www.ijecs.in
International Journal Of Engineering And Computer Science ISSN: 2319-7242
Volume 5 Issues 7 July 2016, Page No. 17148-17151

A Review on RSA Encryption Algorithm

Shaina Garg[1], Dr. Mukesh Kumar Rana[2]

[1]Kurukshetra University, Haryana College of Technology and Management,
Ambala Road, Kaithal, Haryana, India
shainagarg29@gmail.com

[2] Kurukshetra University, Haryana College of Technology and Management,
Ambala Road, Kaithal, Haryana, India
Mukesh_rana09@rediffmail.com

Abstract: ***The protection afforded to an automated information system in order to attain the applicable objectives of preserving the integrity, availability and confidentiality of information system resources is called computer security. Integrity of a message should be preserved as it travels from the sender to the recipient, it is compromised if the message is modified during transit. The principle of availability states the resources should be available to authorized parties at all times. The principle of confidentially specifies that only the sender and the intended recipient should be able to access the contents of a message. Data security is a very vital thing to ensure the privacy of a user from others. For an organization, it is very necessary to keep the information safe from various attackers. Computer and network security is a battle of wits between a perpetrator who tries to find holes and the designer or administrator who tries to close them. Strong encryption algorithms can be used to make it impossible for an attacker to attack the node that is strongly protected by multiple keys. This work is focused on the use of dynamic keys for securing the data and for securing data transmission.***

Keywords: Security, Plain Text, Cipher Text, Encryption, Key, Decryption.

1. Introduction

Cryptography is the science of using mathematics to encrypt and decrypt data. It enables to store sensitive information or transmit it across insecure networks so that it cannot be read by anyone except the intended recipient.

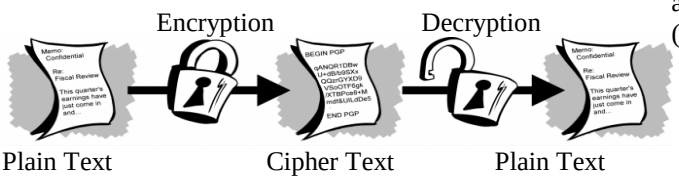

Fig 1: Encryption and Decryption

It is divided into two groups that are (i) symmetric (Private key cryptography) and (ii) asymmetric (Public key cryptography). Symmetric encryption is a form of cryptosystem in which encryption and decryption are performed using the same key. In this scheme, only one key is used and the same key is used for encryption and decryption of messages. Both the parties must agree upon the key before any transmission begins and nobody else should know about it. Various examples of symmetric algorithms are: Data Encryption Standard (DES), Advanced Encryption Standard (AES), International Data Encryption Algorithm (IDEA) etc.

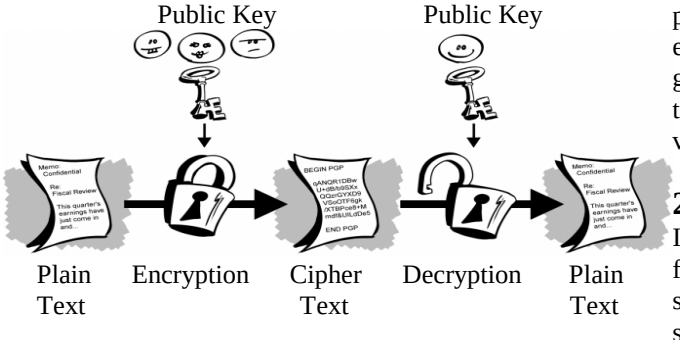

Fig 2: Private Key Encryption

Asymmetric encryption uses a pair of keys for encryption: a public key, which encrypts data, and a corresponding private, or secret key for decryption. No other key can decrypt the message, not even the original key used for encryption. The beauty of this scheme is that every communicating party needs just a key pair for communicating with any number of other communicating parties. Various examples of asymmetric algorithms are: Ronald Rivest, Adi Shamir and Len Adleman (RSA) etc.

