ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 7, July 2015

Multi-Round Encryption Algorithm- A Review

Jan Mohd Najar[1], Ashish Sharma[2]

Research Student, Department of CSE, Bells Institute of Management and Technology, Shimla, India[1]

Assistant Professor, Department of CSE, Bells Institute of Management and Technology, Shimla, India[2]

ABSTRACT: The rise of internet and cloud computing have posed a big challenge to the security of sensitive information transmitted over the network and the data stored in various distributed databases. Number of solutions has been provided in the past to secure these resources. This paper will throw light on the past work and proposes a new multi round encryption scheme with variable key length and hidden file format. The additional feature of database security is added to the proposed work to enhance the security of data stored in various online/offline databases.

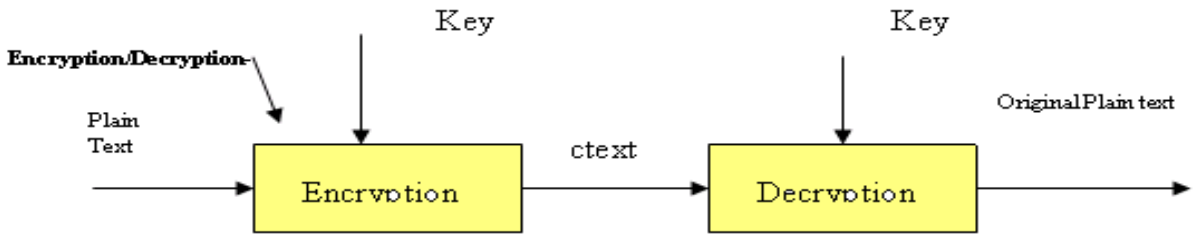
KEYWORDS: multi round encryption, key, file format, database security

I. INTRODUCTION

The advent of distributed networks have made it unsecure to transmit the useful information over it. Transmitting sensitive data as such may result in the huge loss of information and privacy. Cryptography techniques have made it possible to reliably transmit the data from one party to another. These can be of private key cryptography making use of the shared key for encryption as well as for decryption or public key cryptography making use of two different keys for encryption and decryption. The use of various digital signature techniques has enhanced the authenticity of the users.

A. Encryption & Decryption:

The procedure of hiding communication in such a method/s as to conceal its matter is encryption. An encrypted data is cipher-text. The procedure of whirling cipher-text back into plaintext is decryption.



Encryption Procedure

Encryption is used for protected transportations and data storage, mainly for verification of identifications and the communication of subtle data. It can be used throughout a technological environment, including the operating systems, middleware, applications, file systems, and communications protocols.

B. Cryptography Goals:

1. Confidentiality: Information in computer transmitted data is accessible only for reading by authorized parties.
2. Authentication: Origin of message is correctly identified with an assurance that identity is not false.
3. Integrity: Only authorized parties are able to modify transmitted or stored information.
4. Non-Repudiation: Requires that neither the sender, nor the receiver of message be able to deny the transmission.
5. Access Control- Requires access may be controlled by or for the target system.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 7, July 2015

6. Availability: Computer system assets are available to authorized parties when needed.

II. RELATED WORKS

Steven M. Bellovin et.al [1] in 1992 proposed an encryption technique that provides security against dictionary attacks. This technique also protects users having weak passwords. Jacques Patarin et.al [2] in 1995 presented two new types of asymmetric algorithms; Hidden Field Equations (HFE) and Isomorphism of Polynomials (IP). The former one can be used for digital signature and encryption, and the latter is used for signatures as well as for zero knowledge authentications. M Bellare et.al [3] in 1997 discussed the various notions and schemes for symmetric encryption in a concrete security framework providing four different notions of security against chosen plaintext attack. They also discussed the security analysis of various methods to encrypt data using a block cipher in CBC mode. Thomas Wu [4] in 1998 presented a new protocol suitable for authentication of users and key distribution over an untrusted network. The protocol offers high resistance against dictionary attacks used by active or passive intruders. The user passwords are stored in a database in a form other than plain text there by giving tough time to the attackers. This protocol also uses various techniques of zero knowledge proofs thereby improving the performance of the protocol. Eiichiro Fujisaki et.al [5] in 1999 tried to integrate asymmetric and symmetric encryption techniques. The proposed work shows a simple and generic conversion from asymmetric and symmetric encryption techniques into an asymmetric encryption technique which is very strong against chosen cipher text attacks. The conversion can be used efficiently over asymmetric encryption environment. Mihir Bellare et.al [6] in 2000 proposed integrity of plain texts and integrity of cipher texts as two possible notions of authentication over symmetric encryption techniques. The security of encryption scheme is analysed by generic composition using a given encryption technique and a given MAC. Encrypt-and-MAC plain text, MAC-then-Encrypts and Encrypt-then-MAC were three composition methods considered.

