ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 5, May 2017

A Survey on Classic Cipher in Cryptography

Payal Chhabra[1]

P.G. Student, Department of Information Technology, College of Technology, G.B Pant University of Agriculture and Technology, Pantnagar, Uttarakhand, India[1]

ABSTRACT: Today, in the admirable growth of internet environment, information security and data security is most challenging aspects that uses in many areas like computers, e-mail and communication. Cryptography is a technique of hiding the information that is recognized as encryption. Security is sharing or transferring of data without any alteration or hacking done by illegal operators. Here, there are several cryptographic algorithms [9]which send the information as cipher text and cannot be unstated by the introducers. Cryptography preserved confidentiality, authentication, integrity, availability and identification and also provide security and privacy of data to the user. Cryptography compromises the necessary protection in contradiction of the data intruders. The plain text is encrypted into a cipher text at receiver site and then cipher text is decrypted into plain text at receiver site for security purpose. In this paper, study of various encryption techniques has conceded out for providing data and information security.

KEYWORDS: Cryptography, Substitution and Transposition techniques, Comparison analysis.

I. INTRODUCTION

The word cryptography is derived from the Greek word in which ‘crypto’ means "hidden or secret" and 'graphy' means "writing". In cryptography only those can read and process it for which it is untended.Cryptography [7] is an art and science thatprotect the information in such a way that onlyanticipated recipient able to repossess this information. It is very convincing to encrypt the message so that intruder cannot recite the message. Cryptography is an art of hiding information throughtranslating the message. The art of secret writing or hiding information into an unreadable format called cipher text. Only those whokeep a secret key can decrypt the message into plain text. The system in which plain text in encrypted at sender side andcipher text is decrypted at receiver side using a unique key is called a Cryptographic system. Steganography and Cryptography are closely related and it also scrambles messages so that they cannot be understood by unauthorized user. According to Kerckhoffs law for cryptography “the superiorityof a cryptographic system is only be determined by small part of information called secret key i.e. otherinformation of the system did not give any information about the existence of hidden messages”. Knowledge of the key is mandatory to uncover or identify a message.

Cryptographic systems are characterized into threeextents:

1. The type of operations used for transforming plaintext to cipher text. Entirely encryption algorithms are based on two general ethics: first one is substitution, which mapped each element in the plaintext into another element, and another is transposition, which rearranged the elements in the plaintext.
2. The number of keys used. Symmetric, single-key, secret-key, or conventional encryption in which both sender and receiver uses same key. Asymmetric or public key encryption in which sender and receiver uses a different key.
3. The way in which the plaintext is processed. Processes one input block of elements at a time, producing an output block for each input block is called block cipher. Processes the input elements continuously and producing output one element at a time is called stream cipher.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 5, May 2017

Types of cryptography
Cryptography algorithms play an essential role in information security. It divided into Symmetric and Asymmetric key cryptography.

Symmetric Key Cryptography (Secret Key Cryptography)
In Symmetric key encryption similar key is used for encryption and decryption. The key iscirculated before transmission between two parties. Key plays amajor role in encryption and decryption process. Uncertainty a feeble key is used in the algorithm then data can be decrypted. The size of the key decides the asset of Symmetric key encryption. In SKC, the sender and the receiver aware with that same secret code or key and messages are encrypted by the sender and decrypted by the receiver through same secret key. It can be of 2 types: Stream Buffer in which digits of a message is encrypted one at a time. Block cipher in which number of bits is encrypted as a single unit.

Asymmetric Key Cryptography (Public Key Cryptography)
In asymmetric key encryption two different keys are used, one key for encryption and another key for decryption and users acquire the Key from a Certificate Authority. Asymmetric key (or public key) encryption solve the key distribution problem. In PKC private keys and public keys are used. For encryption public key is used and for decryption private key is used. Public key is known to public and private key is known to the user.

