IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

An Review To Multi-Level Encryption

[1]Satyander, [2]Shalini Bhadola, [3]Kirti Bhatia

[1]M.Tech Student, [2]Assistant Professor, [3]Assistant Professor
Computer Science and Information Technology,
Sat Kabir Institute Of Technology & Management, Bahadurgarh, Haryana, India

Abstract : In this era, the most important thing for user as well as for an organization is network security where data of most of companies/organization is stored on clouds. So we must have to find a solution so that data must be safe during network transmission. In this regards most efficient way is to encrypt the data which we transmit from source to destination. Then at destination again decrypt the original data form encrypted data. Some of the data is more critical like some government data or military communication, banking transactions etc.. When data falls in wrong hand may leads to big devastating.

In this paper, a solution for above situation a multi-level encryption is given. In this multilevel encryption, data is more secure than the conventional encryption which involves multiple rounds of encryption with same or different keys and this make the algorithm complex and more powerful.

Index Terms **- Cryptography, Encryption, Decryption, private-key, public-key, RSA, AES, Multilevel Encryption.**

I. INTRODUCTION

Data security is importance in present time as lots of information is being communicated via network. A suitable methodology for privacy transformation is best to make a data protected over network. Different methods are implemented in order to protect the sensitive data. Now a days most of the data is secured by the technique of encryption and certificates. Most of methods are based on cryptography technique.

Multi-level encryption is a new concept that is used for making the system more secure than existing cryptosystems. Multi level encryption is the process of encrypting the plain text with one or more time with same of different no of keys. It makes the process more complex and powerful than existing.

II. CRYPTOGRAPHY AND TYPES

Cryptography: It is a technique to which information is send in a secure manner so that only authorized user is able to receive this information. It refers to the scrambling of the data and make it meaningless for the third party during transmission

There are three basic components of cryptography system

- **Plain text** : Source / information/data / original message
- **Key** : Necessary for encryption process.
- **Cypher text** : Unrecognized data /encrypted data / encrypted message

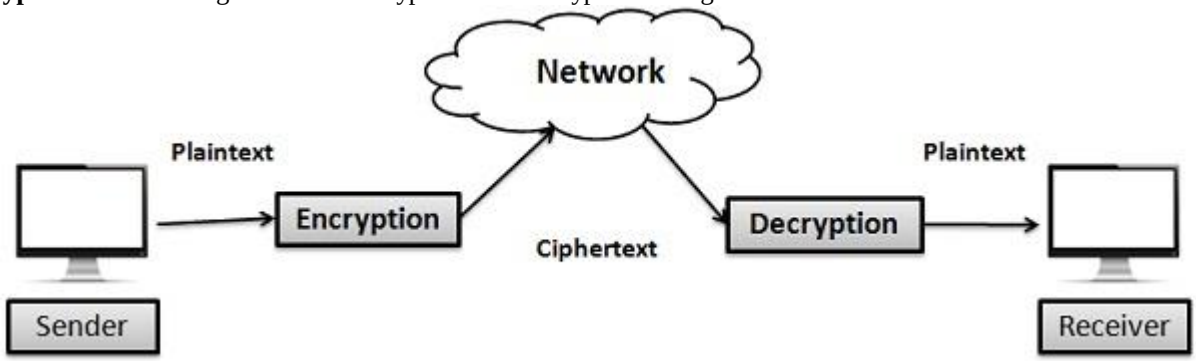

Fig 1: Encryption Decryption Process

The original text is encoded with encryption algorithm. This process called as encryption. The reverse process to get back the encrypted data into plain text by using decryption algorithm. This process is called decryption. Decryption process is the reverse of encryption.

Objectives of cryptography are:

- **Confidentiality :** Confidentiality means to the keep information secret / private.
- **Data integrity :** It ensure accuracy and consistency (validity) of data over its lifetime.
- **Authentication :** It ensure that data is genuine and verified at any stage and completely trustworthy.

Of course, the algorithm requires the key to be kept secret or long enough so that it takes even longer to break. For example, a 40-bit key has one trillion combinations whereas a 128-bit key has 3.4*1026 trillion combinations [1]. There are two types of key-based algorithms i.e Symmetric and Asymmetric.

Symmetric Key Algorithms, also known as private-key / conventional / secret-key algorithm. It require that sender and receiver uses a single key before they start communicate securely. In this type of algorithms, the encryption key used for encryption and the decryption key used for decryption are the same and security of information depends on the degree of key secrecy from the unauthorized user / intruders.