S. papadimitrious [7] in 2001 proposed a novel probabilistic symmetric encryption technique based on the chaotic dynamics. The technique makes use of virtual attractors which are created and maintained artificially, each attractor representing a symbol that is used to encode messages. The space is partitioned in the clusters of virtual attractors. These set of states are transferred into cipher text for transmission. Proving the position of the same chaotic system of difference equations, the receiver can perfectly reconstruct this virtual space. Jee Hea An et.al [8] in 2002 presented a new composition method namely commit then encrypt and sign. The proposed scheme applies the digital signature and encryption operations in parallel unlike other generic sequential composition schemes. The technique combines the hash sign switch technique leading to efficient online or offline encryption. John black et.al [9] in 2003 proposed a new encryption technique known as KDM security that is suitable for key dependent messages. The scheme can be used in both public key and shared key encryptions. Phillip Rogaway [10] in 2004 proposed a nonce-based symmetric encryption technique. The scheme makes use of an initialization vector (IV). The user supplies a message m, key k and initialisation vector (IV), getting back the one and only corresponding cipher text. They also explore the various definitions, structures, and properties of nonce-based encryption techniques. Zhi-hong et.al [11] in 2005 proposed a novel image encryption technique. The grey values of image pixels are changed, shuffled in such a way to confuse the relationship between the cipher image and the original image. Arnold cat map technique is used to shuffle the pixel positions in spatial domain. The output of Chen's chaotic system is pre-processed making it suitable for grey scale image encryption and the shuffled image is encrypted by the pre-processed signal pixel by pixel. Reza Curtmola et.al [12] in 2006 proposed a searchable symmetric encryption technique that allows outsourcing its data to the receiver privately, maintaining the ability to selectively search over it. Thomas Eisenbath et.al [13] in 2007 expressed the fact of an increased demand for security for various electronic appliances with the rise of pervasive computing age. Light weight cryptography is the main tool for developing security solutions in case of pervasive devices. However the computational complexity that is inherent in the ciphers poses a major challenge. S. Behniaa et.al [14] in 2008 presented a digital image encryption technique making use of various chaotic systems. The chaotic cryptographic technique used by them is symmetric key cryptography. A typical coupled map is mixed with a one dimensional chaotic map and used for securing image encryption. The proposed scheme is presented in detail along with crypt analysis and implementation. Alexandra Boldyreva et.al [15] in 2009 proposed order preserving symmetric encryption technique for allowing efficient range of queries on an encrypted data stored in a database. The proposed technique makes use of pseudo random functions making it as random as possible subject to the order preserving constraint. They deigned an efficient ope scheme and verified its security under pseudo randomness of an underlying block cipher.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 7, July 2015

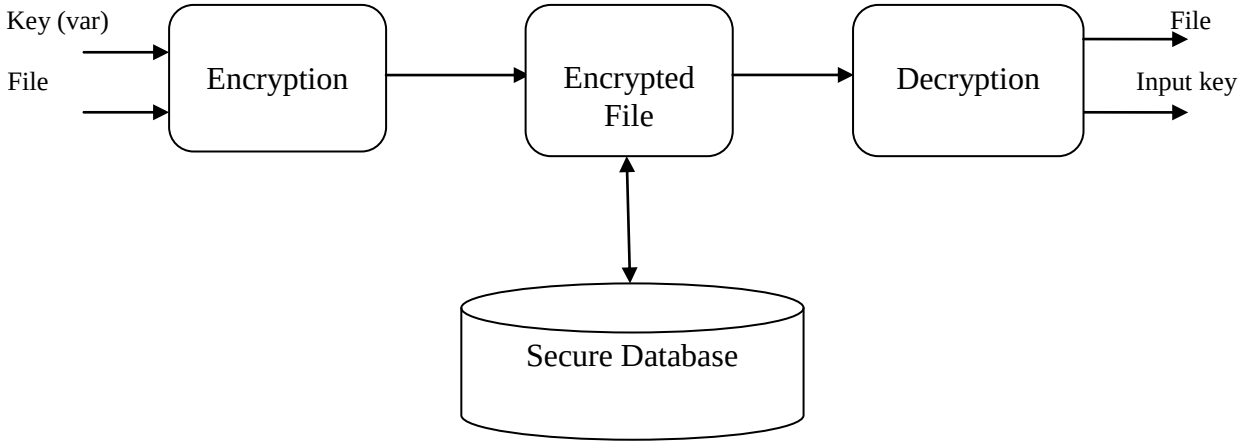
Diaa Salama Abd Elminaam et.al [16] in 2010 evaluated the performance of various symmetric encryption algorithms. The impact of growing distributed environment poses a challenge in securing the Applications that run over it. Although encryption techniques are fruitful for security systems, but consume various system resources like CPU time, memory and battery power. The proposed work evaluates six most common used encryption algorithms; AES, DES, 3DES, RC2, Blowfish and RC6. Crypt analysis has been carried out on these algorithms to demonstrate their respective effectiveness. Jawahar Thakur et.al [17] in 2011 emphasised the security needs with the rising internet and network applications. The paper provides a comparison between three symmetric key algorithms namely DES, AES and blow fish. A comparison is made among these algorithms based on the parameters of speed, block size and key size.