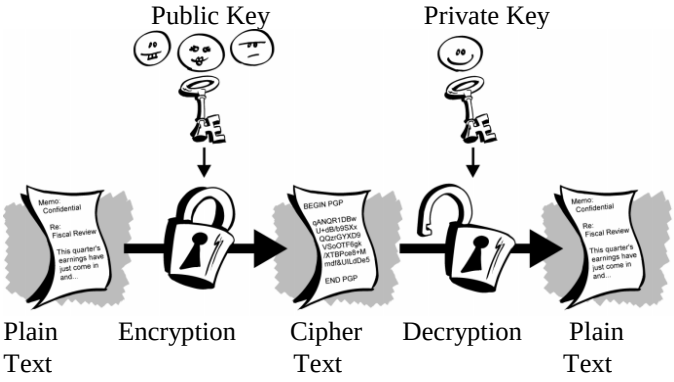

Fig 3: Public Key Encryption

Data that can be read and understood without any special measures are called plain text. The method of disguising plaintext in such a way as to hide its substance is called encryption. Encrypting plain text results in unreadable gibberish called cipher text. The process of reverting cipher text to its original plain text is called decryption. The word or value which is used for encryption/decryption is called key.

2. Literature Survey

In this section the work done by the various researchers in the field of cryptographic algorithm for data security. From this survey various gaps have also been drawn and defined in section 3.

Elisa Bertino [1] explained the challenges, concept and approaches of database security. Many concepts regarding database security were provided and most significant techniques were discussed which were based on accessing control system. He defines the key access control models which were mandatory access control models and the role-based access control (RBAC) model. He also described security for advanced data management systems. The major drawback was that a new device was to be issued, when an individual user required to change the subscription.

Hua Li [2] *et al*. explained new compact dual-core architecture used in AES. The practice of using a new compact architecture started that consisted of two independent cores that practice encryption and decryption simultaneously. In order to provide round keys for encryption and decryption, proposed key generation unit with 32-bit data path was explored. The concept used to implement shift rows was the important design which helps to increase the encryption time. The major limitation was that in comparison to the other designs, this design also requires fewer more hardware resources.

H. C. Williams [3] modified the RSA public-key encryption algorithm. He suggested that if the encryption procedure was broken into a certain number of operations than remainder used as modulus could be factored after few more operations. This technique was in similar appearance to RSA so as produce digital signatures. The main limitation of this scheme was that very large prime numbers were used and generated mathematical errors were observed.

Adam J. Elbirt [4] *et al.* explained the AES block cipher algorithm using FPGA based kit. They proposed that for hardware implementations of encryption algorithms, reprogrammable devices were the best choice. The disadvantage was that when the implementation size was increased then the number of rounds unrolled also enhanced and this increase was partially offset by the packing of the round keys within the round structure.

Hung-Yu Chien [5] highlighted an efficient time bound hierarchical key assignment scheme. They proposed a tamper resistant device that has a new time bound key assignment scheme. It significantly improves the computational performance and reduces the implementation cost as well.

Taher Elgamal [6] proposed a signature scheme based on discrete logarithms and implemented Diffie-Hellman key distribution scheme that achieves a public key cryptosystem. The security of both systems depends on the difficulty of computing discrete logarithms over finite fields.

Martin E. Hellman [7] extended the shannon theory approach to cryptography. He discussed about Shannon's random cipher model which was conservative than in such case when a randomly chosen cipher was considered, the security falls significantly. The concept of matching a cipher to a language and the trade-off between local and global uncertainty were also developed. The limitation of this approach is that it is not directly applicable to designing practical cryptographic systems.

Jason H. Li [8] *et al.* worked on scalable key management and clustering scheme for secure group communication in *Adhoc* and WSN. They describe scalable key management and clustering to achieve more secured system. The scalability problem was solved by partitioning communicating devices into subgroups with a leader in each subgroup. The Distributed Efficient Clustering Approach (DECA) provided robust clustering to form subgroups. Analytical and simulation results pinpoint the fact that DECA was energy efficient and resilient against node mobility. This scheme was not suitable for large cluster size.