During the transmission key must remain secret. Encryption process can be done like $ENCRYPTION_{KEY}$(MESSAGE) = CIPHER TEXT and Decryption processes as: $DECRYPTION_{KEY}$(CYPHER TEXT) = MESSAGE respectively. This method is extremely fast and efficient. It also provides integrity and confidentiality. But it fails to provide authentication. [2][3][4].

Asymmetric key algorithm, also known as public-key algorithms which operate with public encryption key and private decryption key. Encryption key is made public and any sender can use the key to encrypt the message, but only a authorized user can use the private key (decryption key) to decrypt the ciphertext. There are some example which are based on this type of algorithms like RSA, Rabin and Elgamal [1][2][4]. Asymmetric algorithms are hard to implement and require significant processing power due to fundamental mathematical operations such as modulus. In this paper we will talk about the AES and RSA algorithm and their implementation in multilevel security layers which will be fast and as much more secure than existing AES and RSA.

Proposed Multi-level encryption can work better compared to single encryption. Multi-level encryption involved the encryption of a message single or multiple times by using one algorithm with same key or same algorithms with different keys or by using different algorithms[13]. But the proposed algorithm works faster and provide extra security to data in an efficient manner. Not all algorithm with multiple computations are always better but an efficient algorithm can provide same layer of security in faster way.

III. Related Work and Implementations

The idea of multi-level encryption is used for both symmetric and asymmetric encryption is not a new approach. Security is always a prime issue for purchase researchers and experimenters. There are some implementations done by researchers using hybrid approach as well as multi level cryptography approach.

There are lot of approaches which uses the same technique for multi-level encryption.

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.[11]

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).

Original Data/ Plain Text – GURUKULA
Algorithm – $C = ((P + 1) + 3) + 5$ …….. (N Times)
International Journal of Computer Theory and Engineering, Vol. 5, No. 4, August 2013
639
Cipher Text –
HVSVLVMB (After First Cycle)
KYVYOYPE (After Second Cycle)
PDADTDUJ (After Third Cycle)
…….
……..
Encrypted N Times

Multi-Level Cryptography Algorithm (Multi-Prime RSA and DES) : Multi-level cryptography was implemented using DES and RSA, and subsequently using DES and Multi-prime RSA. [13][14].

Encryption algorithm :

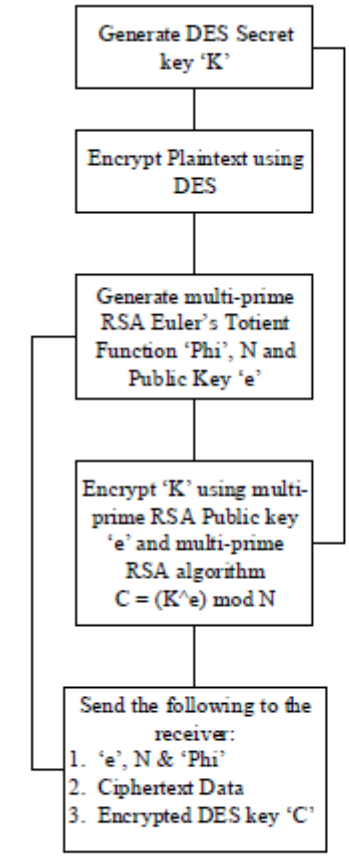

Fig.2. Multi-Level Encryption on Sender Side.

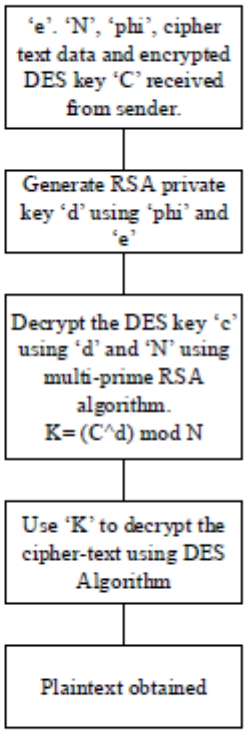

Fig.3. Multi-level Decryption on Receiver Side.

- Generate DES Secret key. (Since DES is a symmetric key algorithm, only one key is generated and shared).
- Use this Secret Key to encrypt the plaintext data using DES.
- Generate RSA Public Key 'e' and (Euler's Totient function), product of primes N.
- Use this key to encrypt the DES Secret Key using the RSA algorithm.
- The following information is shared with the receiver.

