally not used because of the complexity involved in this method.
The most important feature of cryptography is that nothing is permanent here. We cannot predict the consistency and credibility of any cipher. Continuous efforts are being made to break the different encryption methods and the time they take to decrypt the code depends on the complexity in the method they use for encryption.
Cryptography contains communications that are generality designed to keep secrets from the third party. However the public growth demands the use of cryptography in the need of law enforcement and national security. As a result, Cryptography plays a major role in all secure communications and transactions.
In this project, we analyse the various ciphers which has been used and is being used and find out the most efficient among them based on their complexity and easiness in keygeneration.

2 PRELIMINARIES

Plain Text: The text or the message that needs to be communicated privately
Cipher Text: The coded text.
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 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.

- *Alka Benny,*
  Substitute Lecturer,
  St. Teresa's (Autonomous) College, Ernakulam,
  Pincode: 682011, Kerala, S.India.
  Email-ID: alkabenny30@gmail.com
- *Mesly Mathews,*
  Graduate Student,
  St. Teresa's (Autonomous) College, Ernakulam,
  Pincode: 682011, Kerala, S.India.
  Email-ID: meslymathews@gmail.com

Goals of cryptography

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

Cryptanalysis: Study of principles and methods of deciphering cipher text without knowing the key.

3 Sections

3.1 Ciphers and Secure Communications

Ciphers are generally classified into:

1. Symmetric cipher
2. Asymmetric cipher
3. Stream Cipher
4. Block cipher

Symmetric cipher is also known as conventional cipher.

Basic Components of symmetric ciphers:

i. Plain text: Original message.
ii. Encryption algorithm: Takes the plain text as the input and using the key produces the cipher text.
iii. Decryption algorithm: Takes cipher text as the input and using the key produces the plain text.
iv. Secret key: Information which is kept secret and which is known only to the sender and the receiver.

Monoalphabetic and Polyalphabetic Substitution ciphers:

Multiple occurrence of the plain text character is replaced by same cipher txt character in the encryption method of monoalphabetic substitution ciphers.

If the multiple occurrences are replaced by different cipher text characters, it is called polyalphabetic substitution ciphers.

Cryptographic systems or ciphers can generally be classified into symmetric, asymmetric, stream and block ciphers. Symmetric ciphers are also known as conventional ciphers, single key ciphers or traditional ciphers. These are the oldest and most used cryptographic ciphers. In a symmetric cipher, the key that deciphers is same as the key that enciphers the plain text. The most widely used symmetric ciphers are AES and DES.

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. This is known as Public Key Cryptography since one pair of key can be published without affecting the message security.

A stream cipher is a symmetric key cipher in which the plain text digits are combined with a pseudorandom cipher key stream. In a stream cipher, each plain text digit is encrypted one at a time with corresponding digit of the cipher text key stream. In practise, a digit is called 0 bit and the combining operation an XOR.

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. One widespread implementation of such ciphers named a Fiestel network is notably implemented in DES cipher. Many other realisations of block cipher include the AES.

3.1.1 Language Redundancy and Cryptanalysis:

The letters are generally not equally commonly used. In English 'E ' is by far the most common letter followed by T, R, N, I, D, A and S. Other letters like J, Z, K, Q and X are fairly rare.

Cryptanalysis used for frequency of ingle letter statistic will not be used for polyalphabetic substitution cipher. Sometimes, it is difficult to analyse a ciphertext based only on information about the frequency of a single letter.

3.2 Ciphers- An Introduction

3.2.1 Caesar Cipher:

Caesar, if he had anything confidential to say, used to write it in a coded form, i.e. 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

'H'

** H→7

Plain: (7-3)%26=4%26=4

'E'

** O→14

Plain: 11%26

'L'

** R→17

14%26

'O'

Therefore**, Plain text:** Hello

Caesar cipher is a special case of additive cipher where the shift k can be determined as we wish. Here the encryption algorithm is

C ≡ E (P,k) ≡ (P+k) (mod 26)

And decryption algorithm is

P ≡ D (C,3) ≡ (C-3) (mod 26)

Additive cipher is prone to mainly two types of attacks:

1. Brute Force Attack:
   In brute force attack, they try by shifting letters in all possible ways and hence, in all 26 possibilities, they may succeed in breaking the code. Therefore, Additive cipher is not much reliable.
2. Statistical attack:

   Addiive ciphers are subject to statistical attack. The adversary can use the frequency of occurrence of characters for a particular language.

