Multiphase Encryption: A New Concept in Modern Cryptography

Himanshu Gupta and Vinod Kumar Sharma

***Abstract*—Data Security is a challenging issue of data communications today that touches many areas including secure communication channel, strong data encryption technique and trusted third party to maintain the database. The rapid development in information technology, the secure transmission of confidential data herewith gets a great deal of attention. The conventional methods of encryption can only maintain the data security. The information could be accessed by the unauthorized user for malicious purpose. Therefore, it is necessary to apply effective encryption/ decryption methods to enhance data security. The multiple encryption techniques of present time cannot provide sufficient security. In this research paper, the new encryption technique named as —Multiphase Encryption is proposed. In this encryption technique, original data is encrypted many times with different strong encryption algorithms at each phase. This encryption technique enhances the complexity in encryption algorithm at large extent.**

***Index Terms*—Multiphase encryption, data security, 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]. Cryptography is the practice and study of hiding information. 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. Cryptography is used in applications present in technologically advanced societies; examples include the security of ATM cards, computer passwords, and electronic commerce, which all depend on cryptography [2].

The basic principle of Cryptography is defined as: A message being sent is known as plaintext. The message is then coded using a cryptographic algorithm. This process is called encryption. An encrypted message is known as ciphertext, and is turned back into plaintext by the process of decryption [3]. The method for decryption is the same as that for encryption but in reverse direction. It is applicable in each phase of encryption. The graphical presentation of this encryption and decryption process is shown in Fig. 1.

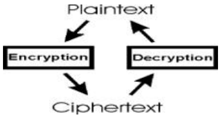

Fig. 1. Encryption-decryption process

For making any communication process footprint it must be assumed that some eavesdropper has access to all communications between the sender and the recipient. A method of encryption is only secure if even with this complete access, the eavesdropper is still unable to recover the original plaintext from the cipher text.

There is a big difference between security and obscurity. If a message is left for somebody in an airport locker, and the details of the airport and the locker number is known only by the intended recipient, then this message is not secure, merely obscure. If however, all potential eavesdroppers know the exact location of the locker, and they still cannot open the locker and access the message, then this message is secure.

Multiple encryptions is the process of encrypting an already encrypted message one or more times, either using the same or a different algorithm. The terms cascade encryption, cascade ciphering, multiple encryption, multiple ciphering and super decipherment have been used in the literature for the similar meaning. Super-encryption refers to the outer-level encryption of a multiple encryption [4].

Under the same key length and for the same size of the processed data, RSA is about several hundred times slower than AES; triple-DES is about three times slower than AES [1]. In cryptography, as the complexity increases in the encryption algorithm, execution time may be increased but it enhances the data security enormously.

Picking any two ciphers, if the key used is the same for both, the second cipher could possibly undo the first cipher, partly or entirely. This is true of ciphers where the decryption process is exactly the same as the encryption process—the second cipher would completely undo the first. If an attacker were to recover the key through cryptanalysis of the first encryption layer, the attacker could possibly decrypt all the remaining layers, assuming the same key has been used for all layers. To prevent that risk, one can use keys that are statistically independent from each layer.

II. Background

Diffie and Hellman have argued that the 56-bit key used in the Federal Data Encryption Standard (DES) is too small and that current technology allows an exhaustive search of the 256 keys. Although there is controversy surrounding this issue, there is almost universal agreement that multiple encryption using independent keys can increase the strength of DES [5].

Manuscript received November 15, 2012; revised January 24, 2013.

Himanshu Gupta is with the Amity Institute of Information Technology, Amity University Campus, Sector – 125, Noida (Uttar Pradesh), India (e-mail: himanshu_gupta4@yahoo.co.in).

Vinod Kumar Sharma is with the Department of Computer Science, Gurukula, Kangri Vishwavidyalaya, Haidwar, India (e-mail: vks_sun@ymail.com).

DOI: 10.7763/IJCTE.2013.V5.765

Multiple encryption a s found in 3DES and AES provides cryptographic assurance of a message's integrity. The simplest approach to increasing the key size is to encrypt twice, with two independent keys $K1$ and $K2$. Letting P be a 64-bit plaintext, C a 64-bit ciphertext, and K a 56-bit key, the basic DES encryption operation can be represented as

$C = S_K\,(P)$, and simple double encryption is obtained as $C = S_{K2}\,[S_{K1}\,(P)]$

While exhaustive search over all mentioned keys ($K1$-$K2$ pairs) requires more operations and is clearly infeasible, this cipher can be broken under a known plaintext attack (where corresponding plaintext and ciphertext are both known) with 2^{56} operations [6]. The time required is therefore no greater than is needed to cryptanalyze a single 56-bit key exhaustively (although there is very significant additional cost for memory). If P and C represent a known plaintext--ciphertext pair, then the algorithm for accomplishing this double encryption encrypts P under all 2^{56} possible values of $K1$, decrypts C under all 2^{56} values of $K2$, and looks for a match. For obvious reasons, this is called a "meet in the middle" attack [7].