Hung-Min Sun [9] *et al.* proposed dual RSA algorithm and also did the acute analysis of the security of the algorithm. Dual RSA was a variant of RSA which is helpful in some specific situations that require two instances of RSA with the advantage of reducing the storage requirements for the keys. The main drawback of using dual RSA was that the computational complexity of the key generation algorithms was also optimised.

Mao-Yin Wang [10] *et al.* configured single and multi-core AES architectures for flexible security. According to them the major building blocks for the architecture of AES was a group of AES processors. Each AES processor provides a block cipher scheme with a novel key expansion design approach for the original AES algorithm. In this multi core architecture the memory controller of each AES processor was designed for the maximum overlapping between data transfer and encryption and thus reducing interrupt handling load of the host processor.

Tomasz Rams *et al*. [11] surveyed a group key distribution scheme with self-healing property. They analyzed and compare the most significant key distribution schemes by looking at the selective key distribution algorithms, at the redistributed secret data management, and the self-healing mechanisms. Limitation of the self-healing techniques adds some redundant information to the broadcast message so as to allow user nodes to recover previous session keys which were lost due to communication errors.

Zhiguo Wan *et al.* [12] worked on hierarchical attribute based solution for flexible and scalable access control in cloud computing. They proposed hierarchical attribute-set-based encryption by extending cipher text policy attribute-set-based encryption with a hierarchical structure of users. The proposed scheme not only achieves scalability due to its hierarchical structure but also inherits flexibility. It employed multiple value assignments for access expiration time to deal with user revocation more efficiently than existing schemes.

Yang Li *et al.* [13] worked on New Fault-Based Side-Channel Attack called fault sensitivity analysis attack Using Fault Sensitivity. They explained the successful FSA attacks against three Advanced Encryption Standard hardware implementations, where two of them were resistant to the differential fault analysis. They also discussed the countermeasures against the proposed FSA attacks.

Chong Hee Kim *et al.* [14] improved differential fault analysis on AES key schedule. Proposed advanced encryption standard for which the main target is known DFA. Implementation of AES is known to be vulnerable to DFA which could be split into two categories depending on the fault location that has the DFA on the state and the DFA on the key schedule. The major limitation is that if the key schedule is not redone for

recomputation then it cannot prevent DFA on the AES Key Schedule. The major problem was that if the key schedule was not done again for recomputation then it cannot prevent DFA on the AES Key Schedule.

Shengrong Bu *et al.* [15] worked on Distributed Combined Authentication and Intrusion Detection with Data Fusion in High-Security Mobile Ad Hoc Networks. Multimodal biometrics was deployed to work with intrusion detection systems to alleviate the short comings of unimodal biometric systems. Each device in the network had measurement and estimation limitations, Observations of each device were fused and more than one device could be chosen using Dempster-Shafer theory for data fusion. Combining continuous authentication and intrusion detection could be an effective approach to improve the security performance in high-security MANETs.

L.J. Garcia Villalba *et al.* [16] securely extended optimized link state routing protocol. Their study presented an extension of OLSR called COD-OLSR that provides security for OLSR in case of incorrect message generation attacks which can occur in two forms. This was one of its main features and was taken into account for current topology of node sending the message. The behavior of COD-OLSR against different attackers in a variety of situations is evaluated.

Ho Won Kim *et al.* [17] designed and implemented a private and public key crypto processor and its application to a Security System. A special-purpose microprocessor was optimized for the execution of cryptography algorithms. This crypto processor could be used for various security applications such as storage devices, embedded systems, network routers, security gateways using IP Sec and SSL protocol, etc. They had presented the design and implementation of a crypto processor composed to a 32-bit RISC processor and coprocessor blocks dedicated to the AES, KASUMI, SEED, triple- DES, ECC and RSA crypto algorithms.

