A STUDY OF VARIOUS CRYPTOGRAPHIC ALGORITHMS

Omkar Prasad[1]*,Palak Keshwani*[2]

[1]*B.E. Student , CSE Dept., KITE, Raipur*

[2]*Asst. Professor CSE Dept., KITE, Raipur*

E-mail.- Omnayak97@gmail.com,palakeshwani@gmail.com

ABSTRACT

The techniques ensuring secure transmission and storage of information has been ever increasing. Cryptography is evergreen and developing. Cryptography protects users by providing functionality for the encryption of data and authentication of other users. Compression is a method of reducing the number of bits or bytes needed to represent a given set of data. It decreases disk space. Cryptography is a ways of sending useful data in a secret way. There are many techniques available and among them AES is one of the most powerful techniques. Encryption algorithms transform messages by adding some cryptographic protection, such as confidentiality, authenticity or integrity to them. These algorithms employ one or more keys that are cryptographic variables used to control the algorithm and provide security against attackers. This paper deals with a comparative study of encryption algorithms along with their applications in real world scenario.

Keywords *: Encryption, decryption, Compression, Cryptography, Security, Integrity.*

1. Introduction

In traditional telecommunication systems, securing the channel meant securing the messages. With the advent of internet and advancement in packet switching techniques, securing the channel is neither possible nor effective. This increases the importance of cryptography. Websites defines cryptography as “the enciphering and deciphering of messages in secret code or cipher; also the computerized encoding and decoding of information”. Cryptography aims at hiding information and making it secure. Where as , there is another field of study which is concerned with the techniques of defeating such attempts called cryptanalysis. Cryptology is a broad domain which includes both cryptography and cryptanalysis.The art of cryptography is considered to be born along with the art of writing. As civilizations evolved, human beings got organized in tribes, groups, and kingdoms. This led to the emergence of ideas such as power, battles, supremacy, and politics. These ideas further fuelled the natural need of people to communicate secretly with selective recipient which in turn ensured the continuous evolution of cryptography as well. The roots of cryptography are found in Roman and Egyptian civilizations .The importance of information and communication systems for society and the global economy is intensifying with the increasing value and quantity of data that is transmitted and stored on those systems. At the same time, the systems and data are also vulnerable to a array of threats, for example, unauthorized access and use, misuse, change, and demolition. The hiding of information is called encryption, and when the information is unhidden, it is called decryption. A cipher is used to accomplish the encryption and decryption. Merriam-Webster’s Collegiate Dictionary defines cipher as ―a method of transforming a text in order to conceal its meaning. The information that is being hidden is called plaintext; once it has been encrypted, it is called ciphertext. To hide any data two techniques are mainly used one is Cryptography other is Steganography. In this paper ,we use Cryptography. Cryptography is the science of protecting data, which provides methods for converting data into unreadable form, so that valid user can access information at the destination. Cryptography is the science of utilizing the mathematics to encrypt and decrypt data.

2. Description

Computers are used by large number of people for different purposes, such as banking, shopping, military, student records, etc.. Privacy is a critical issue in many of these applications. Cryptography is the transformation of readable and understandable data into a form which cannot be understood in order to secure data. Cryptography means the methodology of hiding the messages, cryptography comes from the Greek word "Kryptos", which means hidden, and "graphikos" which means writing.

The information that we need to hide, is called plaintext , It’s the original text, It could be in a form of characters, numerical data, executable programs, pictures, or any other kind of information, The plaintext for example is the sending of a message from the sender before encryption, or it is the text at the receiver after decryption. The data that will be transmitted is called cipher text , it's a term refers to the string of "meaningless" data, or unclear text that nobody must understand, except the recipients, it is the data that will be transmitted exactly through network. Many algorithms are used to transform plaintext into cipher text. Encryption is a mechanism of converting readable and understandable data into "meaningless" data .The Key is an input to the encryption algorithm, and this value must be independent of the plaintext, This input is used to transform the plaintext into cipher text, so different keys will yield different cipher text, In the decipher side, the inverse of the key will be used inside the algorithm instead of the key. Computer security is a word for a collection of tools designed to protect any data from hackers, theft, corruption, or natural disaster while allowing these data to be available to the users at the same time. The example of these tools is the antivirus program. By using cryptography many goals can be achieved. These goals can be either all achieved at the same time in one application, or only one of them. These goals are:

1. Confidentiality: It is the most important goal, it ensures that nobody can understand the received message except the one who has the decipher key.
2. Authentication: It is the process that assures the communicating entity is the one that it claimed to be.
3. Data Integrity: It makes sure that the received message has not been modified.
4. Non-Repudiation: It is used to prove that sender has send the message and received by the specified party, so the recipient cannot claim that the message was not sent. 5. Access Control: It is the process of preventing an unauthorized use of resources. This goal controls who can have access to the resources, If one can access, under which restrictions and conditions the access can be occurred, and the permission access of a level.

Cryptography Applications

Cryptography has found its application in more than what one can imagine. Major sectors which use cryptographic techniques include defense, government and law enforcement agencies, banking, insurance, business and industry. It has even found its way into sectors like healthcare, education, tourism and social welfare. Cryptography could be applied to text, image, audio and video based scenarios including both real time and non-real time systems. During the last years, the use of embedded cryptographic processors has spread from low-cost crypto-processors, such as smart cards used for holding decryption keys, to more modern applications, such as user authentication, identity management, e-mail, mobile communication, electronic payment schemes, digital right management and trusted computing Initiative (TCI).

Types of Cryptography

Secret Key Cryptography: When the identical key is utilized for both encryption and decryption , the mechanism is known as secret key cryptography ,for example, DES, Triple DES, AES, RC5 etc.