III. PROPOSED ALGORITHM

We intend to propose multi round encryption algorithm with variable length key. The strength of this work will be with variable length key & concealed file format. The source file is encrypted into text file, thus at the time of decryption user has to provide as into what format the file is to be decrypted into. For example;

a. The source file is a.doc.
b. a.doc is encrypted and saved as a.txt with a.doc is deleted
c. At the time of decryption user has to provide key & file format e.g .doc, .pdf, .exe etc.

This adds to the complexity of the algorithm.
Subsequently work (algorithm) will be tested on various file format/s and comparative analysis will be performed on existing algorithms eventually crypt analysis will be performed on the said algorithm. The diagrammatic representation of the proposed work is as;



Encryption and Decryption process

A. Objectives:

1. Analyse and compare various existing encryption approaches.
2. Propose a new multi round key based encryption algorithm, develop same in high level language
3. Test proposed technique on different file formats with varying key length.
4. Providing database security.
5. Subsequently perform crypt analysis on proposed technique.

IV. CONCLUSION AND FUTURE WORK

A multi round encryption scheme with variable key length will be proposed to provide high security to the data. Database security as an additional feature will be added to the proposed technique to secure databases. The technique uses hidden file format giving hard time to the attackers. The work will be implemented using java technology.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 7, July 2015

REFERENCES

1. Steven M. Bellovin & Michael Merritt, "Encrypted key exchange: password-based protocols secure against dictionary attacks", Research in Security and Privacy, 1992. Proceedings., 1992 IEEE Computer Society Symposium
2. Jacques Patarin "Hidden Fields Equations (HFE) and Isomorphism's of Polynomials (IP): Two New Families of Asymmetric Algorithms", Advances in Cryptology — EUROCRYPT '96, Lecture Notes in Computer Science Volume 1070, 1996, pp 33-48
3. M Bellare, A Desai, E P Rogaway, P.A concrete security treatment of symmetric encryption, Foundations of Computer Science, 1997. Proceedings. 38th Annual Symposium.
4. Thomas Wu,'' The secure remote password protocol (1998) '' , Computer science Department Stanford university, November 11, 1997.
5. Eiichiro Fujisaki, Tatsuaki Okamoto, **"**Secure Integration of Asymmetric and Symmetric Encryption Schemes**",** Advances in Cryptology — CRYPTO' 99, Lecture Notes in Computer Science Volume 1666, 1999, pp 537-554.
6. Mihir Bellare & Philip Rogaway, "Optimal asymmetric encryption", Advances in Cryptology- Eurocypt'94 Lecture Notes in Computer Science Volume 950, 1995, pp92-111.
7. S. Papadimitrious, "A Probabilistic Symmetric Encryption Scheme for very fast secure communication based on Chaotic Systems of different equations'', Int. J. Bifurcation Chaos 11, 3107 2001.
8. Jee Hea An, Yevgeniy Dodis, & Tal Rabin "On the Security of Joint Signature and Encryption", Advances in Cryptology — EUROCRYPT 2002Lecture Notes in Computer Science Volume 2332, 2002, pp 83-107
9. John Black, Phillip Rogaway, &Thomas Shrimpton, "Encryption-Scheme Security in the Presence of Key-Dependent Messages ", Cryptography Lecture Volume 2595, 2003, pp 62-75
10. Phillip Rogaway, "Nonce-Based Symmetric Encryption, Fast Software Encryption" Lecture Notes in Computer Science Volume 3017, 2004, pp 348-358.
11. Zhi-Hong Guana,, FangjunHuanga, & WenjieGuanb, "Chaos-based image encryption algorithm", Physics Letters A, Volume 346, Issues 1–3, 10 October 2005, Pages 153–157
12. Reza Curtmola, Juan Garry, Seny Kamara and Rafail Ostrovsky," Searchable Symmetric Encryption" Lecture Notes in Computer Science Volume 5476, 2006.
13. Sandeep Kumar , ChristofPaar , Axel Poschmann , & Leif Uhsadel , "A Survey of Lightweight-Cryptography Implementation ", Design & Test of Computers, Issue No.06 - November-December (2007 vol.24).
14. S. Behniaa, A. Akhshania, H. Mahmodia, & A. Akhavanb, "A novel algorithm for image encryption based on mixture of chaotic maps", Fractals Volume, January 2008, Pages 408–419.
15. Alexandra Boldyreva, Nathan Chenette, Younho Lee, &Adam O'Neill, "Order-Preserving Symmetric Encryption", Advances in Cryptology - EUROCRYPT 2009 , pp 224-241
16. Diaa Salama Abd Elminaam, Hatem Mohamed Abdul Kader & Mohiy Mohamed Haldoud , Evaluating The Performance of Symmetric Encryption Algorithms, International Journal of Network Security , Vol. 10, No. 3, PP.213-219, May 2010.
17. Jawahar Thakur, Nagesh Kumar, "DES, AES and Blowfish: Symmetric Key Cryptography Algorithms Simulation Based Performance Analysis", International Journal of Emerging Technology and Advanced Engineering, , Volume 1, Issue 2, December 2011.