3. Gap in study

The following observations have been drawn from the literature survey and are listed below:

a) Single key of short length is not capable to provide secured cryptographic model.
b) Long length key can be able to provide secured cryptographic model.
c) In order to keep all the primitives in limit optimized hardware is required.
d) Use of dynamic keys are preferred for encryption process.
e) There is a need to optimize the key arrangement in order to achieve secured cryptographic model.

4. Results and Discussion

Problem Formulation: There are some specific problems with RSA. One of the problems with RSA is factoring because if M is factored then it is really feasible and quite easy to find private key. So, keeping in mind we proposed modified RSA.

Proposed work is stated below.

1. Select four prime numbers i, j, k and l at random.
2. Multiply i, j, k and l which come up with M.
3. Choose a number relatively prime to Y and call it d.
 Where Y = (i-1)(j-1)(k-1)(l-1).
4. Find e such that e*d = 1 mod Y.
5. Public Key is (m, e).
6. Private Key is (m, d).
7. Cipher Text = power (PT, e) mod (m).
8. Plain Text =power (CT, d) mod m.

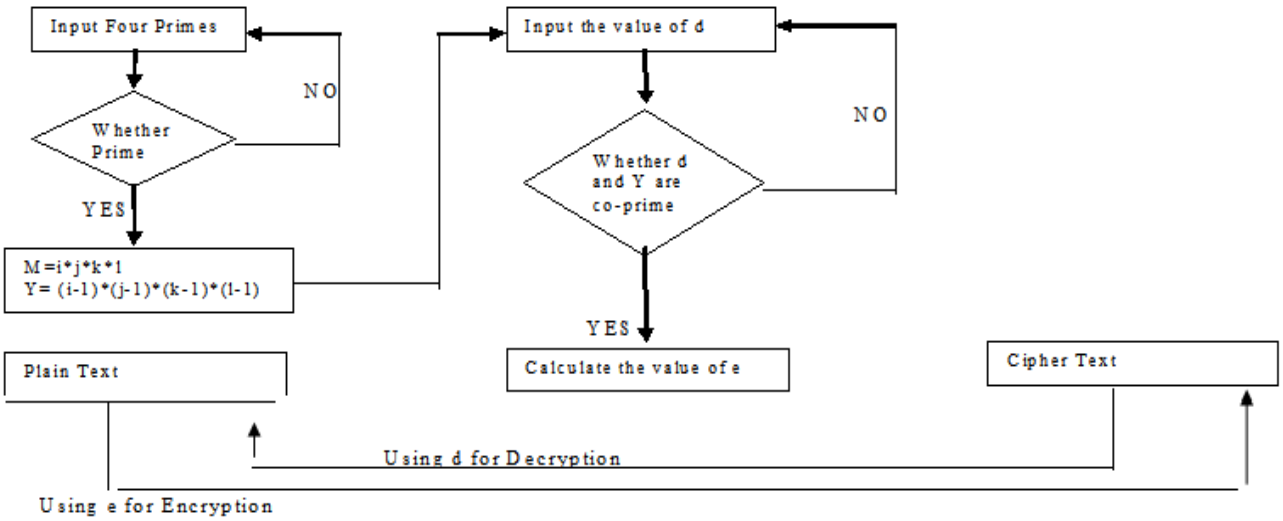

Fig 4: Flowchart of Proposed Algorithm

Conclusion and Future Scope

After studying various encryption algorithms it is found that the strength of the algorithm depends on the length of the key. As the key length is increased the security of algorithm is also increased but performance degrades and vice-versa. To avoid this we have to optimize the key length. After critically analyzing RSA it is found that there are some flaws in it and to overcome these flaws a new algorithm has been proposed. The proposed algorithm increases the security of the system and also reduces the computation time. In future work can be carried out to decrease the complexity of the algorithm.

References

[1] E. Bertino, N. Shang and S. S. Wagstaff, "An Efficient Time-Bound Hierarchical Key Management Scheme for Secure Broadcasting", IEEE Transactions on Dependable and Secure Computing, Vol. 5, No. 2, pp. 65-70, 2008.

