Geeta Kocher al. International Journal of Recent Research Aspects ISSN: 2349-7688, Special Issue: Engineering Research Aspects Feb 2015, pp. 1-4

Review of Symmetric Ciphers

Geeta Kocher[1], Sharad Chauhan[2], Dr. Kamal Sharma[3]

[1]Student, M. Tech, Dept. of CSE, E-Max School of Engineering, Badhauli
[2]Assoc. Professor & Head, Dept. of CSE, E-Max School of Engineering, Badhauli
[3]Director, E-Max School of Engineering, Badhauli

***Abstract*— Network is an interconnection of various nodes that are used to share and exchange information. Security implies assurance of data integrity, independence from unauthorized access of computational resources. Broadly, Network security refers to confidence that information and services available on network cannot be used by unauthorized users. Cryptography techniques can be employed to secure information. This paper summarizes the various issues of symmetric cryptography.**

Index Terms: **Cryptography, Encryption, Decryption.**

I. INTRODUCTION

Network is an interconnected collection of autonomous computers to share and exchange the data [1].
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. There are four fundamental precepts for preventing the information loss:

- Confidentiality specifies that information should be protected from eyes of unauthorized internal users and only sender and intended receiver must be able to access the contents of a message.
- Authentication mechanisms help establish proof of identities and Fabrication is possible in the absence of proper authentication mechanisms
- Integrity ensures that information will not be accidentally or maliciously altered or destroyed during transmission. At receiving end information should appear exactly as was stored or sent.
- Availability means message must be available to authorized parties at all the times otherwise interruption takes place.

1.1 NETWORK THREATS

Particularly security is needed against modern attacks that can be very dangerous. Automation of attacks, privacy concerns are some of the key characteristics of modern attacks. These can be classified as common person's view & a technologist view. Former includes criminal, publicity & legal attacks. These attacks mainly concentrate on manipulating some aspects like purchase orders, business opportunities, how to maximize financial gain. Latter includes theoretical concepts behind these attacks and practical approaches used by attackers. Theoretical concepts define four types of attacks namely: Interception, Modification, Fabrication, and Interruption.

II. NETWORK SECURITY MECHANISMS

- Firewall
- Intrusion detection system
- Cryptology

Firewall is a popular tool used by organizations for network security and came into picture to achieve protection from outside attacks. It tracks all the details of the user requests on the network and firewall policy states that the details of every request made by the users must pass through the firewall. It can help to prevent malicious users on the internet from accessing the data or services on a private network. A firewall is a means of controlling and analyzing data passing between the networks and is a special type of router, which applies rules for allowing and stopping traffic. It stands like a security guard on the main gate between internal network and outside Internet. A firewall can be application gateway or packet filter. Whereas application gateway is like a proxy server (deputy or substitute) decides the flow of application level traffic, packet filter examines each packet and decides whether to pass or discard.
No matter how much secure a system is made, there would be attackers, who would constantly try to find their way, and we call them Intruders as they try to intrude into the privacy of a network. Intruders can be of three types: Masquerader, Misfeasor, and Clandestine. They are impossible to prevent but an attempt is made to detect them. So Intrusion detection systems can act as good deterrents to intruders. These can be categorized as Statistical anomaly detection and Rule based detection. According to Statistical anomaly detection, behaviors of users are captured to detect whether are legitimate or not which are again detected according to defined threshold or profile based. According to Rule based detection, a set of rules are applied to see if given behavior is suspicious enough to classify as an attempt to intrude and are detected according to Anomaly detection and penetration identification. However, no single mechanism is there that will support all functions required. Only one particular element underlies many of the security mechanisms in use: Cryptographic techniques; hence our focus is on this area.
Cryptology is as old as writing itself and has been used for thousands of years to safeguard military and diplomatic communications. In the past decades, we have witnessed an explosive growth of the digital storage and communication of data, triggered by some important breakthroughs such as the Internet and the expansive growth of wireless communications. These new information and communication technologies require adequate security. Cryptology is the science that aims to provide information security in the digital world.

