Performance Evaluation of Ciphers Using CRYPTOOL 2.0

Kulwinder kaur

AIET, Faridkot, PUNJAB

ABSTRACT

Cryptography is an emerging technology, which is important for network security. Research on cryptography is still in its developing stages and considerable research effort is required. This paper includes the complete step by step implementation of advance encryption technique, i.e. encrypting and decrypting 128 bit data using the AES and its modification for enhanced reliability and security. The encryption process consists of the combination of various classical techniques such as substitution, rearrangement and transformation encoding technique. The encryption and decryption module include the key expansion module which generates the key for all iterations. The modification includes the addition of an arithmetic operation and a route transposition cipher in the attacks iterative rounds. The key expansion module is extended to double the number of iterative rounds in order to increase its immunity against unauthorized attacks.

Keywords—AES, DES, Symmetric key , Asymmetric key.

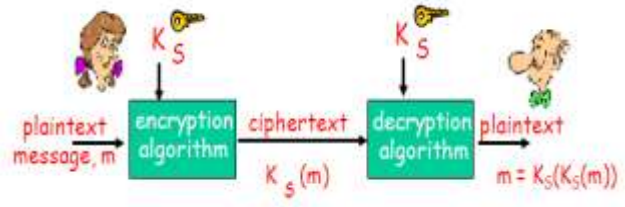
1. Introduction

Network Security has gained immense prominence in the last few years as it is the key aspect of Internet based Security Mechanism and also with the proliferation of handheld wireless information appliances the ability to perform security function with limited computing resources has become increasingly important. 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. These are further grouped as passive and Active. Where as in passive attacks, the attacker does not modify the contents of message. Release of message contents and traffic analysis are the type of passive attacks. In active attacks, the contents of message are modified masquerade, Replay attacks, Alteration of message and Denial of service (DOS) are type of active attacks. The attacks discussed earlier can come in real life, as it can happen up till application level as well as Network level. Whereas in application level attacker can change the contents of a message and in Network level aim is to reduce Network capabilities by number of possible means, which either slow down or completely bring to halt. Practically attacks on computer system are Viruses, Worms, and Trojan horses. The principles of any security mechanism are confidentiality, authentication, integrity, Non repudiation. Where confidentiality ensuring that no one can read the message except the intended receiver. Authentication is the process of proving ones Identity; Integrity assures the receiver that received message has not been altered in any way from the original. Non Repudiation is a mechanism to prove that sender really sent this message. For many people, security just means preventing unauthorized access such as preventing a hacker from breaching into a Network, security is more than that. The easiest way to keep a message secret is to hide the very fact of its existence 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 [1]. 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. In technical terms, the process of encoding plaintext message into cipher text messages is called as Encryption Fig (a) illustrates the idea.

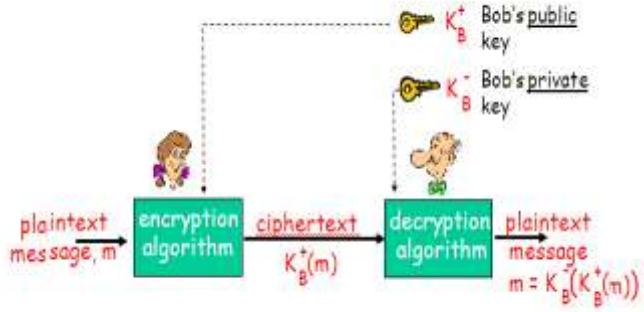
Fig (a) Encryption

Fig (b) Decryption

The reverse process of transforming cipher text message back to plaintext message is called as Decryption. Fig (b) illustrates the idea. 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. Both ideas are illustrated in the fig(c) and (d).



