ISSN: 2278 – 1323
International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)
Volume 2, Issue 12, December 2013

Survey Paper: Cryptography The art of hiding Information

Manoj Kumar Pandey [1]
M.Tech Scholar
Computer Science & Engineering
Chhatrapati Shivaji Institute of Technology
Durg

Mrs. Deepty Dubey [2]
Assistant Professor
Computer Science & Engineering
Chhatrapati Shivaji Institute of Technology
Durg

Abstract— Data security is one of the important aspects of data communication. The confidential data being sent via electrical media is very sensitive, which can be accessed for malicious purpose. The conventional methods of encryption can only maintain the data security so modern cryptography is very much needed to enhance the data security, so need of developing new concept and new cryptography is demand of the hour. Therefore it is necessary to apply efficient encryption technique to enhance data security. This paper mainly focuses on the different kind of encryption techniques that existing.

Index Terms— **Data security, Encryption, Multiphase encryptions, Multiple encryption.**

I. Introduction

Cryptography is the science of devising methods that allow information to be sent in a secure form in such a way that the only person able to retrieve this information is the intended recipient [1]. The highly use of networking leads to the data exchange over the network while communicating to one and another system. While communication it is very important to encrypt the message so that intruder cannot read the message. Network security is highly based on cryptography. Cryptography is an art of hiding information by encrypting the message using algorithms. The cryptography system is a system which performs encryption and decryption process. The encryption process takes plain text as input and produce an output called cipher text using keys. The decryption process performs same as encryption but in reverse order. Cryptography algorithm mainly falls under two categories i.e. Asymmetric and Symmetric encryption techniques. In modern times, cryptography is considered a branch of both mathematics and computer science, and is affiliated closely with information theory, computer security, and engineering [2]. A plain text is encrypted using an algorithm called "encryption algorithm". A cipher text is decrypted using an algorithm called "decryption algorithm". A key is used at the time of encryption and decryption process. The security level of cryptography is determined by the key space (size of key). This paper holds some of the encryption techniques and security issues.

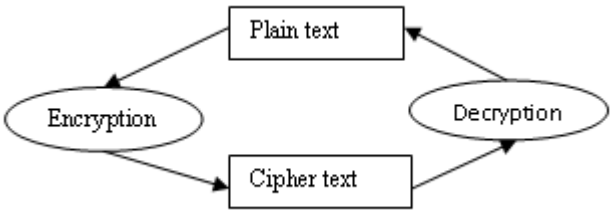

Fig 1: Encryption and decryption process

II. Cryptography Goals

Cryptography is used to achieve many goals some of the goals are as follows:

1. Authentication: it is a process of giving identity to someone to access particular resource using the keys.

2. Confidentiality: It is most important goal of cryptography, which ensure that nobody understand the message except the one who has the cipher key.

3. Data Integrity: It is the process of ensuring that nobody is allowed to alter the transmitted message except the party who is allowed to do so.

4. Non-Repudiation: Ensure that neither the sender nor the receiver of the message should be allowed to deny the transmission of the message.

5. Access Control: Ensure that only the authorized parties are able to access the transmitted message.

III Basic Terminology used in cryptography

1. Plain Text: The original message which is to be sent from sender to the receiver. This plain text is put as an input at the time of encryption process.

For example: if Ram wants to send a message "hello world" to Sohan then it is consider as a plain text.

2. Cipher Text: Cipher text is a text which is being sent from sender to receiver and it is not understandable by anyone. It is output of the encryption process. For example: "*@97K&A%L#1" is a cipher text produced for plain text "hello world".

3. Encryption: It is a process of converting a plain text into cipher text by using encryption key and an algorithm known as encryption algorithm.

4. Decryption: it is a process of converting a cipher text into a plain text by using decryption key and an algorithm known as decryption algorithm.

5. Keys: A Key is a numeric or alpha numeric text or may be a special symbol. The Key is used at the time of encryption takes place on the Plain Text and at the time of decryption takes place on the Cipher Text. The selection of key in Cryptography is very important since the security of encryption algorithm depends directly on it [3].

