Volume 9, Special Issue No. 1, February 2018

ISBN: 978-93-5300-455-2

International Journal of Advanced Research in Computer Science
(ISSN: 0976-5697)
REVIEW ARTICLE

ICRACC 2018
(23rd–24th February 2018)

Available Online at www.ijarcs.info

Cryptography In Network Security: A Much Needed Technique

P.Srilakshmi
Department of Computer Applications,
S.S.S. Shasun Jain College for Women,
T. nagar, Chennai.

AparnaR.
Assistant Professor, Department of Computer Applications,
S.S.S. Shasun Jain College for Women,
T. nagar, Chennai.

ABSTRACT

In today's world we people have stated using the internet for many purposes be it for browsing, internet banking, E-mailing, social media and for many more things. But is our information safe and secure? Network security is very important and there are many algorithms which will help us to keep our data safe from people who hack into our system. In this paper we will study the different cryptographic algorithms which in keeping the data safe.

Keywords: cryptography,algorithms, cipher, encryption and decryption

I. INTRODUCTION

Network security is very important for the safety of our data because many of us use mobile phones and laptops (PDAs) in which we store most of our personal details like contacts, e-mails and even banking details in order to protect these files and information we use cryptography. The following are the most common algorithms which are used for network security[1] blowfish algorithm, RSA, RC4, data encryption standard, Diffie Hellman algorithm. These algorithms help us to keep the private data a secret. Cryptography encrypts[2] the details and only the person with the key will be able to access the information, the algorithms will help us to encrypt and decrypt the informations. In this paper we will study and compare these algorithms.

II. IMPORTANT TERMS IN CRYPTOGRAPHY

A. *Cryptography*

Cryptography is the method of keeping private information safe from other people. It is also known as cryptology. The practice and study of techniques for secure communication

B. *Encryption*

The process of converting plain text to a text which looks meaningless (cipher text) is called encryption.

C. *Decryption*

The process of converting the cipher text back to plain text (original text) is called decryption

D. *Cipher(cypher)*

Cipher is a group of algorithms which is used to encrypt and decrypt the messages and information. This is also called as cryptosystem.

E. *Key*

Key is a group of text which is used to encrypt and decrypt the message.

III. CRYPTOSYSTEMS AND ITS TYPES

Cryptosystems[3] are set ofalgorithms which are used to implement a security service. These cryptosystems are highly in demand to ensure security during data storage and transmission.

It consists of three process:

- Key generation

  Key generation is the process of generating keys for cryptography. The key is used to encrypt and decrypt data whatever the data is being encrypted or decrypted

- Encryption

  Encryption is the process of converting original information (called plaintext) into unintelligible text (called ciphertext).

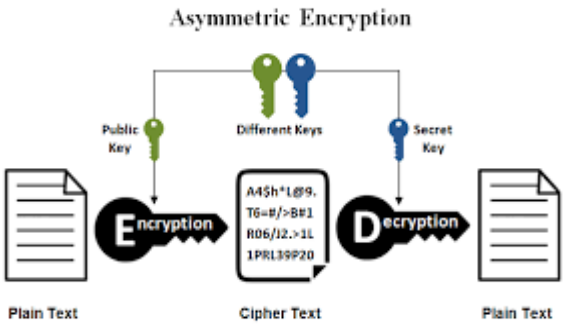
- Decryption

  Decryption is the process of transforming data that has been rendered unintelligible through encryption back to its original form.

This is of two types based the type of key used in Asymmetric cryptosystem[1] and symmetric cryptosystem [1].

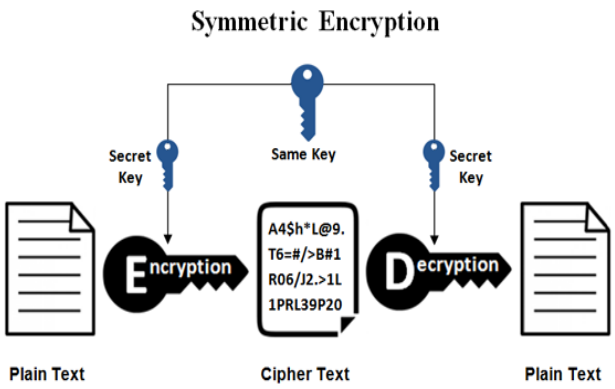
A. *Asymmetric cryptosystem*

This type of system uses one key for encryption and a different key for decryption. This is also known as public key cryptography. The keys used in this system are numbers. The keys are paired up. One key which can be shared is called public key, the other key which cannot be shared is called private key. Here only private key can decrypt the message. Some common algorithms are RSA, Diffie-Hellman key exchange.