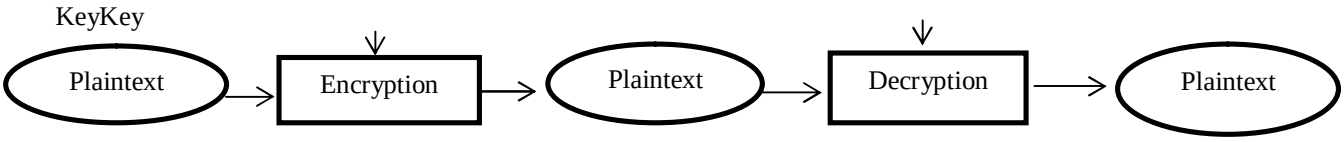

Figure 1.1 Diagram of cryptography process

Terms used in cryptography

1 Plain Text or Normal Text: The original text or message used in communication.

2 Cipher Text: The original text is encrypted in un-readable message. This coded message is called Cipher Text.

3 Encryption: Process of converting Plain text into Cipher text.

4 Decryption process: Process of converting Cipher text into Plain text.

5 Key:A key is a numeric or mathematical formula. In encryption process it takes place on Plain text and in decryption process it takes place on cipher text.

Objectives of cryptography:
1) **Confidentiality**:Confidentiality is a provision used to preserve the content of information by authenticating the sender and receiver before sending and receiving data. Secrecy is similar to confidentiality and privacy. There are numerous methodologies to providing confidentiality so that no one can recite the message except the intentional receiver. It means that only the genuine people are able to understand the message content and no one else.
2) **Integrity**: Data is free from any kind of modification among sender and receiver so data should be transmit between sender and intended receiver without any alteration being perceived. Data integrity is a service which discourses the unauthorized alteration of data. To guarantee data integrity, one must have the capacity to detect data manipulation by unauthorized parties. Data manipulation comprises such things like insertion, deletion, and substitution. Receiver assuring that the received message has not been altered in any way from the original.
3) **Non-repudiation**: Sender cannotcontradict his or her intents in the creation or transmission of the information.Non-repudiation is a service which prevents an entity from denying previous obligations or actions. Once disputes arise due to an entity denying then certain actions were taken, a means to resolve the situation is necessary. It is a mechanism to

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 5, May 2017

prove that the sender really sent this message. Means that neither the sender nor the receiver can untruthfully deny that they have sent a definite message

4) **Authentication**: The sender and receiver confirm each other's identity. Sender and receiver should be authenticated before sending and receiving data. Authentication is a service associated to identification. This function smears to both entities and information itself. Two parties entering into a communication should identify each other. Information sent over a channel should be authenticated for instance origin, date of origin, data content, time sent, etc.

II. OVERVIEW OF CLASSICALSYMMETRIC CRYPTOGRAPHY

Cryptographic algorithms [6, 2] are classified as classical cryptographic techniques and modern cryptographic techniques. Classical cryptographic techniques are developed in the most primitive days to provide confidentiality to the information. Modern cryptographic techniques are providing enhanced services like confidentiality, authentication, etc., to the information.

Substitution Techniques

Substitution ciphers analytically replace letters or groups of letters with other letters or groups of letters.

Caesar Cipher: **Caesar cipher** is also recognized as **Caesar's cipher**, the **shift cipher**, **Caesar's code** or **Caesar shift**, is one of the simplest and most usually known as encryption techniques. In this technique each letter in the plaintext is replaced with the letter standingsome fixed number of places further down the alphabet. Thissubstitution cipher was earliest use by Julius Caesar in which only 25 keys to try.

A shift may be of any amount, so that the encryption and decryption algorithm is:
Encryption: C = E (p) = (p + k) mod (26) where k takes on a value in the range 1 to 25.
Decryption: p=D(C) = (C – k) mod (26)

For example: k=3
Plain text: HELLO
Cipher text: KHOOR

Monoalphabetic Ciphers: Caesar cipher is not so protected because of 25 possible keys. A melodramatic increase in the key space can be completed by allowing an arbitrary substitution. A Monoalphabetic cipher customs fixed substitution for each letter of the alphabet over the entire message. Monoalphabetic substitution cipher or simple substitution cipher depend on a fixed replacement structure. Hence, if "a" is encrypted to "B" then every time the letter "a" in the plaintext replace with the letter "B" in the cipher text.

Example:
Plaintext: HELLO MESSAGE
Cipher text: IFMMP NFTTBHF

There are lots of different Monoalphabetic substitution ciphers, in fact infinitely many, as each letter can be encrypted to any symbol, not just another letter.

