Hybrid Data Encryption Standard

Umesh Diwekar[1], Ambrish Srivastav[2]
[1, 2] SWAMI VIVEKANAND COLLEGE OF ENGINEERING

Abstract- *All the conventional encryption techniques are very weak and brute force attack and traditional cryptanalysis can be used to easily determine the plain text from encrypted text. Data encryption standard (DES) is a private key cryptography system that provides the security in communication system but now days the advancement in the computational power the DES seems to be weak against the brute force attacks. We proposed a hybrid algorithm to encrypt the plain text message for its security. By using an Enhanced DES algorithm the security has been improved which is very crucial in the communication and field of Internet. If the transposition technique is utilized before the original DES algorithm then the intruder required first to break the original DES algorithm and then transposition technique. So the security is approximately double as compared to a simple DES algorithm.*

Keywords- Columnar, Cipher text, Decryption, DES, Encryption, LPT, Plain text, RPT, SCTTMR, Transposition Cryptography, Hill Cipher, Information Security

I. INTRODUCTION

In today's world, it is impossible to imagine without web or internet. This modern era is dominated by paperless transactions in business, private or government offices by means of use of E-mail messages, E-cash transactions, etc. Due to this there is a great need of transmission of data through internet. In various business sectors, there may be sensitive and confidential information like banking transactions, credit information, government information, sensitive information is transferred over web using E-mails, etc. The confidentiality, authentication and integrity of such important information should be maintained and protected [1]. To protect this type of sensitive information from unauthorized access, there is a great need of security. To protect sensitive text information from unauthorized access various encryption techniques are used. Encryption technique is first used by Julius Caesar. When Julius Caesar sent messages to his generals, he didn't trust his messengers. So he replaced every A in his messages with a D, every B with an E, and so on through the alphabet. Only someone who knew the "shift by 3" rule could decipher his messages. Example. For a message "secret", if shift by 3 rule (+3) is applied for number of times, then encrypted message will change as follows:
+3 +3 +3
secretvhfufwykixiz and so on.

To decrypt it again start from last encrypted message and reverse shift the characters by 3 (-3) and finally original message can be obtained.

Encryption plays a main role in information security. The encryption techniques methods are used to convert our text information in a non-readable form at sender side and convert that information in readable form again at receiver side.

Cryptology is the study of cryptosystems. It can be divided into two competing skills – concealment and solution.

The concealment portion of cryptology is called cryptography. The aim of cryptography is to render a message incomprehensible to the unauthorized reader. Cryptography concerns with the design of cryptosystems. The process of creating non-readable text information or cipher so that only intended person is only able to read the information is called Cryptography. It uses mathematical algorithms to encrypt and decrypt data. It enables you to store sensitive information or transmit it across insecure networks so that it cannot be read by anyone except the intended recipient. Cryptography is often called "code making".

The solution portion of cryptology is called cryptanalysis. While cryptography is the science of securing data, cryptanalysis is the science of analyzing and breaking secure communication i.e. breaking of cryptosystems. Cryptanalysis is often called "code breaking". Figure 1 shows the encryption process and Figure 2 shows the decryption process [2].

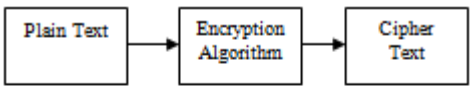

Figure 1: Encryption Process

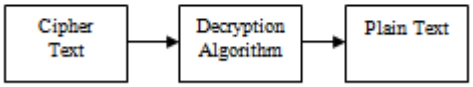

Figure 2: Decryption Process

As shown in figure 1 and figure 2, Cryptography consists of two main steps: Encryption & Decryption. Using encryption process text information is converted non-readable form. Decryption is reverse of encryption process. Plaintext information is the intended original message. Cipher text information is the coded message. There are two techniques of plain text encryption: Substitution Technique and Transposition Technique.

In substitution technique, the letters of plain text are replaced by other letters or any number or by symbols. Ex. Caesar cipher, Hill cipher, etc. In transposition technique, some sort of permutation is performed on plaintext. Ex. Rail Fence method, Columnar method, etc.