Fig(c) Encryption symmetric key process



Fig(c) Encryption Asymmetric key process

There are two key aspects of such algorithms: algorithm types and algorithm modes. An algorithm type defines what size of plain text should be encrypted in each step of algorithm. It can be stream cipher in which Encrypting one plain text byte at a time where as in Block cipher, a block of bytes are encrypted at one go. Stream cipher relies on confusion (a technique of ensuring that a cipher text gives no clue about the original plain text) and block cipher uses both confusion and diffusion (increases the redundancy of plaintext by spreading into rows and columns). There are four algorithm modes namely Electronic Code Book (ECB), Cipher Block Chaining (CBC), Cipher Feedback (CFB) and output Feedback (OFB). Let us briefly discuss symmetric key cryptography, also referred to as Private Key or Secret Key Cryptography as one key is used for both Encryption and Decryption. Obviously both parties (sender & receiver) must agree upon the key before and transmission begins and nobody else should known about it. Methods of symmetric key cryptography. DES(Data Encryption Standard), DoubleDES ,Triple-DES,IDEA(International Data Encryption Algorithm,RC4(Rivest Cipher 4),RC5, Blowfish ,AES (Advanced Encryption Standard . Few problems exists, first is key exchange or key agreement. Second, one key per communicating parties is required. For more communicating parties if such same key is used then no secret left. Well, every problem has solutions and that is Asymmetric key cryptography also known as Public Key Cryptography. Method for asymmetric cryptography are: RSA(Rivest Shamer Adleman ,Digital signature ,Message digest abbreviated MD (including MD1,MD2,MD3,MD4,MD5), Secure Hash Algorithm(SHA) Elliptical curve cryptography (ECC).From above discussion, it is clear that even if confidential information flows out of network and if it is in encrypted form then outsiders cannot make sense of it. However Encryption cannot work in other direction. Outsiders can still break inside a corporate network. Consequently, better schemes are desired to achieve protection from outside attacks. This is where Firewall comes into picture. A firewall is a special type of router, which applies rules for allowing and stopping traffic. It stands like a sentry on the main door 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.

2. Related Work

Susan et.al (2007) concluded that the Security field is a new, fast moving career. 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 [1].

Mohamed A. Haleem et.al (2007) discussed a trade off between security and throughput in wireless network where Markov Decision Process and OFDM (orthogonal frequency Division Multiplexing) helped out to determine channel estimation, tracking and prediction. It also uses channel opportunities (acceptable signal to noise ratio) to maximize the throughput. It defines mathematical models to capture the security-throughput trade-off, adversary models and their effects, joint optimization of encryption and modulation (single and multirate), the use of Forward Error Correcting (FEC) codes to protect encrypted packets from bit errors, and simulation results for Rijndael cipher [2].

2.1 Field of Attacks

Igor Kotenko et.al (2003) describes the approach to active vulnerability assessment of computer networks based on modeling and simulation of complex remote attacks and its implementation. Two types of experiments have been fulfilled with the Attack Simulator: (1) simulation of attacks on macro-level (imitation of malicious actions against computer network model); (2) simulation of attacks on micro-level (generation malicious network traffic against a real-life computer network) [3].

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 [4].

2.2 Field of Firewall

Robert N. Smith et.al 2003 proposed his paper to introduce a cascade of (potentially simpler and less expensive) firewalls in the secure data network—where, between the attacker node and the attacked node, multiple firewalls are expected to provide an added degree of protection. This approach, broadly following the theme of 'redundancy in Engineering Systems' Design, and provide more completeness in the level of security protection by the firewalls. The cascade of (i.e., multiple) firewalls can be placed across the secure data network in many ways, we present heuristics for placement of these firewalls across the different nodes and links of the network. Performance of these heuristics is presented using simulation, along with some early

analytical results [5] .

Guanhua Yan et.al addressed optimized placement and ordering of distributed firewall rules to mitigate the worst-case damage that can occur to individual firewalls and proposed a heuristic-based algorithm to migrate rules among distributed firewalls. Experimental results show our solution can balance workloads on distributed firewalls effectively and efficiently [6].

2.4 Field of Intrusion Detection System

Weijan huang et.al (2010) discussed the defects about distributed intrusion detection system and analyzed the improvements and demonstrated the importance in e-commerce

2.5 Field of Cryptography

Othman O. Khalifa et.al (2004) discussed basic concepts, characteristics, and goals of various cryptography. In today's information age, communication plays an important role which is contributed to growth of technologies therefore privacy is needed to assure the security that is sent over communication media [7].

A.Murat Fiskiran et.al (2002) showed some cryptographic algorithms that has 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 [8].

2.6 Field of Symmetric Key Cryptography

Aameer Nadeem et.al(2005) presented **,** performance of 4 secret key algorithms (DES,3-DES,AES,Blowfish) were compared by encrypting input files of various contents and sized on different hardware program and performance measurement approach was JAVA in which Blowfish was the fastest algorithm and Execution results are presented in ECB mode (for block ciphers) and CFB (for block ciphers)[9].

Kyung Jun Choi et.al (2006) investigated various cryptographic algorithms suitable for wireless sensor network based on MICAz-type motes in which MD5 and RC4 showed best performance in terms of power dissscipation and in terms of cryptographic processing time used [10].

Yan Wang et.al (2009) analysed time evaluation of known cryptographic algorithms such as RSA,3-DES,AES using NFC/VC++.and also using Random number generating mechanism showing run time characteristics which highlights difference between three algos namely AES, RSA , Triple-Des in which AES is the best one[11].