III. CRYPTOLOGY

Information security comprises many aspects, the most important of which are confidentiality and authenticity. Confidentiality means keeping the information secret from all except those who are authorized to learn or know it. Authenticity involves both ensuring that data have not been modified by an unauthorized person (data integrity) and being able to verify who is the author of the data (data origin authentication).
Cryptology is usually split up into two closely related fields: cryptography and cryptanalysis. Cryptography studies the design of algorithms and protocols for information security. The ideal situation would be to develop algorithms, which are probably secure, but this is only possible in very limited cases. Therefore, the best way to assess the security of a cryptographic algorithm or protocol is by testing all possible known attacks on it. Cryptanalysis is concerned with this study of mathematical techniques that attempt to break cryptographic primitives. The cryptographic algorithms are usually split up into two families: symmetric algorithms and public-key algorithms. Symmetric algorithms (also called secret-key algorithms) require that the communicating parties share the same secret key. In public-key algorithms (also called private-key algorithms), the public key is made public and the private key is kept secret by a single entity.

Related terms of cryptography are described below:

- **Plaintext** - the original message or message in an understandable form same as clear text.
- **Cipher text** - the coded message after the transformation.
- **Cipher**- algorithm for transforming plaintext to cipher text.
- **Cryptography**- The art of developing ciphers is called cryptography.
- **Crypto-analyses**- The art of breaking ciphers is called crypto-analyses.
- **Key** –The secret information in a cryptographic operation known only to sender/receiver.

Every encryption and Decryption process has two aspects. The algorithm and the key used for encryption and decryption. In general, the algorithm used for encryption and Decryption process is usually known to everybody. However it is the key used for encryption and decryption that makes the process of cryptography secure. Whereas key is nothing but the secret information in cryptographic operation. Broadly, there are two cryptographic mechanisms depending on what keys are used. If same key or one key is used for encryption and decryption we call the mechanism as symmetric key cryptography. If two different key is used for decryption on we call the mechanism as asymmetric key Cryptography.

In public key cryptography, the encryption and decryption is performed with a different key, while in secret key cryptography both parties possess the same key. Secret key cryptosystems can be further divided into block ciphers and stream ciphers. While block ciphers operate with a fixed transformation on large blocks of data, stream ciphers and typically operate with a time-varying transformation on smaller units of plaintext, usually bits. Let us introduce them further:

(a) **STREAM CIPHERS**

These types of algorithms are designed to accept a stream of plain text to produce a stream of cipher text. Processes the input continuously producing an element at a time. The example is one-time pad or Vernam scheme that is the simplest known and provably secure stream cipher. It uses a random sequence as key stream, which is added modulo two with the plaintext in order to produce the ciphertext.

(b) **BLOCK CIPHERS**

They are designed to take data blocks of a particular (fixed) size, encrypt them with a key of particular size, and yield a block of ciphertext of a particular size. For most block ciphers, the ciphertext is produced by repeatedly applying a so-called round function. The key material used in the round function is called a round key. The round keys are computed from the key using a key-schedule algorithm.

Symmetric Key Cryptography:

Symmetric key cryptography also referred to as Private Key or Secret Key Cryptography as same key is used for both Encryption and Decryption. The Mechanism is as shown in figure 1.1

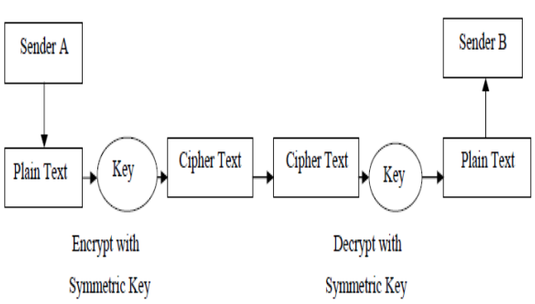

Fig.1.1: Symmetric Key Cryptography

Methods of Symmetric Key Cryptography:

1. **DES (Data Encryption Standard):** DES is a block Cipher. It encrypts data in block size 64 bits and produces 64 bits of Cipher text. The key length is 56 bits. The working is as follows.