Decryption algorithm :

- Generate the private key 'd' using ϕ and 'e'.
- Use this key to decrypt the DES secret key using RSA.
- The secret key thus obtained is then used to decrypt the cipher-text data using DES.

Hybrid Algorithm with DSA, RSA and MD5 : Khushdeep Kaur, Er. Seema proposed a new approach by combining DSA, RSA and MD5 algorithm as a hybrid link for wireless devices. This is very efficient and secure hybrid algorithm for providing security to mobile nodes. They tested their proposed algorithm with different scenarios and it is providing better response time, less network delay and best throughput. The hybrid algorithm provides better results than other algorithms. This algorithm can be implemented to mobile nodes for security purposes. Also our research shows that it is helping in efficient routing of packet with much less load on servers. [15]

Dual RSA : Dual RSA have been introduced by sun et al. In dual RSA two instances of RSA will share the same public and private key exponents. So it will reduce the memory requirements required for storing both keys because both key exponents are same. Twin RSA is also used to reduce storage requirements. Here there are two different RSA instances such as T1=r1s1, T2=r2s2. As usual we have public key (e) and private key (d). These keys should satisfy the following equations such that ed≡1 mod Ø (T1) and also ed≡1 mod Ø (T2) [16].

RSA algorithm with modified keys exchange : Sami A. Nagar and Saad Alshamma speedup the RSA algorithm through a new generation keys method called RSA-Key Generations Offline to generate and save all keys values in tables within database. They proposed four security levels, in which each level has its own database and numbers of sets, these levels identified according to the e values and key length, before using the RSA algorithm between gateways must get a Ready Acknowledgment from RSA Handshake Database protocol, this protocol is responsible for creation or update the identical gateways database, level selections and establishment the algorithm between gateways. Nagar and Alshamma proposed a new method of keys exchange to increase the difficulty for any one knows the exchanged values between gateways, and then try to get the n, e and d values, This approach was known as Concept of Keys Exchange, where algo exchanges the indexes Nid, Eid, Did instead of n, e, d values.

Concept of Kth Residue : Wang Rui, Chen Ju, Duan Guangwen developed k-RSA algorithm in which the idea of kth power residue theory and RSA algorithm were combined. This algorithm not only inherits the advantage of RSA, whose security depends on the difficulties of factoring large integers and finding discrete logarithms, but also had high flexibility of parameters. It is designed for improved security and had agreed balance between speed and space. At the same time, it can realize functions like hierarchical system management, secret sharing and so on. The result shows that, in k-RSA algorithm d is smaller than e. And that's why new algorithm can largely reduce the computation time of decryption. [18].

Rebalanced RSA : Rebalanced RSA introduced by Wiener in 1990 used to give the good improvement in RSA decryption and also encryption. Normally we have to choose the small public key exponent [8]. But we should not choose the small private key exponent because it is unsafe. So here's wiener is mainly discuss the

weak spot of the use of the private exponent in algorithm .In this algorithm public exponent e is very smaller than the modulus, so automatically it will reduce the encryption costs when we are going to maintain low decryption costs. If we choose a private exponent L so that both Lr and Ls are small. So Rebalanced RSA is mainly used to balance encryption time and decryption time. It is also used to balance the cost and also the memory. Rebalanced RSA reduces the overall cost of encryption and decryption process and rebalance the difficulty of encryption and decryption. It is well suitable for many practical applications. It is just like the same calculation that is done in RSA-CRT for encryption and decryption. The only difference is that we modify this algorithm by choosing the public exponent much smaller than Z can be used [17].

DES, RSA, Hybrid algorithm : A framework for data security was proposed in 2016, where separate frames were designed for client and server. A user registration process was included on the server side for authorization. The approach included 3 phases to be applied on the data, namely, DES, RSA, Hybrid algorithm. The keys that were used in the last step were string, modulus, private, public and integer key [9].

Hybrid Crypto Hardware Utilizing Symmetric-Key and Public-Key Cryptosystems : Another approach was proposed for combining symmetric and public key methods in 2012. Again, AES and DES were used for data encryption and RSA was used for key exchange. The system comprising of many modules was modelled using Verilog HDL using Mdel Sim SE 5.7e. It also consisted of a pseudorandom number generation unit for the key generation process in addition to a GCD computation unit to be used in the RSA algorithm [10].