Play fairCipher: Play fair cipher was the first example of a digraph substitution cipher which is based on the use of a square matrix of 5X5 alphabetic letters arranged in a suitable manner [10]. Following are the steps of play fair cipher:

1. Select a key and place it in the matrix, the remaining letters of English alphabet are then one by one positioned in the matrix of Play fair cipher.
2. Disrupt the plain text into pairs and if a pair is same, then acquaint with a filler letter like 'x' after the first letter, otherwise if the pair are reside in the same row of matrix then each letter is interchanged by the immediate right respectively.
3. If the pair of letters is in same column of matrix then each letter is replaced by the immediate below respectively.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 5, May 2017

4. Pair of letters is neither in same column nor in same row then are they replaced with the letter on the same row respectively.

Example:key=play fair example

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

Plain text: Hide the gold pairing: Hi de thegoldx

Cipher text: bm odzbxdnage

Hill Cipher:Another curious multiletter cipher isa polygraphic substitution cipher which is based on linear algebra called,Hill cipher. Hill cipher [3] was the first polygraphic cipher in which more than three codes can be performed atone time.This encryption algorithm takes "m"uninterrupted plaintext letters and substitutes for"m" ciphertext letters. The replacement is determined by m linear equations in which each character is assigned a numerical value (a = 0, b = 1, … z = 25). For m = 3, the system can be described as follows:

C1 = (k11p1 + k12p2 + k13p3) mod 26
C2 = (k21p1 + k22p2 + k23p3) mod 26
C3 = (k31p1 + k32p2 + k33p3) mod 26

Encryption: C = KP mod 26

Decryption: $P=K^{-1}C \bmod 26$

Example: key=GYBNQKURP message= ACT

$$\begin{pmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{pmatrix} \begin{pmatrix} 0 \\ 2 \\ 19 \end{pmatrix} = \begin{pmatrix} 67 \\ 222 \\ 319 \end{pmatrix} = \begin{pmatrix} 15 \\ 14 \\ 7 \end{pmatrix} \begin{pmatrix} \bmod 26 \end{pmatrix}$$

Ciphertext is: $\begin{pmatrix} 2 \\ 0 \\ 19 \end{pmatrix}$

One-Time Pad: This encryption technique usages a random key which isas equivalentas the message being sent with no repetition. The word "pad" derives from early implementations where the key material was dispersed as a pad of paper, so that the top sheet could be easily decided and cracked once use. This technique is unbreakable or cannot be crackedbecause of indiscriminate output generated by OTP has no statistical relationship with plaintext and that plaintext is paired with a random secret key or one-time pad.Ciphertextholds no information about the plaintext apart from the maximum possible length of the message; there is ultimately no approach to break the code. In this technique,every bit or character of the plaintext is encoded by itsequivalent bit or character from the pad by modular addition. If the key is accurately randomand as long as the plaintext, then that key is certainly not reused in process and entirely undisclosed, then the resulting ciphertext will be challenging to decrypt or break. It has also been definite that any cipher with the faultless secrecy property must use keys with meritoriously the same requirements as OTP keys.

Transposition Techniques

Transposition techniques [11]rearrange the order of letters in a message and performing some sort of permutation on the plaintext letters to achieve different kind of mapping.

Rail fence: Rail fence or zigzag technique is a simplest technique in which the plaintext iswritten downwards and diagonally on consecutive "rails" of an imaginary fence and then read off as a sequence of rows.

For example: Plaintext: "meet me after the toga party" with a rail fence of depth 2.

m ^{e}e^{t} m ^{e}a ^{f} t ^{e} r^{t} h^{e} t^{o} g^{a} p^{a} r^{t} y

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 5, May 2017

Ciphertext: MEMATRHTGPRYETEFETEOAAT
This sort of thing would be insignificant to cryptanalyze.

Simple column TranspositionTechnique: Anextramultifarious technique in which message is written out in a rectangle, row by row, and then read out by column by column, also permute the direction of the columns. Key of the algorithm is the order of the columns.