3.2.2 Playfair Cipher

Since Caesar cipher was found to be insecure, a large number of efforts were made for the development of a cipher which provides more security in communication. One such effort was the encryption of multiple letters.The Playfair cipher is an example. This cipher was developed by Charles Wheatstone in 1854 but was named after his friend Baron Playfair.

Consider the following example:Here, we take MONARCHY as the keyword. Consider a 5*5 matrix constructed by filling the letters of the keyword from left to right and from top to bottom and then filling the remaining column by letters in alphabetic order.Here i & j are considered as a single letter.Consider the plain text BALLOON.When two letters are repeated, filler 'x' is used as shown below:

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

BA LX LO ON

Here X is the filler.

Method of encryption

To encrypt a message, first break the given plain text into diagraphs. So here our plain text becomes

BA LX LO ON

Here x is the filler.

If the letters (each digraph) appear on the same row, replace them by letters to their immediate right respectively.

If the letters appear on the same column, replace them with letters to their immediate below.

If the letters are not in the same row or column replace them with letters on the same row respectively but at the other pair of corners of the rectangle defined by the original pair.

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

BA LX LO ON

IB SU PM NA

JB SU PM NA

Cipher text: **IBSUPMNA or JBSUPMNA**

Like most classical ciphers, the Playfair cipher can easily be cracked if there is enough text. Obtaining the keys relatively straightforward if both plain text and cipher text are known. Identifying nearly all the reversed di graphs in the cipher text and matching the pattern to the test of known plain text. Words containing the pattern are an easy way to generate possible plain text which further leads to the construction of key.

Decryption:

Here, the cipher text is broken into digraphs.

So, 'JBSUPMNA' becomes

JB SU PM NA

If the letters appear on the same row replace them with letters to their immediate left.

If the letters appear on the same column replace them with letters just above them.

JB SU PM NA

BA LX LO ON

Cryptanalysis:

Obtaining the key is relatively straightforward if both the plain text and cipher text are known; however, we want to find the key without knowing the plain text. It should be recognised that guessing some of the plain text and using them to reconstruct the key square I the easiest way to crack this cipher.

3.2.3 Hill Cipher

This is a polyalphabetic substitution cipher. It is also a block cipher.

When we consider m as the block size,

$$K = \begin{pmatrix} K11\ K12\ K13\ldots\ldots\ldots\ldots K1M \\ K21\ K22\ K23\ldots\ldots\ldots\ldots\ldots K2M \\ \vdots \\ KM1\ \ KM2\ KM3\ \ldots\ldots\ \ KMN \end{pmatrix}$$

$$P = \begin{pmatrix} P1 \\ P2 \\ \vdots \\ PM \end{pmatrix}$$

C1= K11P1+K12P2+…… K1MPM

C2=K21P1+K22P2+……..K2MPM

⋮

CM=KM1P1+KM2P2+……KNMPM

Eg: encrypt 'pay more money' using e

$$K = \begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix}$$

Here m = 3

Pay

$$P = \begin{pmatrix} 15 \\ 0 \\ 4 \end{pmatrix}$$

Encryption C = kp (mod 26)

$$\begin{pmatrix} C1 \\ C2 \\ C3 \end{pmatrix} = \begin{pmatrix} 17 & 7 & 5 & 15 \\ 21 & 18 & 21 & 0 \\ 2 & 2 & 19 & 24 \end{pmatrix} (\text{mod}26) = \begin{pmatrix} 375 \\ 819 \\ 486 \end{pmatrix} \text{mod}26$$

$$= \begin{pmatrix} 11 \\ 13 \\ 8 \end{pmatrix} \rightarrow \begin{pmatrix} L \\ N \\ S \end{pmatrix}$$

Similarly,

'Mor'→ $\begin{pmatrix} 12 \\ 14 \\ 17 \end{pmatrix} \rightarrow \begin{pmatrix} H \\ D \\ L \end{pmatrix}$ emo→ $\begin{pmatrix} 4 \rightarrow \\ 12 \\ 14 \end{pmatrix} \begin{pmatrix} E \\ W \\ M \end{pmatrix}$ ney→ $\begin{pmatrix} 13 \rightarrow \\ 04 \\ 24 \end{pmatrix} \begin{pmatrix} T \\ R \\ W \end{pmatrix}$

Cipher text: LNS HDL EWM TRW

Decryption

$P=k^{-n}C\%26$, n=1

Similarly the other block can be decrypted

Cryptanalysis attacker

m*m

to decrypt the message passing through the channel the attacker have to know k . To know the k ,the attacker have to try 0 to 25 values for each element in the 3*3 matrix.