2.7 Field of Stream & Block Ciphers

P. Kitsos et.al (2003) three different implementations of Triple DES block cipher was presented in VHDL languages and implemented in XIINX FPGA, devices where they are based on pipeline Techniques and suitable for high speed application[12].

Brian Baldwin et.al **(**2008), Study of fault injection attacks on a Feistal algorithm is done using VHDL and proposed a novel approach for a simple attack scenario on the expanded version of that algorithm as block ciphers are typically resistant to direct attacks [13].

Akhil kaushik et.al (2010), 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 Bruth force attacks and Replay attacks, also it can changes the format of key while sending it from one end to another[14].

Jung Kyu Han et.al (2008) proposed an efficient multimedia content encryption scheme for mobile handheld devices (EMCEM), which uses a block cipher to encrypt some parts of content and a stream cipher to encrypt the others. Experimental results have shown that EMCEM has much better performance than encrypting content completely using a block cipher.[15]

Weir, J et.al (2008) introduced how to hide a visual cryptography share into a halftone image. The results were very robust and can resist print and scan tempering. Based on this, they also generated an animation using this scheme.[16]

2.8 Field of Asymmetric Key Cryptography

Thongpon Teerakanok et.al(2009)proposed a new algorithm "Parallel-key cryptographic algorithms (PCA)", based on Asymmetric key cryptography and is strengthened against bruth force attack and Factorization attack. Also it shows the comparison with RSA,one of the Symmetric cryptographic algorithm[17].

2.9 Field of Hash Function

Elkamchouchi et.al (2006) presented a new secure hash algorithm based on dynamic structure algorithm called secure hash dynamic structure algorithm (SHDSA). It uses a famous secure hash algorithm (SHA) given by the National Institute of Standards and Technology (NIST) [18].

3. Methodology

Study and analysis the performance of various ciphers is done using CRYPTOOL. Developing new Cipher "BEST" and

Comparison of "BEST" with existing Ciphers are done using Java. CrypTool is free software and an e-learning tool illustrating cryptographic concepts with graphical user interface. Main features are: Cryptographic methods can be applied and analyzed, comprehensive online help (understandable without a deep knowledge of cryptography), contains nearly all state-of-the-art cryptography functions, Easy entry into modern and classical cryptography and last but not the least it's not a "hacker tool".

The current release version CrypTool 1.x is written in C++, and it runs only on the operating system Microsoft Windows. In contrast, the two projects which developed since 2007 the newly designed successors in pure-plug-in architecture make very good progress: Cryptool 2.0 uses the concept of visual programming to clarify cryptographic processes. Jcryptool 1.0 is platform independent and offers both document-centric and a function-centric perspective.

4. Challenges & Objectives

1. Study of various Stream and block ciphers.

2. Analysis of various Ciphers.

3. Performance evaluation of Ciphers.

4. Developing new Cipher "BEST".

5. Comparison of "BEST" with existing Ciphers.

5. Applications

Cryptography is extremely useful; there is a multitude of applications, many of which are currently in use. A typical application of cryptography is a system built out of the basic techniques. Such systems can be of various levels of complexity. Some of the more simple applications are secure communication, identification, authentication, and secret sharing. More complicated applications include systems for electronic commerce, certification, secure electronic mail, key recovery, and secure computer access.

5.1 Secure Communication

Secure communication is the most straightforward use of cryptography. Two people may communicate securely by encrypting the messages sent between them. Thanks to the development of public-key cryptography, the tools exist to create a large-scale network of people who can communicate securely with one another even if they had never communicated before.

5.2 Identification and Authentication

Identification and authentication are two widely used applications of cryptography. Identification is the process of verifying someone's or something's identity. Another important application of cryptography is authentication. Authentication is similar to identification, but authentication is broader. Authentication merely determines whether that person or entity is authorized for whatever is in question

5.3 Electronic Commerce

Over the past few years there has been a growing amount of business conducted over the Internet - this form of business is called electronic commerce or *e*-commerce. *E*-commerce is comprised of online banking, online brokerage accounts, and Internet shopping, to name a few of the many applications. One can book plane tickets, make hotel reservations, rent a car, transfer money from one account to another, buy compact disks (CDs), clothes, books and so on all while sitting in front of a computer. However, simply entering a credit card number on the Internet leaves one open to fraud. One cryptographic solution to this problem is to encrypt the credit card number (or other private information) when it is entered online, another is to secure the entire session. When a computer encrypts this information and sends it out on the Internet, it is incomprehensible to a third party viewer. The web server ("Internet shopping center") receives the encrypted information, decrypts it, and proceeds with the sale without fear that the credit card number (or other personal information) slipped into the wrong hands. As more and more business is conducted over the Internet, the need for protection against fraud, theft, and corruption of vital information increases.