A. Terminologies in Cryptography

An encryption technique has five ingredients [2]:

1. Plaintext: This is the original intelligible message or data that is fed into the algorithm as input.
2. Encryption Algorithm: The encryption algorithm performs various substitutions and transformations on the plaintext.
3. Key: The key is also input to encryption algorithm. The key is a value independent of the plaintext and of the algorithm. The algorithm will produce a different output depending on the specific key being used at the time.
4. Cipher text: This is the scrambled message produced as output. It depends on the plaintext and secret key.
5. Decryption Algorithm: This is essentially the encryption algorithm run in reverse. It takes the cipher text and the secret key and produces the original plaintext.

B. Types of Cryptography

Cryptography is a technique in which secret messages are transferred in the encrypted form from sender to receiver over the communication line.

Cryptographic techniques are very useful to protect secret information. They protect the secret or confidential information by converting the information to some unintelligible form using a key. To retrieve the information, the encrypted information should be converted back to original information using some keys. Based on the key, the cryptography can be classified into two categories [1]:

1. Shared key cryptography
2. Public key cryptography

Shared key cryptography also called symmetric key cryptography or private key cryptography or secret key cryptography in which, same key is used for encryption and encryption i.e. both the sender and the receiver know the same key. Ex. DES, 3DES, AES, etc. Messages are encrypted by the sender using the key and decrypted by the receiver using the same key.

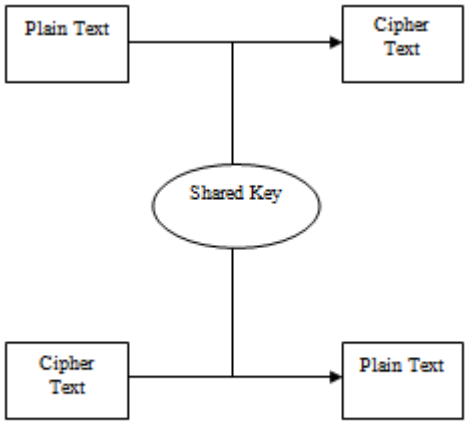

Figure 3: Shared Key Cryptography

Figure 3 shows process of secret key cryptography [2]. Here same key is shared by both sender and receiver for encryption and decryption.

Public key cryptography also called asymmetric key cryptography which uses different keys for encryption and decryption. Ex. RSA, Digital signature scheme, etc. The public key is known to all the receivers, is used for encrypting the plaintext message. The private key is known only to the user of that key. With public key cryptography, keys work in pairs of matched public and private keys. Figure 4 shows the process of public key cryptography where public key used by sender for encryption and all the receivers use their private keys for decryption. Messages encrypted using the public key cannot be decrypted using the public key. Public key encrypted messages can only be decrypted using corresponding private key which is kept secure.

Asymmetric key cryptography is very slower and has very higher computational costs which are most of the time prohibitive for multimedia data. Symmetric key cryptography is fast, comparatively lower cost and may be used for multimedia data.

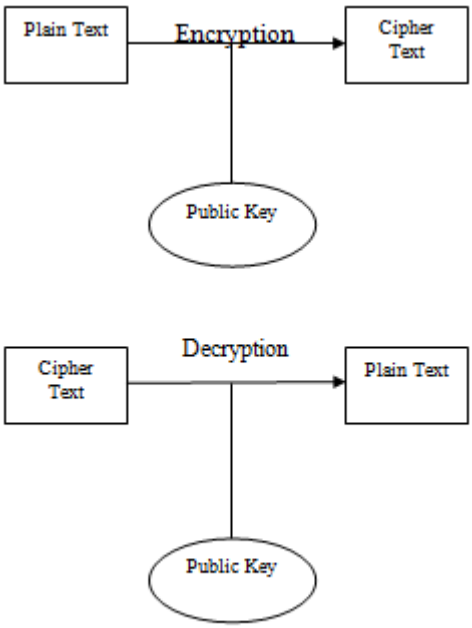

Figure 4: Public Key Cryptography

Hash function is another type of cryptography which makes use of some mathematical transformation.

II. LITERATURE SURVEY

This section consists of brief description of few classical and modern plain text encryption techniques.