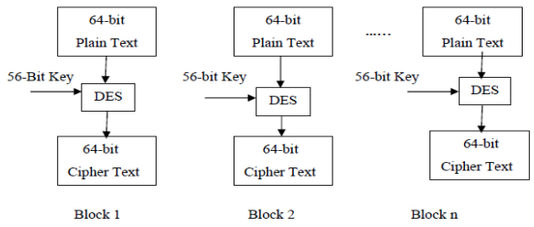

Fig.1.2: Working of DES

2. **Double DES:** As the name suggests Double DES does twice as what DES does only once. It uses two keys. Here concept of meet-in-middle attack is introduced. It means Encryption from one end and Decryption from other end and matching the result in middle, hence meet in middle attack. The process of Encryption is as follows.

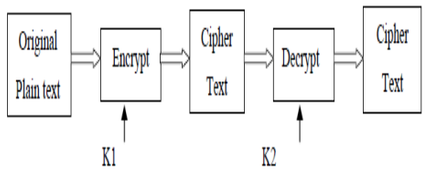

Fig.1.3: Double DES Encryption

The decryption process works in reverse under and shown as follows.

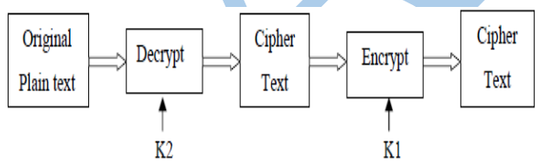

Fig.1.4: Double DES Decryption

3. **Triple DES**: Triple DES means three times DES. The working is as follows.

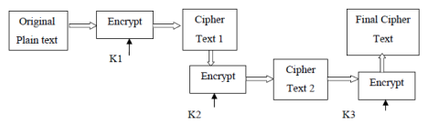

Fig.1.5: Triple DES with three keys

4. **AES (Advanced Encryption Standard):** AES is a non feistel i.e. permutation- substitution network that encrypts and decrypts a data block of 128 bits. It uses 10, 12 or 14 rounds. The key size that can be 128, 192 or 256 bits depends on the number of rounds, but the round keys are always 128 bits. AES is based on Rijndael algorithm.

IV. LITERATURE REVIEW

C. Sanchez-Avila et.al (2001), the structure and design of Rijndael cipher (new AES) have been analyzed, remarking its main advantages and limitations, as well as its similarities and dissimilarities with DES and T-DES. Finally, a performance comparison among new AES, DES and T-DES for different microcontrollers has been carried out, showing that new AES have a computer cost of the same order than the one needed by T-DES [2]

A. Murat Fiskiran et.al (2002) showed some cryptographic algorithms that have properties that make them suitable for use in constrained environments like mobile information appliances, where computing resources and power availability are limited characterization of the instructions executed by these algorithms, and demonstration that a simple processor is sufficient. Also a set of public key, symmetric key and hash algorithms suitable for such environments and studied their workload characteristics It also describes the instructions needed by different algos: Diffie Hellman key exchange, AES, Hash. All are compared using simple RISC style processor with ALU and shifter and workload characteristics can be determined [3].

Subbarao V. Wunnava (2002) presented the results of investigations conducted by the authors regarding the emerging data security methodologies. Emphasis is placed on the applicability of these algorithms in the academic, industrial and

commercial environments. Of the several methodologies considered for the
AES (Advanced Encryption Standard), MARS has become one of the front running and adaptable methodologies for the data security over global networks [4].

Othman O. Khalifa et.al (2004) discussed basic concepts, characteristics, and goals of various cryptography. Mainly it focused on the analysis of the two types of cryptography exists, based on the availability of the key publicly: Private Key cryptography and public key cryptography [5].