Brute force attack is extremely difficult on hill cipher because the key is an m*m matrix each entry in the matrix has one of the 26 values

Statistical attack

Hill cipher does not preserve the statistic of the plain text attackers can't run frequency analysis on single letters, digraphs and trigraphs a frequency analysis of the word of size m might work but this is very rare, that a plain text has many stings of size m that are the same.

Known plain text attack (KPA)

Hill cipher can easily be broken with KPA . KPA is an attack model of cryptanalysis where the attacker has samples of both the plain text and the encrypted text.

3.2.4 Autokey cipher

In auto key cipher the key is a string of sub keys where each sub key is used to encrypt the corresponding character in the

plain text . The first sub key is a predetermined value secretly agreed upon by the sender and the receiver

The second sub key is the value of the first plain text character (0 and 25).The third sub key is the value of the second plain text.

Encryption algorithm: (p + k)(mod 26)

Eg: k1 = 12 (initial key) plain text, "attack is today"

Plain text: a t t a c k I s t o d a y
Plain text 0 19 19 0 2 10 8 18 19 14 3 0 24
Values:
Key stream: 12 0 19 19 0 2 10 8 18 19 14 3 0 24
Cipher text
Value : 12 19 12 19 2 12 18 0 11 7 17 3 24
M T M T C M S A L H R D Y
Key stream: 12 0 19 19 0 2 10 8 18 19 14 3 0
Plain text : 0 19 19 0 2 10 8 18 19 14 30 24

Cryptanalysis:

It definitely hides the single letter frequency statistics of plaintext .however it is still vulnerable as brute force attack as the additive cipher. The first subkey can only be one of the 25 values. We need polyalphabetic cipher that only hides the characteristic of the language and also should have large key domains .

3.2.5 One time pad

One time pad , also known as vernam cipher or the perfect cipher is a cryptoalgorithm where pain text is combined with a random key. It cannot be cracked but requires the use of a one timepreshared key of same size as the message being sent.

In this technique a plain text is paired with a random secret key. Then each bt 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

Keystream: 23 12 2 10 11

Cipher text

Value:4 16 13 21 25

E Q N V Z

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.

But this cipher is generally not used because of practical problems. Generation and distribution of keys is difficult. So the thrive for a better cipher continued.

3.3 DES and AES:

3.3.1 Data Encryption Standard:

Data Encryption Standard (DES) is a symmetric cryptosystem. Physically a 16 round Fiestal cipher, DES was originally designed for implementation in hardware.

DES has been used worldwide for over 20 years and because of the fact that it is a defined standard, any system implementing DES can communicate with one using it.

DES is mainly used in banks and business around the globe and also in the news agencies and to protect the password file in UNIX operating system in CRYPT.

Strength of DES:

Since the adoption as a federal standard, there has been conscience over the level of security offered by DES. These conscience falls into 2 categories:

1. Key size
2. Nature of algorithm

Key size- the use of 56 bit keys

With a key size of 56 bits there are around 2^{56} bit possible cases, which is approximately $7.2*10^{8}*10^{8}$ keys. Then a brute force attack appears impractical assuming that i=on an average half of the key space has to be searched a single machine performing 1 DES encryption could take ,more than a 1000 years to break the cipher.

However, the assumption of one encryption per user was overly conservative. As far as back in 1977, Diffy and Hallman postulated that the technology existed to build a parallel machine with one million encryption devices each of which could perform one encryption per user. This would bring the search time down to 10 hours.