For example: Key: ZEBRA permutation: 3 4 2 1 5 6
Plaintext: come home tomorrow
Ciphertext:1 2 3 4 5 6
c o m e ho =mtoeowoercmrhmoo
m e t o m o
rrow

Comparison of Various Techniques

Parameters / Techniques	Key Type	Key Size	Attack Type	Developed by	Advantage	Limitations
Caesar cipher	Substitution	25 keys	Brute force	Julius Caesar	One of the easiest methodologies used in cryptography.	Cracked by brute force attack because of 25 possible selections of key.
Hill cipher	Substitution	25 keys	Known plaintext attack	Lester S. Hill	Extensively more numerical nature than a portion of the others.	Encrypts identical plaintext blocks to identical ciphertext bl ocks
Playfair	Substitution	25 keys	Brute force attack, Frequency analysis	Charles Wheatstone	Convenient since it needs no special tools to use.	There is a minor bit of ambiguity in decryption process.
Monoalphabetic	Substitution	-	Known Plaintext A ttack	-	Easier to evoke the key phrase than anunplanned permutation of letters.	Easy to breakdownsince they reflect the frequency data of the original alphabet
One time pad	Substitution	Equal To plain text size	Key and ciphertext chosen	Frank Miller	Key is used one and only one time.	Only secure if each key is used to encrypt a single message
Rail fence	Permutation	-	Known cipher text, Chosen plaintext	-	Letters arranged in a zigzag manner which increase the difficulty of cracking the code.	number of possible solutions are so small that a cryptanalyst can try them all by hand

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 5, May 2017

Columnar transposition	Permutation	-	Frequency analysis attack.	-	Increase the security by combining with other ciphers	Problem with decipher, means receiver has to work out the column lengths by dividing the length of cipher text by the key length.

III. CONCLUSION

After studied all the above definite cryptography techniques it can be concluded that Cryptography provides secure communication, integrity, authentication and confidentiality over an internet. This criticismshowed that Caesar cipher is not so good because it gives a difference of 1 bitand it is also seen that Playfair giving better results by giving a difference of 7 bits.Thepurpose of this paper is to provide the fundamental knowledge about the cryptography algorithms and comparison of available symmetric key encryption techniques based on some parameters like limitation attack, Key factor, pros and consetc. Symmetric is faster and simpler as compared to asymmetric.The Playfair is significantly harder to break as well as stronger than a Monoalphabetic substitution cipher. The future work can be done in comparative study of various Asymmetric algorithms based on different factors like flexibility, speed, encryption time, scalability, etc. which found out best technique to provide better security to the complicated or unsecured network.

REFERENCES

[1]. Ajay kakkar, "Comparison of Various Encryption Algorithms and Techniques for secured Data Communication in Multinode Network" in International Journal of Engineering and Technology Volume 2 No. ISSN: 2049-3444 © 2011 – IJET, 2012.
[2]. Anjula Gupta,et.al, "Cryptography Algorithms: A Review "in International Journal of Engineering Development and Research, Vol.2 No.2.
[3]. Chris Christensen, "The Hill Cipher", MAT/CSC 483, 2006.
[4]. Fauzan Saeed and Mustafa Rashid, "Integrating Classical Encryption with Modern Technique" in JCSNS, Vol. 10, no.5,2010.
[5]. Mini Malhotra et.al, "Study of Various Cryptographic Algorithms" in International Journal of Scientific Engineering and Research, Vol.1, No.3, PP.77-88, 2013.
[6]. M.B.Nivetha, et.al, "A Comparative analysis of Cryptography Algorithms" in International Journal of Innovative Research in Electrical Electronical and Instrumentation Control Engineering, Vol.2, No.10, pp.2102-2105, 2014.
[7]. Manoj Kumar Pandey, et.al, "Survey Paper: Cryptography The art of Hiding Information" in International Journal of Advanced Research in Computer Engineering & Technology (IJARCET), ISSN: 2278 – 1323, Volume 2, Issue 12, 2013.
[8]. Shashi Mehrotra Seth et.al, "Comparative Analysis of Encryption Algorithms for Data Communication" in International Journal of Computer Science and Technology, Vol.2, No.2 pp.292-294, 2011.
[9].S.Pavithra, "Study and performance analysis of cryptographic algorithms" in International Journal of Advanced Research in Computer Engineering & Technology Volume 1 No. ISSN: 2278 – 1323, Issue 5, July 2012.
[10]. V. Umakanta Sastry, N. Ravi Shanker and S. Durga Bhavani, "A Modified Playfair Cipher Involving Interweaving and Iteration" in International Journal of Computer Theory and Engineering, Vol. 1, no. 5, 2009.
[11]. William Stallings, "Cryptography and Network Security: Principles & Practices", second edition, chapter 2 page 29.