M. Nordin[5] The Caesar cipher is one of the earliest known and simplest ciphers. The method is named after Julius Caesar, who apparently used it to communicate with his generals [1]. It is a type of substitution cipher in which each letter in the plaintext is 'shifted' a certain number of places down the alphabet. For example, with a shift of 1, A would be replaced by B, B would become C, and so on. The Caesar cipher offers essentially no communication security, and it can be easily broken even by hand [1].

M. Nordin[5] The Playfair cipher is a polygraphic cipher which enciphers two letters at a time. The Playfair cipher was the first practical digraph substitution cipher. The scheme was invented in 1854 by Charles Wheatstone, but was named after Lord Playfair who promoted the use of the cipher [4]. The technique encrypts pairs of letters, instead of single letters as in the simple substitution cipher. The Playfair is significantly harder to break since the frequency analysis used for simple substitution ciphers does not work with it. Frequency analysis can still be undertaken, but on the 25*25=625 possible digraphs rather than the 25 possible monographs. Frequency analysis thus requires much more cipher text in order to work [3].

It was used for tactical purposes by British forces in the Second Boer War and in World War I and for the same purpose by the Australians during World War II. This was because Playfair is reasonably fast to use and requires no special equipment [3]. A typical scenario for Playfair use would be to protect important but non-critical secrets during actual combat. By the time the enemy cryptanalysts could break the message the information was useless to them.

M. Nordin[5] The Affine cipher is a special case of the more general monoalphabetic substitution cipher. The cipher is less secure than a substitution cipher as it is vulnerable to all of the attacks that work against substitution ciphers, in addition to other attacks [5]. The cipher's primary weakness comes from the fact that if the cryptanalyst can discover (by means of frequency analysis, brute force, guessing or otherwise) the plaintext of two cipher text characters, then the key can be obtained by solving a simultaneous equation.

Kashish Goyal[6] Vigenere cipher was proposed by Blaise de Vigenere in the 16th century [2]. Vigenere cipher is poly-alphabetic substitution cipher in which a single plain text letter can be converted into multiple cipher text letters. This conversion depends on the position of the letter in the plain text e.g. c may be converted into g because it is at position 3 in the plain text but c can be changed into z because its position in the plain text is 5. Vigenere cipher makes use of Vigenere table of size 26 X 26.

Kashish Goyal[6] Blowfish cipher was developed by Bruce Schneier. Blowfish is a variable-length key, 64-bit block cipher [2]. The algorithm consists of two parts: a key-expansion part and a data- encryption part. Key expansion converts a variable-length key of at most 56 bytes into several sub key arrays totaling 4168 bytes. Data encryption occurs via a 16-round Feistel network. Each round consists of a key-dependent permutation, and a key- and data-dependent substitution.

Ramandeep Sharma[2] Rail fencing technique involves: Writing plain text message as a sequence of diagonal and reading it as a sequence of row to produce cipher text [3]. In a Rail Fence cipher, after removing the spaces from the original message, write the characters in the message in the zigzag pattern. The key for the Rail Fence cipher is just the number of rails.

Kashish Goyal[6] Modern ciphers use both substitution and transposition to encrypt the message that increases the security of data. The data is encrypted in blocks instead of single characters at time. The well-known example

of block cipher is Data Encryption Standard (DES). DES uses 56-bits key and encrypt 64-bits of data as a single block [3].

AES uses the same key for both encryption and decryption. The AES standard states that the algorithm can only accept a block size of 128 bits and a choice of three keys - 128, 192, 256 bits. Depending on which version is used, the name of the standard is modified to AES-128, AES-192 or AES- 256 respectively [5].

The Rijndael Algorithm is the new Advanced Encryption Standard (AES) recommended by the US National Institute of Standards and Technology (NIST) for protecting sensitive, unclassified government information [7]. Since Rijndael is an iterated block cipher, the encryption or decryption of a block of data is accomplished by the iteration of a specific transformation. As input, Rijndael accepts one-dimensional 8-bit byte arrays that create data blocks. The plaintext is input and then mapped onto state bytes. The cipher key is also a one-dimensional 8-bit byte array. With an iterated block cipher, the different transformations operate in sequence on intermediate cipher results.