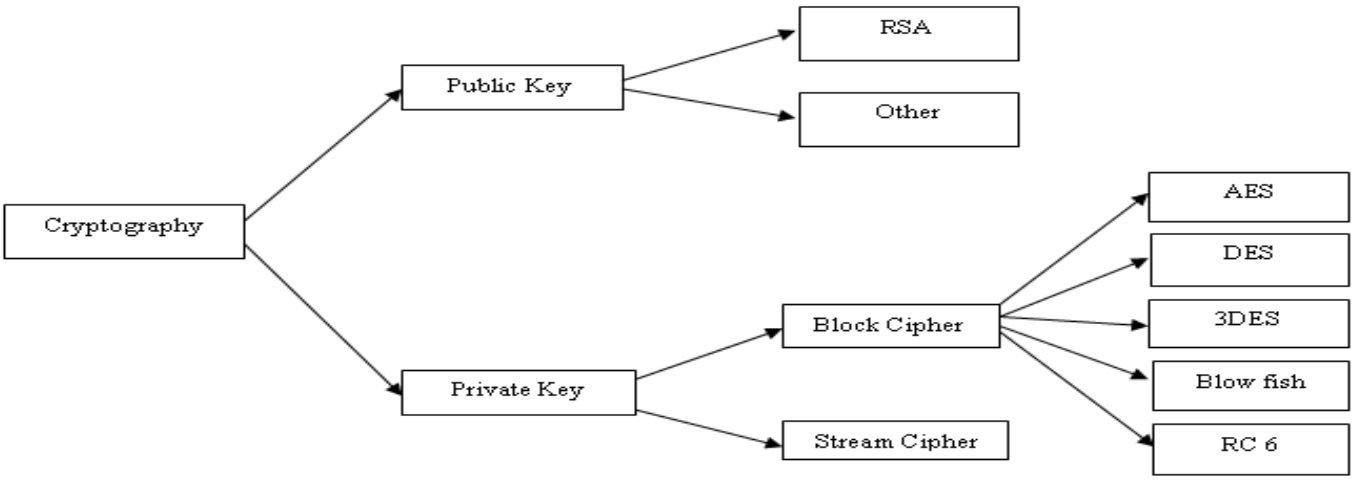

Figure 2: commonly used encryption technique

IV Classification of Cryptography

Cryptography can be divided into two major category based on the use of key.

1. **Symmetric Encryption (Private Key Encryption):** In this type of encryption same key is used at the time of encryption and decryption. The key distribution has to be made before the transmission of the information starts. The key plays a very important role in this type of encryption.
   Example: DES, 3DES, BLOWFISH, AES etc.
2. **Asymmetric Encryption (Public Key Encryption):** In this type of encryption different key is being used for encryption and decryption process. Two different key is generated at once and one key is distributed to other side before the transmission starts.
   Example: RSA algorithm.

V Brief description of Most commonly used algorithm:

1. **Advance encryption algorithm (AES):** AES algorithm is one of the most widely used encryption algorithm. AES is a block cipher .It has variable key length of 128, 192, or 256 bits; default 256. It encrypts data blocks of 128 bits in 10, 12 and 14 round depending on the key size. AES encryption is fast and flexible; it can be implemented on various platforms especially in small devices [4].
   Four different stages are used, one of permutation and three of substitution:
   - Substitute bytes: Uses an S-box to perform a byte-by-byte substitution of the block
   - ShiftRows: A simple permutation
   - MixColumns: A substitution that makes use of arithmetic over $GF(2^8)$
   - AddRoundKey: A simple bitwise XOR of the current block with a portion of the expanded key.

