Volume 2, Issue 12, December 2012 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Performance Evaluation Using Cryptographic Technique

Sumedha Kaushik[1]
[#]*Department of ECE &M. M. University Ambala,(Haryana) India*

Ankur Singhal[2]
[#]*Department of ECE &M. M. University Ambala,(Haryana) India*

Abstract—***Network is an interconnected collection of autonomous computers to share and exchange the data. Security implies safety, including assurance of data integrity, freedom from unauthorized access of computational resources and disruption of services. So, network security refers in a broad sense to confidence that information and services available on network cannot be accessed by unauthorized users. Unconditionally secure message authentication is an important part of cryptography. Cryptography is the practice and study of techniques for secure communication in the presence of third parties. It is about constructing and analysing protocols that overcome the influence of adversaries and which are related to various aspects in information security such as data confidentiality, data integrity, authentication, and non-repudiation. Various cryptographic techniques have been studied by using information test and randomness test. And it is found that 3DES (EBC) is better in comparison to other cryptographic algorithms.***

Keywords— ***Network security, date integrity, data confidentiality, authentication, cryptography, 3DES (ECB) .***

I. INTRODUCTION

Network is an interconnected collection of autonomous computers to share and exchange the data. Security implies safety, including assurance of data integrity, freedom from unauthorized access of computational resources and disruption of services. So, network security refers in a broad sense to confidence that information and services available on network cannot be accessed by unauthorized users. So, Network Security is the most vital component in information security because it is responsible for securing all information passed through networked computers. Network Security refers to all hardware and software functions, characteristics, features, operational procedures, accountability, measures, access control and administrative and management policy required to provide an acceptable level of protection for Hardware and Software , and information in a network. The Cryptography tool is used to enhance the security of network. The goal of Cryptography [1] is to make it possible for two people to exchange a message in such a way that other people cannot understand the message which can be achieved by transforming the original information into some other form. This transformation can takes place the form of encoding messages that make them Non-Readable. This art and science of achieving security is known as Cryptography [2, 3]. The Greek meaning of Cryptography is hidden writing or art of changing plaintext message. Cryptography is used increasingly be business, individuals and the Govt. for ensuring the security and privacy of information and communication. The theory of solving cryptographic system is known as cryptanalysis and a person who attempts to break a cipher text message or modified message is cryptanalyst. The scientific study of cryptography and cryptanalysis is cryptology.

II. RELATED WORK

Meyer C.H. et al. proposed that Cryptography is the only known practical method for protecting information transmitted through potentially hostile environments, where it is either impossible or impractical to protect the information by conventional physical means. Also, damage resulting from message alteration, message insertion, and message deletion can be avoided. Administrative and physical security procedures often can provide adequate protection for offline data transport and storage. However, where file security methods are either nonexistent or weak, encryption may provide the most effective and economical protection. The authors gives an overview of cryptographic methods using symmetric and asymmetric algorithms and demonstrates why future cryptographic applications should use a hybrid approach, i.e., combination of symmetric and asymmetric (public key) methods [4]. Garfinkel, S.L. et al. investigate that the RSA algorithm can be used for a kind of unforgeable digital signature. In this application, the secret key is used to encrypt a message, which can then itself be decrypted by anyone possessing the public key. Digital signatures can play a role in many activities that do not require secrecy but require sender authentication and guaranteed message integrity. Because it offers the possibility of true privacy and secrecy, public key cryptography has become a cause celebre among many computer users. Nevertheless, the RSA algorithm, developed in 1977, remained the stuff of academic curiosity for nearly 20 years and did not enjoy widespread use. Three factors combined to delay the spread of public key cryptography: the speed disparity between low-cost and high-cost computers, intellectual property law, and the US government's export control laws, which remain a problem to this day [5]. Sanchez-Avila C. et al. studied that in October 2000, after three years of competition between 15 candidate algorithms, the National Standards and Technology (NIST) chose the