Aameer Nadeem et.al (2005) presented**,** performance of 4 secret key algorithms (DES, Tri-DES, AES, Blowfish) were compared by encrypting input files of various contents and sized on different hardware program. The algorithms have been implemented in a uniform language, using their standard specifications, to allow a fair comparison of execution speeds. Pentium-II having frequency 266MHz (running Microsoft Windows OS) and Pentium-IV with 2.4 MHz machine (running Windows XP OS) are the basis for time measurement with their goal to measure the encryption times of considered algorithms. The performance results have been summarized and discussed a tradeoff between performance and security and a conclusion has been presented. The performance measurement approach was JAVA in which Blowfish was the fastest algorithm among DES, 3-DES, AES and Execution results are presented in ECB mode (for block ciphers) and CFB (for stream ciphers) and concluded on the basis that an algorithm having more complex rounds and a larger number of rounds is generally considered more secure. So, concluded Blowfish as the fastest one among all. [6]

Kyung Jun Choi et.al (2006) investigated various cryptographic algorithms suitable for used in wireless sensor network utilizing MICA z-type motes & Tiny OS is investigated. Usage of resources including memory, computational time and power for each cryptographic algorithm was characterized experimentally. MD5 and RC4 showed best performance in terms of power dissscipation and in terms of cryptographic processing time used. ATMEL AT mega 128 L microprocessor is on board in MICA z-based motes. 128KB programmable flash memory used to store executable program code, 4KB SRAM used for temporary storage. To measure encryption key set up time a 128 bit size key that provides 2^128 possible keys was used. RC4 was considered as the best as it is XOR based stream cipher cheaper, less complex, and fastest and uses 8-bit block size which can be efficiently handled by ATMEL [7].

Like Zhang et.al (2007) focused on application level attacks and explores how the packet payload can be used for identifying application level attacks. It also discusses the current status of network anomaly detection, and emphasized the importance of payload based detection research using existing problems, and proposed an efficient method to detect payload related attacks. The method is divided into a training phase and a detection phase. In the training phase, Principal Component Analysis (PCA) on several important packet fields was done to reduce the data dimension, and then constructed the most appropriate profile based on the PCA results. In the detection phase, an anomaly score defend against unknown attacks is demanding increased research in this area [8].

Susan et.al (2007) concluded that the Security field is a new, fast moving career. A focus on security stabilizes course material, reduces worry about student hacking, and helps to provide students the skills necessary to become security analysts. It also defines the set of skills required by Network Security analysts as network Security skills emphasize business practices, legal foundations, attack recognition, network optimization and describes active learning exercises that assist the students in learning these important skills. This actually summarized all the skills relating to network security, and discussed active learning exercises that assist students in learning these important skills. Main focus was on security information skills that are to be used in Securing the Network [9].

Yudhvir et.al (2008) devoted to the security and attack aspects of cryptographic techniques and also discussed dominant issues of Security and various information theory characteristics of various cipher texts. The simulation based information content test such as Entropy, Floating Frequency, Histogram, Ngram, Autocorrelation and Periodicity on ciphers was done. The simulation based Randomness test such as Frequency test, Pokers test, Serial test, Long run test on ciphers were done using CrypTool. Finally, they were benchmarked some well- known cryptographic algorithms in search for the best compromise in security [10].

Jyothi Yenuguvanilanka et.al (2008) addresses the performance of Rijndael AES Encryption algorithm of key length 128 bits. Two hardware models based on HDL and IP core are used to evaluate the performance of the algorithm. The encryption time and also the performance metrics such as size, speed and memory utilization are evaluated, using these models. Results are compared to a reference model and have shown an increase in the throughput per slice measure. Finally we have seen single core HDL model is 27 times faster than SoPC hardware model using the same target [11].

A. Kaushik et al. developed a new algorithm block encryption standard for transfer of data (BEST) implemented in C++ and JAVA and results are compared with AES and DES. It shows that it protect from brute force attacks and Replay attacks, also it can change the format of key while sending it from one end to another [12].