2. **Data encryption standard (DES):** The initial key consists of 64 bits. However, before the DES process even start, every eight bit of the key is discarded to produce a 56-bit key. DES Encryption is based on the two fundamentals attributes of cryptography: substitution and transportation. DES consists of 16 steps, each of which is considered as round. Each round performs the steps of substitution and transportation as: In the first step, the 64-bit plain text block is handed over to an Initial Permutation (IP) function. The Initial Permutation is performed on plain text. Next, the IP produces two halves of permutated block; say Left Plain Text(LPT) and Right Plain Text(RPT)[4][5]. Then, each LPT and RPT goes through 16 rounds for encryption process. In the end, LPT and RPT are rejoined and a Final Permutation is performed on the combined block and result of this process produce 64-bit cipher.
3. **Triple Data encryption standard (3DES):** 3DES was developed in 1998 and derived for DES. It applies DES encryption 3 times to perform encryption and decryption process is just reverse of encryption process. It uses key length 56*3=168 bits. 3DES encryption can be performed using either 2 key or 1 key. 3DES encryption follows encrypt-decrypt-encrypt (EDE) sequence.
   - If 3DES encryption uses two key K1 and K2 respectively then
     C = E (K1, D (K2, E (K1, P)))
     P = D (K1, E (K2, D (K1, C)))
   - If 3DES encryption uses one key K1 then
     C = E (K1, D (K1, E (K1, P)))
     P = D (K1, E (K1, D (K1, C)))

   3DES with two key is relatively most popular alternative to DES and has been adopted by for use in the key management standards ANS X9.17 and ISO 8732 [4].

4. **Multiphase encryption:** Multiphase encryption is a modern encryption technique. Multiphase encryption comprises number of such phases which are strongly protected due to multiple encryption in each phase [2].In multiphase encryption the number of phases can be extent to n number of phase depending upon the type of data and required security.

Example:

Plain text (P): = HELLOWORLD
Algorithm (C): = ((P+1) +3) +2…… (N times)
Cipher Text:

IFMMPXPSME (After first cycle)
LIPPSASVPH (After second cycle)
NKRRUCUXRJ (After third cycle)
……
……
Encrypted N Times.

VII Literature survey

Mohammed Abutaha [6] mentioned that the main disadvantage of symmetric key cryptography is that all parties involved have to exchange the key used to encrypt the data before they can decrypt it. This requirement to securely distribute and manage large numbers of keys means most cryptographic services also make use of other types of encryption algorithms. Secure MIME (S/MIME).
for example uses an asymmetric algorithm - public/private key algorithm - for non-repudiation and a symmetric algorithm for efficient privacy and data protection.

RSA is much slower than symmetric encryption, what typically happens is that data is encrypted with a symmetric algorithm and then the comparatively short symmetric key is encrypted using RSA.

Yogesh Kumar [7] has done the comparison between DES and AES and found that DES is faster and AES is Slower, key distribution is difficult in DES and key distribution is easy, complexity of DES is O (Log N) and complexity of RSA is O (N3), Security in DES is Moderate and Security in RSA Height, Nature of DES is closed and Nature of RSA is Open, Secure services in DES is done confidently and Secure service in RSA is done Confidentially with integrity and no repudiation.

Simar Preet Singh, and Raman Maini [8] has done comparison between algorithms and found that AES shows poor performance results compared to other algorithms, since it requires more processing power. They also found that 3DES requires always more time than DES because of its triple phase encryption characteristic.

Shashi Mehrotra Seth and her collegue Rajan Mishra(2011) jointly has done a Comparative Analysis Of Encryption Algorithms. The experimental results shows the comparison of three algorithm AES, DES and RSA using same text file for five experiment, output byte for AES and DES is same for different sizes of files. The authors noticed the RSA has very smaller output byte compare to AES and DES algorithm. Time taken by RSA algorithm is much higher compare to the time taken by AES and DES algorithm.

1Shashi Mehrotra Seth, 2Rajan Mishra [9] concluded that memory usage while encryption time difference is very minor in case of AES algorithm and DES algorithm. RSA consume longest encryption time and memory usage is also very high but output byte is least in case of RSA algorithm.