Rijndael algorithm to be adopted as Advanced Encryption Standard (AES) by the U.S. Department of Commerce, replacing to Data Encryption Algorithm (DES), which has been the standard since 1977. The authors analyse the structure and design of new AES, following three criteria: a) resistance against all known attacks; b) speed and code compactness on a wide range of platforms; and c) design simplicity; as well as its similarities and dissimilarities with other symmetric ciphers. On the other side, the principal advantages of new AES with respect to DES and T-DES, as well as its limitations, are investigated. Thus, for example, the fact that the new cipher and its inverse use different components, which practically eliminates the possibility for weak and semi-weak keys, as existing for DES, and the non-linearity of the key expansion, which practically eliminates the possibility of equivalent keys, are two of the principal advantages of new cipher. Finally, the implementation aspects of Rijndael cipher and its inverse are treated. Thus, although Rijndael is well suited to be implemented efficiently on a wide range of processors and in dedicated hardware [6]. Krishnamurthy P. et al. analysed that Encryption algorithms are known to be computationally intensive. They consume a significant amount of computing resources such as CPU time, memory, and battery power. A wireless device, usually with very limited resources, especially battery power, is subject to the problem of energy consumption due to encryption algorithms. Designing energy efficient security protocols first requires an understanding of and data related to the energy consumption of common encryption schemes. In this paper, we provide the results of experiments with AES and RC4, two symmetric key algorithms that are commonly suggested or used in WLANs. Our results show that RC4 is more suitable for large packets and AES for small packets [7].

Kofahi N.A. et al. presented an implementation of three encryption algorithms and a comparison between them based on CPU execution time. The CPU execution time is broken down to kernel and user time. The selected algorithms are: DES, Triple-DES (T-DES) and Blowfish. These are symmetric block encryption algorithms. The objective of this research is to evaluate the performance of the three cryptography algorithms in terms of the processing time required in the kernel and user space for generating the secret key, encryption and decryption operations. The powerful portable programming language Java and JCA (Java cryptography architecture) is used in implementing the encryption algorithms. The performance of the implemented encryption algorithms will be evaluated on SunOS platforms. The results show that the Blowfish algorithm is the fastest, followed by the DES algorithm then the T-DES algorithm [8].

Elbirt A.J. et al. studied that efficient implementation of block ciphers is critical towards achieving both high security and high-speed processing. Numerous block ciphers have been proposed and implemented, using a wide and varied range of functional operations. As a result, it has become increasingly more difficult to develop a hardware architecture that allows the efficient and fast realization of a wide variety of block ciphers. In an effort to achieve such hardware architecture, a study of a wide range of block ciphers was undertaken to develop an understanding of the functional requirements of each algorithm. This study led to the development of COBRA, a reconfigurable architecture for the efficient implementation of block ciphers. A detailed discussion of the top level architecture, interconnection scheme, and underlying elements of the architecture is provided. System configuration and on-the-fly reconfiguration is analyzed, and from this analysis it is demonstrated that the COBRA architecture satisfies the requirements for achieving efficient implementation of a wide range of block ciphers that meet the 622 Mbps ATM network encryption throughput requirements [9].

Bouvry P. et al. studied the problem of designing symmetric key algorithms based upon cellular automata (CAs) is considered. As the basic cryptography scheme, the Vernam cipher is applied. The reliability of the Vernam cipher depends highly on the quality of random numbers used in the process of encryption. One dimensional, nonuniform CAs are considered as a generator of a high quality pseudorandom number sequences (PNSs). The quality of PNSs highly depends on a set of applied CA rules. To find such rules, nonuniform CAs with two types of rules are considered. The search of rules is performed using an evolutionary technique called cellular programming. As the result of collective behaviour of a discovered set of CA rules, very high quality PNSs are generated. The quality of PNSs outperforms the quality of known one-dimensional CA-based PNS generators used for secret key cryptography. The extended set of CA rules, which was found, makes the cryptography system much more resistant to breaking a cryptography key [10].

Salomao, S.L.C. et al. studied that Data security is an important issue in today's computer networks. This paper presents the HiPCrypto chip, which implements the IDEA cryptographic algorithm. HiPCrypto is oriented towards computer network applications demanding high throughput. Its architecture exploits both the spatial and the temporal parallelism available in the IDEA algorithm. When operating at a 53 MHz clock, HiPCrypto can encrypt/decrypt at data rates up to 3.4 Gbps [11].

III. RESULT & DISCUSSION

Encryption techniques were analysed using Cryptography tool simulator with various tests such as Information Theory Tests and Randomness Tests. It was found that the 3DES (ECB) cryptographic Technique is stronger in comparison to other cryptographic Techniques. According to information content test, the value of entropy should be as high as possible, so 3DES (ECB) is having highest value of entropy as compare to hybrid and Caeser is having least value.