The columnar transposition cipher is a fairly simple, easy to implement cipher. It is a transposition cipher that follows a simple rule for mixing up the characters in the plaintext to form the cipher text [6]. Although weak on its own, it can be combined with other ciphers, such as a substitution cipher, the combination of which can be more difficult to break than either cipher on its own.

Gary C. Kessler[1] In Cryptanalysis, the attacker uses various methods to get the plain text from the cipher text. They try to find out the way in which plain text is converted into cipher text and the encryption key used [3]. Various methods were used for identifying ciphers. Identification of permutation, substitution and Vigenère ciphers was done using frequency analysis. An attempt was made to identify block ciphers like DES and Blowfish using pattern recognition method [1]. Other ciphers like stream cipher SEAL and Enhanced RC6 have been identified using neural networks.

M. Nordin[5] The Hill cipher (HC) algorithm is one of the famous and known symmetric algorithms in the field of cryptography. It is a poly-alphabetic cipher proposed by the mathematician Lester Hill in 1929 in the journal of mathematics. Hill cipher requires a matrix based polygraphic system [5]. The Hill cipher takes m successive plaintext characters and substitutes for them m cipher text characters.

The core of Hill cipher is matrix manipulations. For encryption, algorithm takes m successive plaintext characters and instead of that substitutes m cipher characters.
For example m=2; {abcdef…} =ab cd ef… or abcdef… and so on.

In Hill cipher, each character is assigned a numerical value like a = 0, b = 1, ... , z = 25. The substitution of cipher text characters in the place of plaintext characters leads to m linear equation. For m = 3, the system can be described as follows:

$$C=KP$$

where C and P are column vectors of length 3, representing the plaintext and cipher text, respectively and K is a 3 x 3 matrix, which acts as key for encryption. All operations performed with modulus of 26. In Hill cipher key is an invertible m x m matrix, where m is block length. Decryption process uses inverse of matrix K. The inverse matrix K-1 of a matrix K is defined by following equation.

$$KK-1 = K-1K=I$$

Where, I is the Identity matrix. But the inverse of matrix does not always exist and when it exists, it satisfies above equation. The inverse matrix K-1 is used to decrypt the cipher text. In general it can be written as follows:

Encryption Process:

$C=Ek (P) =KP$
Decryption Process:
$P=Dk(C) =K-1C= K-1Kp=P$

If the block length considered as m, there are 26m different m characters blocks are possible.

III. PROBLEM DOMAIN

Security is playing a very important and crucial role in the field of network communication systems and Internet. Data encryption standard (DES) is a private key cryptography system that provides the security in communication system but now the advancement in the computational power the DES seems to be weak against the brute force attacks. The speed of DES algorithm is very low as compared to available hardware resources.

IV. PRAPOSED METHODOLOGY

In cryptography, a transposition cipher is a method of encryption by which the positions held by units of plaintext (which are commonly characters or groups of characters) are shifted according to a regular system, so that the cipher text constitutes a permutation of the plaintext. That is, the order of the units is changed. Mathematically a bijective function is used on the characters' positions to encrypt and an inverse function to decrypt.

A systematic review is a means of evaluating and understanding all available research relevant to a particular research question or phenomenon of interest. A systematic literature review presented in [11] is followed in this research work to conduct the review about encryption methods used in cloud computing for data confidentiality. Some researchers provide a review on security issues in cloud computing but this review aims to focus on the encryption methods used to resolve the security issue of the data confidentiality in cloud environment.

Many researchers contribute their efforts in the field of software engineering/computer science by adopting [11] systematic literature review process such as in [12, 13] systematic literature review process was adopted for the review of aspect oriented implementation of software product lines components and software component reusability assessment approaches. In [13] systematic review process was followed for the analysis of security issues in cloud computing. In [9] systematic review process was adopted to conduct a review on data security in cloud computing.

In other words, a transposition cipher is one in which plaintext symbols are rearranged (i.e., transposed or permuted) to produce cipher text. The method of transposition may be either mathematical or typographical in nature.

The technique which we would be using for this purpose is RAIL FENCE TECHNIQUE.

The explanation is as follows:

Rail Fence Cipher

The Rail Fence cipher is a form of transposition cipher that gets its name from the way in which it is encoded.

In the rail fence cipher, the plaintext is written downwards on successive "rails" of an imaginary fence, then moving up when we get to the bottom. The message is then read off in rows.