5.4 Cryptography in cellular (mobile) phones

Cryptography is not confined to the world of computers. Cryptography is also used in cellular (mobile) phones as a means of authentication; that is, it can be used to verify that a particular phone has the right to bill to a particular phone number. This prevents people from stealing (``cloning'') cellular phone numbers and access codes. Another application is to protect phone calls from eavesdropping using voice encryption.

5.5 Cryptography in financial magnetic stripe cards

The intention is to prevent fraudulent construction of counterfeit cards by Inserting a value on the magnetic stripe that cannot be derived from other card information. Thus when a card is validated online this value can be checked to determine whether the card is genuine or a forgery. Several different standards exist for this mechanism; the most Common being the VISA Card Verification Value (CVV) or the MasterCard equivalent, CVC.For the purposes of this document I will refer to this mechanism as CVV as this is the term in most common use. The majority of magnetic card encryption is based on the Data Encryption Algorithm (DEA), usually called DES or Data Encryption Standard.

5.6 Watermarking & Cryptography

Multimedia applications deploy various cryptographic and watermarking techniques to maintain security. In this context, we survey the main work on two promising approaches for the secure embedding and detection of watermark in an untrusted environment, and we point out some associated challenges.

6. Conclusion

The advanced encryption technique was implemented successfully using java language. Various data messages were encrypted using different keys and varying key sizes. The original data was properly retrieved via decryption of cipher text. The modifications brought about in the code was tested and proved to be accurately encrypting and decrypting the data messages with even higher security and immunity against the unauthorized user.

7. References

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

2. Mohamed A. Haleem, Chetan N.MathurR. Chandramouli, K.P. Subbalakshmi, "Opportunistic Encryption: A trade off between Security and Throughput in Wireless Network" IEEE Transactions on Dependable and secure computing, vol. 4, no. 4.

3. Igor Kotenko, "Active Vulnerability Assessment of Computer Networks by Simulation of Complex Remote Attacks", Proceedings of the 2003 International Conference on Computer Networks and Mobile Computing (ICCNMC'03).

4. 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).

5. Robert N. Smith, Yu Chen, and Sourav Bhattacharya , "Cascade of Distributed and Cooperating Firewalls in a Secure Data Network" IEEE transactions on knowledge and Engineering, vol. 15, no. 5.

6. Guanhua Yan,Songqing Chen,Stephan Eidenbenz , "Dynamic Balancing of Packet Filtering Workloads on Distributed Firewalls", 16TH International Workshop on

Quality of service IWQOS 2008.

7. Othman 0. Khalifa', MD Rafiqul Islam', S. Khan' and Mohammed S. Shebani", Communications Cryptography",RF and Microwave Conference.RFM2004

Proceedings.

8. 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. WWC-5. 2002

9. Aameer Nadeem, Dr. M.Younus Javed, "A performance comparison of data Encryption Algorithm", Global Telecommunications Conference Workshops, 2004.

GlobeCom Workshops 2004. IEEE

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

11. Yan Wang, Ming Hu, "Timing Evaluation of known cryptographic Algorithm", International Conference on Computational Intelligence and security,2009

12. P. Kitsos, s.goudevenos, "VLSI Implementation of Triple DES block cipher", roceedings of the 2003 10th IEEE International Conference on Electronics, Circuits and Systems, 2003. ICECS 2003.

13. Brian Baldwin, Emanuel M. Popovici, Michael Tunstall, and William P. Marnane, "Injection Platform for Block Ciphers" Signals and Systems Conference, 208. (ISSC 2008). IET Irish.

14. Akhil kaushik, Manoj Barnela, Anant Kumar, "Block Encryption standard for transfer Of data", International conference on Networking and Information Technology, 2010.

15. Jung Kyu Han , Hye-Young Chang , Seongje Cho , Minkyu Park , "EMCEM: An Efficient Multimedia Content Encryption Scheme for Mobile Handheld Devices", International Conference on Information Science and Security, 2008. ICISS.

16. Weir, J. , WeiQi Yan , Crookes, D. "Secure mask for color image hiding" Third International Conference on Communications and Networking in China, 2008.

17. Thongpon Teerakanok, "Accelerating Asymmetric key cryptography using PCA", 6th International Conference on Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology, 2009. ECTI-CON 2009.

18. Elkamchouchi, H.M; Emarah, A.-A.M; Hagras, E.A.A, "A New Secure Hash Dynamic Structure Algorithm (SHDSA) for Public Key Digital Signature Schemes", The 23rd National Radio Science Conference (NRSC 2006).