Triple DES uses a "key bundle" which comprises three DES keys, K_1, K_2 and K_3, each of 56 bits.

The encryption algorithm is:

ciphertext = $E_{K3}(D_{K2}(E_{K1}(\text{plaintext})))$

I.e., DES encrypts with K_1, DES *decrypt* with K_2, then DES encrypt with K_3.

Decryption is the reverse:

plaintext = $D_{K1}(E_{K2}(D_{K3}(\text{ciphertext})))$

I.e., decrypt with K_3, *encrypt* with K_2, then decrypt with K_1.

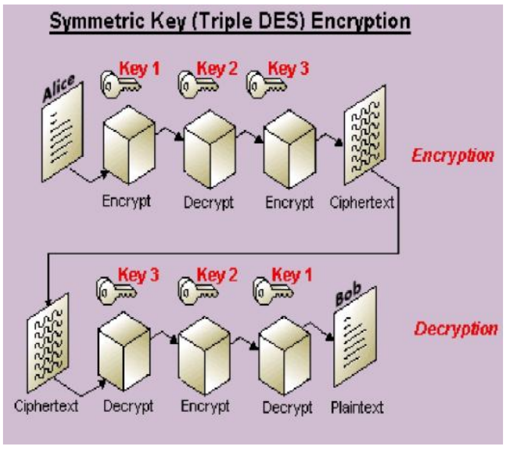

Fig. 2. Description of multiple encryption (triple DES)

In Fig. 2, the whole process of Triple DES is described. Each triple encryption encrypts one block of 64 bits of data. In each case the middle operation is the reverse of the first and last. This improves the strength of the algorithm when using a set of different keys instead of symmetric keys [8].

III. Overview of the Proposed Encryption Technique

This idea differs with existing data encryption techniques to provide network and information security over the wireless network. It may create complexity of data encryption number of times due to performing the same operation multiple times with different encryption key in existing way. As per cryptographic protocol, more and more complexity in data encryption technique enhances the security of data transmission over the wireless channel. Large number of encryption of encrypted data will increase the complexity of data encryption enormously, which will be very complicated to decrypt it.

A. *Example*

Complexity of Existing Encryption Technique / method (Multiple Encryption) = $O\,(N*N*\ldots\ldots\ldots*N)$

Complexity of New (As per proposed idea) Encryption Technique = $O\,(N*N*\ldots\ldots*N)$ * $O\,(N*N*\ldots*N)$ *……………………………* $O\,(N*N*\ldots*N)$.

(Depending upon the multiplicity of the Encryption Technique involved.)

B. *Conventional Encryption Technique (Using Ceaser Cipher Encryption Technique)*

Original Data/ Plain Text – GURUKULA

Algorithm – $C = P + 3$ (Key as Second successor of plaintext)

Cipher Text – JXUXNXOD

C. *Multiple and Multiphase Encryption Technique*

In cryptography, by encrypting a message twice with some block cipher, either with the same key or by using two different keys, then we would expect the resultant encryption to be stronger in all but some exceptional circumstances. And by using three encryptions, we would expect to achieve a yet greater level of security.

For instance, the use of double encryption does not provide the expected increase in security when compared with the increased implementation requirements, and it cannot be recommended as a good alternative. Instead, triple-encryption is the point at which multiple encryptions give substantial improvements in security.

Example:

Original Data/ Plain Text – GURUKULA

Algorithm – $C = ((P + 3) + 3) + 3$ ………… $+ 3)$ (N Times)

Cipher Text –

JKOCPUJW (After First Cycle)

MNRFSXMZ (After Second Cycle)

PQUIVAPC (After Third Cycle)

……………………………………

…………………………………….

Encrypted N Times

In such a way, multiple encryptions will occur in each phase and this process will be repeated number of times up to desired extent. So, multi-phase encryption comprises number of such phases which are strongly protected due to multiple encryption in each phase.

Multi-phase Data Encryption describes the enhanced complexity of data encryption due to performing the same operation multiple times in existing way (single phase encryption techniques).

Example:

Original Data/ Plain Text – GURUKULA

Algorithm – $C = ((P + 1) + 3) + 5$ ………….. (N Times)

Cipher Text –
HVSVLVMB (After First Cycle)
KYVYOYPE (After Second Cycle)
PDADTDUJ (After Third Cycle)
…………………………………….
……………………………………..
Encrypted *N* Times

In such a way, multiple encryption occurs with different encryption keys (encryption algorithms) in each phase of multiphase encryption.