[2] Hua Li and J. Li, "A New Compact Dual-Core Architecture for AES Encryption and Decryption", IEEE Canadian Journal of Electrical and Computer Engineering, Vol. 33, No. 3, pp. 209-213, 2008.

[3] H. C. Williams, "A Modification of the RSA Public-Key Encryption Procedure", IEEE Transactions on Information Theory, Vol. 26, No. 6, pp. 726-729, 1980.

[4] A.J. Elbirt, W. Yip, B. Chetwynd and C. Paar, "An FPGA Based Performance Evaluation of the AES Block Cipher Candidate Algorithm Finalists", IEEE Transactions on Very Large Scale Integration (VLSI) Systems, Vol. 9, No. 4, pp. 545-557, 2001.

[5] H. Chien, "Efficient Time-Bound Hierarchical Key Assignment Scheme", IEEE Transactions on Knowledge and Data Engineering, Vol. 16, No. 10, pp. 1301-1304, 2004.

[6] T. Elgamal, "A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms", IEEE Transactions on Information Theory, Vol. 31, No. 4, pp. 469-472, 1985.

[7] M. E. Hellman, "An Extension of the Shannon Theory Approach to Cryptography", IEEE Transactions on Information Theory, Vol. 23, No. 3, pp. 289-294, 1977.

[8] Jason H. Li, B. Bhattacharjee, M. Yu and Levy, "A Scalable Key Management and Clustering Scheme for Wireless Adhoc and Sensor Networks", Journal of Future Generation Computer Systems, Elsevier Science Publishers, Vol. 24, pp. 860-869, 2008.

[9] K. Bhatele, A. Sinhal and M. Pathak, "A Novel Approach to the Design of a New Hybrid Security Protocol Architecture", IEEE International Conference on Advanced Communication Control and Computing Technologies, pp.429-433, 2012.

[10] M. Y. Wang, C. P. Su, C. L. Horng, C.W. Wu and C. T. Huang, "Single and Multi-core Configurable AES Architectures for Flexible Security", IEEE Transactions on Very Large Scale Integration Systems, Vol. 18, No. 4, pp. 541-552, 2010.

[11] T. Rams and P. Pacyna, "A Survey of Group Key Distribution Schemes With Self- Healing Property", IEEE Communications Surveys and Tutorials, Vol. 15, No. 2, pp. 820-842, 2013.

[12] Z. Wan, J. Liu, and R. H. Deng, "HASBE: A Hierarchical Attribute-Based Solution for Flexible and Scalable Access Control in Cloud Computing", IEEE Transactions on Information Forensics and Security, Vol. 7, No. 2, pp. 743-754, 2012.

[13] Y. Li, K. Ohta and K. Sakiyama, "New Fault-Based Side-Channel Attack Using Fault Sensitivity", IEEE Transactions on Information Forensics and Security, Vol. 7, No. 1, pp. 88-97, 2012.

[14] C. H. Kim, "Improved Differential Fault Analysis on AES Key Schedule", IEEE Transactions on Information Forensics and Security, Vol. 7, No. 1, pp. 41-50, 2012.

[15] S. Bu, F. R. Yu, X. P. Liu, P. Mason and H. Tang, "Distributed Combined Authentication and Intrusion Detection With Data Fusion in High-Security Mobile Networks", IEEE Transactions on Vehicular Technology, Vol. 60, No. 3, pp. 1025-1036, 2011.

[16] L. J. G. Villalba, J. G. Matesanz, D. R. Canas and A. L. S. Orozco, "Secure Extension to the Optimized Link State Routing Protocol", IET Information Security, Vol. 5, No. 3, pp. 163-169, 2011.

[17] H. W. Kim and S. Lee, "Design and Implementation of a Private and Public Key Crypto Processor and Its Application to a Security System", IEEE Transactions on Consumer Electronics, Vol. 50, No. 1, pp. 214-224, 2004.

Author Profile

Shaina Garg received the B. Tech degree in Computer Engineering from Haryana College of Technology and Management in 2014. During 2014-2016, she studied about the cryptography concepts specially RSA Algorithm, how to increase security among the systems.