P. Meelu et al. presents the fundamental mathematics behind the AES algorithm along with a brief description of some cryptographic primitives that are commonly used in the field of communication security. It also includes several computational issues, optimization of cipher as well as the analysis of AES security aspects against different kinds of attacks including the counter measures against these attacks and also highlighted some of the important security issues of AES algorithm [13].

V. Verma et al. presents Advanced Encryption Standard (AES) as a specification for the encryption of electronic data which supersedes DES. The algorithm is a symmetric-key algorithm. Multicrypt is a scheme that allows for the encryption of any file or files. After the analysis of comparison of both type of encryption scheme multicrypt is much better than single type encryption because it is very secure because of many layers (level) of security and authentication. For security of personnel document, single type encryption is enough while for corporate and business purpose multicrypt is better option to secure important files and documents [14].

V. CONCLUSION

Cryptography studies the design of algorithms and protocols for information security. Various Techniques for cryptography like symmetric and asymmetric cryptography has been studied. Symmetric techniques can be further divided as stream ciphers and block ciphers. Various algorithms of symmetric techniques like DES, 3-DES, and AES has been studied and concluded that AES algorithm is better in symmetric cryptography.

VI. REFERENCES

[1]. Atul Kahate, "Cryptography and Network Security", Tata Tata Tata McGraw Hill Publishing Company Limited,2003.

[2]. Sanchez-Avila,C.sanchez-Reillol,R, "The Rijndael block cipher(AES proposal): A comparison with DES, IEEE International Conference on Security Technology,2001.

[3]. A. Murat Fiskiran and Ruby B. Lee. "Workload Characterization of Elliptic Curve Cryptography and other Network Security Algorithms for Constrained Environments" IEEE International Workshop on Workload Characterization, 2002.

[4]. Wunnava S. V, Rassi E, "Data encryption performance and evaluation schemes", Proceedings IEEE in Southeastern, 2002.

[5]. Othman O. Khalifa, MD Rafiqul Islam, S. Khan and Mohammed S.Shebani, "Communications Cryptography", RF and Microwave Conference, 2004.

[6]. Aameer Nadeem, Dr. M.Younus Javed, "A performance comparison of data Encryption Algorithm", Global Telecommunications Conference Workshops,2004. GlobeCom Workshops,IEEE,2004.

[7]. Kyung Jun Choi, John –In Song, "Investigation of feasible cryptographic Algorithm For wireless sensor network", International conference on ICACT Feb 20-22,2006

[8]. Like Zhang, Gregory B. White," Anomaly Detection for Application Level Network Attacks Using Payload Keywords"**,** Proceedings of the 2007 IEEE Symposium

on Computational Intelligence in Security and Defense Applications (CISDA 2007).

[9]. Susan J Lincke, Andrew Hollan, "Network Security: Focus on Security, Skills, and Stability", Proceedings of 37th ASEE/IEEE Frontiers in Education Conference, 2007.

[10]. Yudhvir Singh, Yogesh Chaba, "Information Theory Test based performance evaluation of Cryptographic techniques", International Journal of Information Technology and Knowledge Management, Vol. 1, No. 2, 2008,pp.475-483.

[11]. Jyothi Yenuguvanilanka, Omar Elkeelany, "Performance Evaluation of Hardware Models of Advanced Encryption Standards (AES) Algorithm", IEEE Conference, 2008.

[12]. A.Kaushik, M.Barnela, A.Kumar, "Block Encryption standard for transfer of data," International Conference on Networking and Information Technology, 2010.

[13]. P.Mellu & S.Mali, "AES: A symmetric key cryptographic System", International Journal of Information Technology and Knowledge Management, Vol., No. 4 pp 113-117, 2011.

[14]. V. Verma, A .Dhole, "Analysis of comparison between Single Encryption (Advance Encryption Scheme(AES)) and Multicrypt Encryption Scheme" , International Journal of Scientific and Research Publications, Vol. 2, Issue 4, April 2012.