In the single phase of multiphase encryption is described as multiple encryption where at each cycle different encryption key is used. In this encryption technique, decryption will be performed in reverse order. In multiphase encryption, such processes will be repeated number of times to enhance the complexity in encryption/decryption as well as security of data.

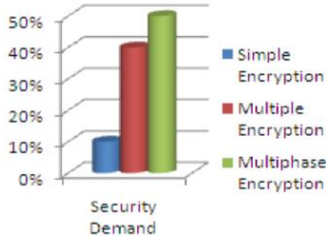

Fig. 3. Security demand of various encryptions

In this figure, as per general survey we can see that the demand of multiphase encryption is increasing day by day in comparison of other simple & multiple encryption techniques to enhance the security in data communication over wireless network.

Applied Cryptography includes the source code for DES, IDEA, BLOWFISH, RC5 and other algorithms [9]. In current scenario, 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.

Cryptographic algorithms and key sizes have been selected for consistency and to ensure adequate cryptographic strength for Personal Identity Verification (PIV) applications [10]. 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.

IV. Conclusion

Multi-phase Data Encryption is an ambivalent technique for data & information security and plays an important role in modern Cryptography. Multi-phase Data Encryption describes the enhanced complexity of data encryption due to multiple operations of single phase encryption techniques in cryptography. 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. The study of multi-phase encryption aims to enhance the potential of upcoming encryption technologies and its implications to defense and government users. The implementation of multi-phase encryption is a strong and positive move in the way of defining a standard for network security. However, as the amount of confidential data communication increases over the insecure wireless network, multi-phase encryption must also be reviewed from a security prospective.

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] J. Heath. Survey: Corporate uses of Cryptography. [Online]. Available: http://www.iinet.net.au/~heath /crypto.html

[3] R. Bose, *Information Theory, Coding and Cryptography*, Second Reprint 2008, the Tata McGraw Hill Publication, pp. 313.

[4] Google Search & Wikipedia Dictionary for Triple DES & relevant topics as well as graphical images (Fig. 2).

[5] R. C. Merkle and M. E. Hellman, "On the security of multiple encryption," *Department of Electrical Engineering, Stanford*, CA published in ACM, A technical note on Programming Technique & Data Structure in Stanford University, vol. 24, no. 7, 1981.

[6] W. Diffie and M. Hellman, "New directions in cryptography," *IEEE Trans. Info*., vol. 22, no. 6, pp. 644-654, Nov. 1976.

[7] P. V. Oorschot and M. J. Wiener, *A Known-Plaintext Attack on Two-Key Triple Encryption*, EUROCRYPT'90, LNCS 473, 1990, pp. 318-325.

[8] W. Diffie and M. Hellman, *Exhaustive Cryptanalysis of the NBS Data Encryption Standard*, June 1977, pp. 74-84.

[9] B. Schneier, "Applied cryptography second edition: protocols, algorithms, and source code in C," *John Wiley and Sons*, 1996, pp. 758.

[10] NIST Special Publication 800-78-2, *Cryptographic Algorithms and Key Sizes for Personal Identity Verification*, February 2010

Himanshu Gupta is a Senior Faculty Member in Amity Institute of Information Technology, Amity University, Noida, India. He is having prestigious membership in various famous and reputed Technical and Research organizations such as CSTA (USA), Computer Society of India (India), TIFR (India), IACSIT (Singapore), UNESCO (Paris) and IEEE Computer Society (USA). With specialization in Network Security & Cryptography. He has successfully filed a patent ―A Technique & Device for Multiphase Encryption‖ under the domain area of Network Security & Cryptography in the field of Information Technology. He has attended many National and International Seminars, Workshops & Conferences and has been presented many research papers in the field of Information Technology. He has visited many countries as Malaysia, Singapore, Bangkok and Cambodia for the academic and research purpose. He has been delivered many technical sessions in the field of ―Network Security & Cryptography‖ in various reputed universities and research organizations as an invited speaker.

Vinod Kumar is associated with teaching and research activities since last 30 years. He is presently working as Professor, Department of Computer Science and Dean, Faculty of Technology, Gurukul Kangri University, Haridwar since last 13 years. He has been Founder Head of the Computer Science Department, Founder Dean, Faculty of Technology and Founder Directorl, College of Engineering and Technology, at GKU Haridwar. Fifteen researchers have already got the degree of Ph.D awarded under his guidance and Eight are pursuing research for their Ph.D. He has published about 75 research papers in various national/ international journal/conferences of repute. He is a member of IEEE, USA and Association of Computing Machinery (ACM), USA. Also, He is a Senior Life Member of Computer Society of India, Life Member System Society of India, Life Member, International Goodwill Society and Life Member of Ramanujan Mathematical Society. He has been Chairman of Haridwar Chapter of Computer Society of India.