Diaa Salama Abd Elminaam1, Hatem Mohamed Abdual Kader2, and Mohiy Mohamed Hadhoud3 [10] have concluded that RC6 requires less time than all algorithms except Blowfish. The AES has an advantage over other 3DES, DES and RC2 in terms of time consumption and throughput. 3DES has low performance in terms of power consumption and throughput when compared with DES.

Himanshu Gupta and Vinod Kumar Sharma [2] mentioned that the source code for multiphase encryption will increase the popularity of Applied Cryptography for the enhancement of data security. At the initial stage, the implementation of multiphase encryption may be complex but it will enhance the security of data communication enormously.
Himanshu Gupta and Vinod Kumar Sharma [2] also mentioned that Multiphase encryption may reduce the problem of key
management in the existing technology of Personal Identity Verification (PIV) due to use of different encryption algorithms with fixed size keys instead of large number of variable length keys.
Himanshu Gupta and Vinod Kumar Sharma [2] concluded that Multi-phase Data Encryption describes the enhanced complexity of data encryption due to multiple operations of single phase encryption techniques in cryptography and the advantage of multiple encryptions is that it provides better security because even if some component ciphers are broken or some of the secret keys are recognized, the confidentiality of original data can still be maintained by the multiple encryptions.

VIII Conclusion

Data security is one of the import aspects of communication. Security of data can be achieved using the art of cryptography. There are many algorithms available for cryptography but the selection of one of the best algorithm is also very important. The algorithm for encryption can be selected based on the type of data being communicated and type of channel through which data is being communicated. In this paper, it has been surveyed that the existing works on the encryption techniques. Those encryption techniques are analyzed well to enhance the data security. As the day passes modern encryption is needed to promote the data security. The study of multiphase encryption techniques enhances the data security but multiphase techniques must also be reviewed for security purpose.

IX References:

[1] Y.Wang and M. Hu, ―Timing - evaluation of the known cryptographic algorithms, in proc. International Conference on Computational Intelligence and Security, Beijing, China Dec 2009.

[2] International Journal of Computer Theory and Engineering, Vol. 5, No. 4, August 2013 Multiphase Encryption: A New Concept in Modern Cryptography by Himanshu Gupta and Vinod Kumar Sharma.

[3] International Journal of Advanced Research in Computer Science and Software Engineering Volume 2, Issue 7, July

2012 A Survey on Various Most Common Encryption Techniques by E.Thambiraja, G. Ramesh and Dr. R. Umarani.

[4] W.Stallings, "Cryptography and Network Security 4th Ed," Prentice Hall, 2005.

[5] Coppersmith, D. "The Data Encryption Standard (DES) and Its Strength Against Attacks."I BM Journal of Research and Development, May 1994, pp. 243 -250.

[6] Mohammed Abutaha, Mousa Farajallah, Radwan Tahboub & Mohammad Odeh Survey Paper: Cryptography Is The Science Of Information Security International Journal of Computer Science and Security (IJCSS), Volume (5): Issue (3) : 2011 298

[7] IJCSMS International Journal of Computer Science and Management Studies, Vol. 11, Issue 03, Oct 2011 Comparison of Symmetric and Asymmetric Cryptography with Existing Vulnerabilities and Countermeasures by Yogesh Kumar1, Rajiv Munjal2, Harsh Sharma3

[8] Simar Preet Singh, and Raman Maini "COMPARISON OF DATA ENCRYPTION ALGORITHMS" International Journal of Computer Science and Communication Vol. 2, No. 1, January-June 2011, pp. 125-127

[9] 1Shashi Mehrotra Seth, 2Rajan Mishra," Comparative Analysis of Encryption Algorithms for Data Communication", IJCST Vol. 2, Issue 2, June 2011 pp.192-192.

[10] Diaa Salama Abd Elminaam1, Hatem Mohamed Abdual Kader2, and Mohiy Mohamed Hadhoud2," Evaluating The Performance of Symmetric Encryption Algorithms", International Journal of Network Security, Vol.10, No.3, PP.213-219, May 2010.