Example: We encipher NOTHING IS AS IT SEEMS by first writing it on two lines in a zigzag pattern (Or rail fence). The cipher text is produced by transcribing the first row followed by the second row.

N T I G S S T E M
O H N I A I S E S

Cipher text: NTIGS STEMO HNIAI SES.

To decrypt, we write half the letters on one line, half on the second.
(Note that if there are an odd Number of letters, we include the “middle” letter on the top line.)

V. CONCLUSIONS

In today's time, the security is playing a very important and powerful role in the field of networking, Internet and various communication system .The electronic communication system is used in banking, reservation system and marketing which required a very tight security system. The original DES implementation has some weaknesses to overcome the most of weakness the Enhanced DES algorithm is developed. The Designed system improved the security power of original DES. The only disadvantage of Enhanced DES is extra computation is needed but the today’s computer have parallel and high speed computation power so the drawback of the Enhanced DES algorithm is neglected because our main aim is to enhance the security of a system. By using the Enhanced DES algorithm the security is very tight and approximately impossible to crack and break the Enhanced DES algorithm.

REFERENCES

[1] Qi-Tao Lin, Chang-Dong Wang, Jing Pan, Lu Ling and Jian-Huang Lai Local Data Security and Privacy Protection in Cloud Service Applications paper present at © 2015 IEEE
[2] B. Padmavathi1, S. Ranjitha Kumari2 A Survey on Performance Analysis of DES, AES and RSA Algorithm along with LSB Substitution Technique paper present at International Journal of Science and Research (IJSR
[3] MILIND MATHUR AYUSH KESARWANI COMPARISON BETWEEN DES , 3DES , RC2 , RC6 , BLOWFISH AND AES paper present at National Conference on New Horizons in IT - NCNHIT 2013
[4] Evaluation of DES, TDES, AES, Blowfish and Two fish Encryption Algorithm: Based on Space Complexity paper present at International Journal of Engineering Research

& Technology (IJERT) ISSN: 2278-0181 Vol. 3 Issue 4, April - 2014

[5] I. Foster, Z. Yong, I. Raicu and L. Shiyong, (2008, 12-16 Nov. 2008), Cloud Computing and Grid Computing 360-Degree Compared, Paper presented at the Grid Computing Environments Workshop, 2008, GCE '08.

[6] A. A. Soofi and M. I. K Fazal-e-Amin, "A Review on Data Security in Cloud Computing", International Journal of Computer Applications, vol. 94, no. 5, (2014), pp. 12-20.

[7] NIST SP 800-145, "A NIST definition of cloud computing", [online] 2012, http://csrc.nist.gov/publications/drafts/800-145/Draft-SP-800-145_cloud-definition.pdf (Accessed: 23 December (2013).

[8] G. RAMESH Dr. R. UMARANI, Performance Analysis of Most Common Symmetrical Encryption Algorithms", International Journal of Power Control Signal and Computation(IJPCSC) Jan-Mar 2012

[9] Gartner, "What you need to know about cloud computing security and compliance", (HeiserJ), [online] 2009, https://www.gartner.com/doc/1071415/need-know-cloud-computing- Security (Accessed 23 December 2013).

[10] Z. Yandong and Z. Yongsheng, "Cloud computing and cloud security challenges in Information Technology in Medicine and Education (ITME)", 2012 International Symposium on, (2012), pp. 1084-1088.

[11] IBM, "what is cloud computing" [online] http://www.ibm.com/cloud-computing/in/en/what-is-cloud- computing.html (Accessed: 14 December 2013). IDG Cloud Computing Survey: "Security, Integration Challenge Growth", [online], http://www.forbes.com/sites/louiscolumbus/2013/08/13/idg-cloud-computing-survey-security-integration-challenge growth.html/(Accessed: 28 December 2013).

[12] D. Catteddu and G. Hogben, "Cloud computing: Benefits, risks and recommendations for information security", European Network and Information Security Agency (ENISA), pp. 1–125.

[13] S. Subashini and V. Kavitha, "A survey on security issues in service delivery models of cloud computing", Journal of Network and Computer Applications, vol. 34, no. 1, (2011), pp. 1-11.