The overall result of the various analysis tests performed on the algorithms is as under:

Table: 1 Result Table

S. No	Parameters → / Algorithms ↓	Entropy	Periodicity	Serial test	Poker test	Frequency test	Brute force	Floating frequency	Auto-Correlation
1	CAESAR	4.13	No	Fail	Fail	Fail	26	Symmetric	Asymmetric
2	XOR-TEST	7.06	No	Fail	Fail	Fail	1024 bytes	Asymmetric	Asymmetric
3	IDEA	7.94	No	Pass	Pass	Pass	128 bits	Asymmetric	Asymmetric
4	RC4	7.93	No	Fail	Pass	Fail	8bits	Symmetric	Asymmetric
5	DES(ECB)	7.95	No	Pass	Pass	Pass	56 bits	Symmetric	Symmetric
6	DES(CBC)	7.94	No	Pass	Pass	Pass	56 bits	Symmetric	Symmetric
7	3DES(ECB)	7.93	No	Pass	Pass	Pass	112 bits	Asymmetric	Asymmetric
8	3DES(CBC)	7.94	No	Pass	Pass	Pass	56 bits	Asymmetric	Symmetric
9	RIJNDAEL (AES)	7.94	No	Pass	Pass	Pass	112bits	Asymmetric	Symmetric
10	RSA	7.94	No	Pass	Pass	Pass	2048 bits	Asymmetric	Symmetric
11	HYBRID (RSA-AES)	7.91	No	Pass	Pass	Pass	2048 bits	Asymmetric	Asymmetric

The autocorrelation has none correlating or wide range with different zigzag patterns. So, according to table 3DES in ECB mode is the best and caeser is given very poor performance. In case of periodicity, no periodicity, no offset or no cycles are preferred. So IDEA, DES in both modes, AES, HYBRID showed no change whereas XOR and CAESER showed poor performance. Based on Randomness analysis test, 3DES (ECB) is much better than other ciphers. 3DES(ECB) passes the entire test so it is obviously secure than other algorithms like XOR,CAESER, AES,HYBRID etc.

IV. CONCLUSION

Various cryptographic algorithms have been studied. These algorithms are analysed using Information Theory Tests and Randomness Tests. These tests are completed using Cryptography tool simulator. According to information content test, and randomness test, it was found that the 3DES (ECB) cryptographic Technique is stronger in comparison to other cryptographic Techniques. It can be implemented in C++, Java, and Dot net for encrypting text files.

REFERENCES

[1] Punita Mellu & Sitender Mali, "AES: Asymmetric Key Cryptographic System", International Journal of Information Technology & Knowledge management, pp. 113-117, 2011.

[2] Sanchez Avila, "The Rijndael block cipher: A Comparison with DES", 35th International Conference security technology, 2001.

[3] Stalling, William, Computer Networking with Internet Protocol & technology, 2nd Edition Pearson Education, Asia 2004.

[4] Meyer C.H., "Cryptography-a state of the art review," Conferrence on VLSI and Microelectronic Applications in Intelligent Peripherals and their Interconnection Networks, pp. 4/150 - 4/154, 1989.

[5] Garfinkel S.L., "Public key cryptography," computer, Vol. 29, Issue 6 , pp.101 – 104, 1996.
[6] Sanchez-Avila C., Sanchez-Reillol R., "The Rijndael block cipher (AES proposal): a comparison with DES," IEEE 35th International Carnahan Conference on Security Technology, pp. 229 – 234, 2001.
[7] Krishnamurthy P., Prasithsangaree P., "Analysis of energy consumption of RC4 and AES algorithms in wireless LANs," IEEE Global Telecommunications Conference, vol.3, pp. 1445 – 1449, 2003.
[8] Kofahi N.A., Turki Al-Somani, Khalid Al-Zamil, "Performance evaluation of three encryption/decryption algorithms," pp. 790 – 793, Vol. 2, 2003.
[9] Elbirt A.J., Paar C., "Instruction-level distributed processing for symmetric-key cryptography," International Parallel and Distributed Processing Symposium, 2003.
[10] Bouvry P., Seredynski F., Zomaya, A.Y., "Secret key cryptography with cellular automata," ACS/IEEE International Conference on Computer Systems and Applications, 2003.
[11] Salomao, S.L.C., Alves, V.C., Filho E.M.C., "HiPCrypto: a high-performance VLSI cryptographic chip," Proceedings Eleventh Annual IEEE International ASIC Conference, pp. 7 - 11 ,1998.