DES was finally proved insecure in 1996 when the EFF announced that it had broken a DES encryption using a special purpose DES cracker machine that was build for less than 2.5

lakh dollars. The attack took less than 3 days. The EFF has published a detailed description of the machine following others to bring their own cracker and of course hardware prices will drop as the speed increases making DES virtually worthless. Fortunately there are a lot of alternatives to DES, the most of which are AES, Triple DES, and e.t.c.

Another conscience is the probability that crypt analysis is possible by exploiting the characteristics of DES algorithm. The focus of conscience has been of the 8 substitution boxes that are used in each round. Because the designs criteria for the boxes were not made publicthere are a suspicion that the boxes were constructed in such a way that cryptanalysis is possible for an attacker who knows the weaknesses in s-boxes. Over the years a number of regularities and unexpected behaviour of the s-boxes have been discovered. Despite this no one has succeeded in discovering the supposed fatal weaknesses to s- boxes.

3.3.2 Advanced Encryption Standard:

Advanced Encryption Standard is a symmetric encryption standard. It is also a block cipher. It encrypts data by breaking plain text into blocks of size 128 bits. It has three versions- One in which the plain text I broken into texts of size 128 bits, 192 bits and 256 bits. I is a non-Fiestal cipher.

History of AES:

NIST in 1998 looked for a replacement for DES and invited for proposals for new encryption standard which they called the Advanced Encryption Standard. Out of 21 proposals 16 were shortlisted in the first AES conference in August 1998.

In the second AES Candidate conference in 1999, 5 were shortlisted and they are MARS, RS6, Serpent, Two Fish, Rijndael.In the third AES candidate conference, Rijndael encryption system was selected as a advanced encryption standard in a meeting in October 2000.

This cryptosystem was developed by 2 Belgium cryptographers, Dr. Joan Darmin and Dr. Vincent Rymen. It is published as a Federal standard in November 2001 as FIPS 197.

AES PARAMETERS:

Block Size	128 bits	128 bits	128 bits
Key Size	128 bits	192 bits	256 bits
No: of Rounds	10	12	14

Security of AES

AES was designed after DES.Most of the known attacks on DES was already tested on AES. None of them has broken the security of AES so far.

Brute force attack

AES is definitely more secure than DES due to largesized key. Let us compare DES with 56 bit key and AES wth 128 bit key.For DES we need 2^56 tests to find out the key while for AES the no. of tests required is 2^128 and therefore the brute force attack on AES is considered impractical.

3.4 CRYPTOLOGY

As cryptology is the science and art of creating secret codes cryptanalysis is the science and art of breaking these ciphers. In addition to studying cryptographic techniques, we also need to study cryptanalysis techniques. This is needed to break other people's code but to learn how vulnerable our cryptosystem is.

3.4.1 Cipher text Only Attack

In cipher text only attack (COA), attacker has access only to cipher text. This is the most probable one because attacker needs only the cipher text. To thwart decryption of thge message of an advisory, a cipher must be very resisting to this type of attack.

3.4.1: Various methods of COA

Brute force attack (Exhaustive key search method):

Here, the attacker tries to use all possible keys. Using the intercepted cipher, the attacker decrypts the cipher text with every possible key until the plain text makes sense. This was difficult in the past but it has become pretty easy now with the development of technology.

Statistical Attack: Here, the cryptanalyst finds the most frequently used character in the cipher text and after finding a few pairs he can find the key and decrypt the message.

Pattern Attack: Some ciphers may hide characteristics of the language but may create some pattern in the cipher text. Using this pattern, a cryptanalyst can break the cipher.

3.4.2 Known Plain Text Attack (KPA)

Here, the attacker has access to plain text – cipher text pairs in addition to the intercepted cipher text that he wants to break.

3.4.3 Chosen Plain Text Attack

This is an attack model for cryptanalysis which presumes that the attacker can obtain the cipher text for arbitrary plain text. The goal of the attack is to gain information which reduces the security of the encryption scheme.

3.4.4 Chosen Cipher Text Attack

Here, the cryptanalyst gather information by obtaining decryption of chose cipher texts. From these pieces of information, the advisory can attempt to recover the hidden secret key

used for encryption.

3.5 Public Key Cryptography

There are two types of cryptosystem:

1. Symmetric and
2. Asymmetric

n a symmetric cryptosystem, a single key is used for encryption and decryption.