Public Key Cryptography: When two dissimilar keys are utilized, one key for encryption and another key for decryption, mechanism is known as public key cryptography ,for example, RSA, Elliptic Curve and etc.

3. Related Work

3.1 DES

DES is a block cipher that utilizes common secret key for the encryption and the decryption. DES algorithm gets a fixed length of string in plaintext bits and convert it through a sequence of process into cipher text bit sting of the same length and its each block is 64 bits.

There are 16 identical stages of processing, called as rounds. There is also an initial and final permutation named as IP and FP.

3.2 3DES

3DES is an enrichment of DES and it is 64 bit block size with 192 bits key size. In this standard, the encryption of process is alike the one in the original DES and raise the encryption level and the average safe time.

3DES is slower than other block cipher methods. It uses either two or three 56 bit keys in the sequence order of encrypt-decrypt-encrypt.

TDES algorithm with 3 keys needs 2^{168} chances of combinations and with 2 keys requires 2^{112} combinations; and the limitation of this algorithm is too time consuming problem.

3.3 AES

AES encrypts all 128 bits in one iteration. This is the reason that it has a comparably small number of rounds. AES encryption is fast and flexible. It can be implemented on a variety of platforms particularly in small devices.

3.4 Blowfish

Blowfish is one of the most general and popular public domain encryption algorithm given by Bruce Schneier, one of the worlds leading cryptologists, and the president of Counterpane Systems and a consulting firm specializing in cryptography and computer security. It encrypts 64-bits block cipher with variety length key and its contains 2 parts.

Data Encryption: Its involves the iteration of a simple function of 16 times. Each round contains a key dependent permutation and data dependent substitution.

Subkey Generation: Its involves converting the key upto 448 bits long to 4168 bits

3.5 RSA

RSA is a public key algorithm given by Rivest, Shamir, Adleman, it involves a public key and a private key. The public key can be identified to everyone and is used for encrypting messages. Messages encrypted with the public key can only be decrypted using the private key. These keys for the RSA algorithm are generated in many ways.

4. Comparison of Cryptography Algorithms

Varioous algorithms are compared in the following table no. 1.

Table 1: Comparision of various algorithms

Algorithm	Created By	Key size(bits)	Block size(bits)
DES	IBM in year 1975	56	64
3DES	IBM in year 1978	112 OR 168	64

AES	Joan Daemen and Vincent Rijmen in year 1998	256	128
BLOWFISH	Bruce Schneier in year 1993	32 OR 448	64

5. Conclusion

Security plays a very important role in conserving the integrity of data. And the ever persisting craving to develop a secure system has brought cryptography in the lime light. In this paper, a survey has been made on various cryptographic techniques like AES, DES, 3DES, Blowfish, RSA . This paper presents the performance evaluation of selected symmetric algorithms -AES, 3DES, Blowfish and DES. In future, we can use encryption techniques in such a way that it can consume less time and power of furthermore and high speed and minimum energy consumption.

6. Aknowledgement

I would like to thank my project guide Mrs. Palak Keshwani for providing guidance to carry out this work.

7. References

[1]. S. Hirani, “Energy Consumption of Encryption schemes in wireless device Thesis”, university of Pittsburgh, Apr. 9, 2003,Retrieved Oct.1, 2008.

[2]. A. Nadeem, "A performance comparison of data encryption algorithms", IEEE information and communication technologies, pp.84-89, 2006.

[3]. Ravi, S., Raghunathan, A., Kocher, P., Hattangady, S.: “Security in embedded systems: Design challenges”. ACM Transactions on Embedded Computing Systems (TECS) 3 (2004) 461-491

[4]. Kocher, P., Lee, R., McGraw, G., Raghunathan, A.: Security as a new dimension in embedded system design. In: Proceedings of the 41st annual Design Automation Conference. DAC '04 (2004) 753{760 Moderator-Ravi, Srivaths.

[5]. Kang, K.D., Son, S.H.: Towards security and qos optimization in real-time embedded systems. In: SIGBED Rev. Volume 3., New York, NY, USA, ACM (2006) 29-34

[6]. S. Kim, Ingrid Verbauwhede, “AES implementation on 8-bit microcontroller,” Department of Electrical Engineering, University of California, Los Angeles, USA, September, 2002.

[7]. M. Feldhofer, J. Wolkerstorfer, and V. Rijmen, “AES implementation on a grain of sand,” IEE Proc. Inf. Security, vol. 152, IEE, pp. 13-20, Oct. 2005.

[8]. National Institute of Standards and Technology. An Introduction to Computer Security: The NIST Handbook. Special publication 800-12. October 1995.

[9]. Atul Kahate “Cryptography and Network Security”, Tata McGraw-Hill Companies, 2008.

[10]. D. Boneh and M. Franklin, “Identity-based encryption form the weil pairing”, in Advance in Cryptology (CRYPTO’01), LNCS 2139, Springer Verlag, 37, 213-229, 2011

[11]. Davis.R, “The Data Encryption Standard in Perspective”, Proceeding of Communication Society magazine, IEEE, Vol 16, Nov 1978.

[12]. Gurjeevan Singh, Ashwani Kumar Singla, K.S. Sandha “Performance Evaluation of Symmetric Cryptographic Algorithms”, International Journal of Electronics and Communication Technology Vol 2 Issue 3, Sep 2011.

[13]. Pratap Chandra Mandal “Superiority of Blowfish Algorithm”, International Journal of Advanced Research in Computers Science and Software Engineering Vol 2 Issue 9, Sep 2012.

[14]. Daemen.J and Rijmen, The Advanced Encryption Standard, Dr. Dobb's Journal, March 2001.

[15]. R.L.Rivest, A.Shamir, L.Adleman, "A Method for obtaining Digital Signatures and Public-Key Cryptosystem", Communication of the ACM, Vol 21, Feb 1978.