IV. CONCLUSION

Multiple encryption is used for better security with the help of different combination of multiple algorithms. In multiple / multi-level encryption, if some cipher are broken still it ensures the confidentiality of data which can be maintained by multiple encryptions. In multi-level encryption its primary task is to provide security as well as confidentiality of data. Case study of different type of multilevel encryption gives the idea and positive aspect toward a new hybrid approach. it also maintain the standard for network security also can be used in different ways like password protection for any application. implementation of these type of algorithms can be used in the field of technology, banking, defence, government officials website for ensuring security.

Multilevel data encryption is a technique which ensures the secrecy and privacy of data and information. it creates complexity in data encryption algorithm due to multiple operations. These operations can be in single phase or multiple phase. These operation can be encrypted with single key or multiple keys during each round of encryption and provide enormous complexity in data encryption.

V. FUTURE SCOPE

Now a days a large no of attacks increases needs for secure communications. So a more secured cryptographic algorithm needs to be proposed and implemented. The multi-level encryption can be widely used in most of the applications. Future work will focus on investigating and implementing a countermeasure against the multilevel implementations and their performance. Also try to prevent vulnerabilities attacks and develop more secure system.

VI. REFERENCES

[1] J. E. Soric, "*Cryptography Honors Project*," http://cs.bluffton.edu/~jsorice/projects/cryptography.

[2] Bruce Schneier, *Applied Cryptography*, 2nd ed., John Wiley and Sons, Inc. 2001.

[3] Paul C. Van Oorschot, and Scott A. Vanstone, Alfred J. Menezes, *Handbook of Applied Cryptography*, CRC Press 1997.

[4] Harry Katzan Jr., *The Standard Data Encryption Algorithm*, Petrocelli Books, 1997.

[5] Himanshu Gupta, Vinod Kumar Sharma, "*Multiphase Encryption: A New Concept in Modern Cryptography*", IJCTE, Vol 05, No 4, 2013.

[6] Shashikant Kuswaha, Praful B. Choudhary, Sachin Waghmare, Nilesh Patil," *Data Transmission using AES-RSA Based Hybrid Security Algorithms*" IJRITCC, Vol 3, No 4, 2015

[7] Zhang Hanli Zhaohui, Yuan Kun, "*An Improved AES algorithm based on chaos*", Multimedia Information Networking and Security, International conference 2009.

[8] Aida Janadi, "*AES immunity Enhancement against algebraic attacks by using dynamic S-Boxes*", ICTTA 2008.

[9] Smita Chourasia, Kedar Nath Singh "*Information Systems Design and Intelligent Applications*" Springer, New Delhi, 2016

[10] Farhan Abdul-Aziz Khan, Adnan Abdul-Aziz Gutub, "*Hybrid Crypto Hardware Utilizing Symmetric-Key and Public-Key Cryptosystems*" International Conference on Advanced Computer Science Applications and Technologies – ACSAT2012 .

[11] Himanshu Gupta and Vinod Kumar Sharma "*Multiphase Encryption: A New Concept in Modern Cryptography*" IJCTE, Volume 5, Number 4, August 2013.

[12] W. Diffie and M. Hellman, "*New directions in cryptography*", IEEE Transactions on Information Theory,Volume 22 , Issue: 6 , November 1976

[13] Rivest, R. L., Shamir, A., Adelmann, L.: "*A method for obtaining digital signature and public –key cryptosystems*", Commun. ACM, 1978, VOL. 21, pp. 120-126.
[14] Chourasia S., Singh K.N.," *An Efficient Hybrid Encryption Technique Based on DES and RSA for Textual Data*". In: Satapathy S., Mandal J., Udgata S., Bhateja V. (eds) Information Systems Design and Intelligent Applications. Advances in Intelligent Systems and Computing, vol 433. Springer, New Delhi.
[15] Kaur, Khushdeep, and Er Seema. "*Hybrid Algorithm with DSA, RSA and MD5 Encryption Algorithm for wireless devices*" IJERA, 2.5 (2012): 914-917
[16] H.M. Sun, M.E. Wu, W.C. Ting, and M.J. Hinck, "*Dual RSA and its Security Analysis"*, IEEE Trans. On Information Theory, vol.53, no.8, pp. 2922-2933, August 2007.
[17] H. M. Sun, M.J. Hinek, and M.-E. Wu, "*On the design of Rebalanced-RSA, revised version of Centre for Applied Cryptographic Research*", Technical Report CACR 2005-35, 2005.
[18] Wang Rui; Chen Ju; Duan Guangwen, "*A k-RSA algorithm*," ICCSN, 2011 IEEE 3rd International Conference on, vol., no., pp.21, 24, 27-29 May 2011