3.5.1Asymmetric key cryptography

The major application of Asymmetric key cryptography is in the areas of ensuring confidentiality, authentication and key distribution.

Every user in an asymmetric cryptosystem has to generate a pair of keys – a public key and a private key.

Encryption using public key implies decryption using private key and vice-versa.

Authenticity is guaranteed but not confidentiality.

3.5.2 Public key and Private Key

This is a pair of keys that have been selected so that if one is used for encryption the other is used for decryption.

3.5.3 RSA

This is the best known and widely used Public Key Scheme. It is developed by Rivert, Shamir and Adleman in 1977. This is based on exponentiation in a finite field over integers modulo a prime. This scheme uses large integers (1024 bits) and highly secure due to the cost of factorisation of large numbers.

Key Generation

- Select two large primes p and q
- Calculate n=p*q(RSA Modulus)
- Calculate the Euler Totient function φ(n)= (p-1)(q-1)
- Select an integer e such that
  gcd (e, φ(n)) = 1, 1 < e < φ(n)
- Calculate d Such that
  E*d(mod φ(n)0 ≡ 1
- Public Key {e,n}
- Private key {d,n}

Encryption:

Let M be the plain text. Then the encryption algorithm is

$C \equiv M^e \pmod n$

Decryption:

Let C represent the cipher text. Then the decryption algorithm is $M \equiv C^d \pmod n$

The areas of application of Public key cryptography are

1. Confidentiality

User A encrypts the plain text using public key of B. So the cipher key can be decrypted using the private key of B thereby making sure that only B can decrypt the message.

2. Authentication

It acts as a digital signature. If the cipher text can be decrypted using the public key of A, then it is encrypted by the private key of A known only to A. This authenticates the origin of message from A.

3.6 Applications of Cryptography

Cryptography is widely used in different fields where highly secure communications play a very important role. They include withdrawal of cash from ATM, Safe browsing, play fair crosswords, e.t.c.

3.6.1Modern crosswords

The Playfair cipher lends itself to crossword puzzles because the plain text is formed by solving others.

Use of play fair cipher is generally explained as a part of preamble to the crossword. This levels the playing field for those players who have not come across the cipher previously.

3.6.2 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.

3.6.3 Steganography

Steganography is the practise of concealing a file, message, image or video within another file. This was the principle of cryptography and is more secure than other ciphers. The advantage of steganography over cryptography is that the intended message does not attr4act itself as object of scrutiny. Plainly visible encrypted messages no matter how much unbreakable arouse interest and may be incriminating in countries where encryption is illegal. Thus Steganography is concerned with concealing the fact that a message is being sent as well as concealing the contents of the message. This is used in some modern printers including HP and XEROX. These printers add tiny yellow dots to each page. The barely visible dots contain encoded printer serial number and date and time stamps.

CONCLUSION

In this project, we have discussed about various ciphers and various attacks to which they are subjected to. Of the ciphers we have considered, Caesar cipher was 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 Caesar cipher but with the knowledge of the plain text and cipher text key is relatively straightforward.

Then we came across the hill cipher. It is secure when compared with Caesar cipher and Play fair cipher because of the complexity in calculating k-1. Here k-1 is an m*m matrix and the attacker needs to try all possible values for each element in the matrix. But if attacker has both the plain text and the cipher text hill cipher can also be broken. The next cipher we came across was OTP. There is no compromise with the security of OTP but this cipher is generally not used because of the difficulty in generation and distribution of key.

So, a thrive for a better cipher continued. This gave rise to DES which was highly secure because it used a key of 56 bits. I t was extremely hard to break the key and a single machine performing 1 DES encryption per user took more than 1000 years to break the cipher. But later a machine was developed to break DES which challenged the cryptographers for an even better cipher. And then came AES which is used till now. So, till now, AES is the most efficient method for secure communication developed till now. But nothing is permanent here and AES can also be broken with the advancement in technology.

REFERENCE

[1] B. Schnieir, *Applied Cryptography*, John Wiley.
[2] D.R Stinson, *Cryptography- theory and practise*, CRS Press.
[3] S. Singh, *The Code Book,* Fourth Estate, London 1999.
[4] Sinkov, *Elementary Cryptanalysis*, The Mathematical Association of America, Washington, 1966.