B. *Symmetric cryptosystems*

This system uses the same key for both encryption and decryption. This is speeder and less difficult than asymmetric cryptosystem[2]. Since we use only one key the key is kept private and the information is kept safe. Most commonly used algorithms are AESand DES[4].



IV. ALGORITHMS

A. *RSA(Rivest Shamir Adleman)*

Ron Rivest, Adi Shamir, and Len Adleman created this RSA public key algorithm[2] in 1978. This is used to for signing and encryptionwithout exchanging the secret key. The key size should be more than 1024 bits for a good security. This algorithm is based on the "factoring problem"[3]. That is, it based on the difficulty of factorization[4] of product of twolarge prime number. The user creates two keys and releases the public key which is based on prime numbers.

B. *Diffie Hellman key exchange*

This algorithm is used for the secure transfer of the cryptographic keys. It is one of the practical examples of public key exchange[5]. It allows two people to have no previous information about each other to establish a secret key on an insecure network. It is used on many internet services such as speech synthesis [7].

C. *DES (Data Encryption Standard)*

This algorithm was developed by IBM. It is a symmetric cryptosystem. DES is used for the electronic encryption of data. It uses a 56-bit key[6]. It is considered insecure due to the less number of keys.

D. *AES (Advanced Encryption Standard)*

Its security is based on the intractability of certain discrete logarithm problems.*AES (Advanced Encryption Standard)*

This is also used for electronic encryption of data. It uses only one key. It has variable key length of 128/192/256 bits [7]. Each key could encrypt or decrypt a 128 bit data. AES is proven to be a relaiable algorithm.

Its security is based on the intractability of certain discrete logarithm problems.

V.APPLICATION AREAS OF CRYPTOGRAPHY

There are many applications which are currently being used. They are:

a. Secure Communication

This is used for communicating with other people securely. We can communicate such that the people trying to eavesdrop will not be able to do so. This is due to the use of public key that we are able to communicate peacefully.

b. Identification and Authentication

Identification is very important aspect. It is the process of verifying a person by cross checking with some proof like the ATM machines used a PIN number to identify the user. The same is applicable to cryptography the user and verified after which access is provided to that person.

c. Secret Sharing

This application allows us to share a secret with a group of people [8]. The actual secret is never disclosed.

d. E-commerce

This is a form of business conducted over the internet. Online shopping, booking tickets, transferring funds are a part of this. But giving credit cards away is not safe. Therefore, the card numbers are encrypted whenever it is entered and the information is thus secured.

VI.COMPARISON BETWEEN THE DIFFERENT ALGORITHMS

Algorithm	key size	Speed	Security
DES	56 bits	SLOW	INSECURE
AES	128,192, 256 bits	FAST	SECURE
RSA	1024 and above	FAST	SECURE
DIFFIE-HELLMAN	3072 BITS	FAST	SECURE

VII.CRYPTOGRAPHY IN DEFENCE

Cryptography is a huge asset to the military forces.With the help of enigma cipher the cryptanalysts attacked the Lorentz cipher.

In today's world, it is a necessity to keep the military[9] orders and plans a secret. The government is also providing funds for making the information secure [10]with the help algorithms. In 2010,stutex an elaborate computer worn was discovered.

Until recently cryptography has been of interest primarily to the defence and diplomatic personnel of governments, guarded over and directed by their national crypto logic services. The use of cryptography itself is not controlled i.e. sending an encrypted email or message, or making an encrypted phone call, is not subject to export control simply because it is encrypted.Hence,it is essential to focus more on strong algorithmic techniques to safeguard the information which carries a very secret message.

VIII.CONCLUSION

Network security has become a very important thing in today's world due to a growth in technology. This growth helps us in so many useful things like online shopping, e-commerce,e-banking,e-business but it also has its demerits like keeping our information safe from other people. Cryptography helps us in keeping this information safe. It has developed very rapidly in a short span of time. Cryptography is now-a-days used in many different fields like defense, air force and many in such places. Cryptography does not give 100% guarantee for keeping data safe at the same time the risk factor is reduced considerably.

IX. REFERENCES

[1] Prof. Mukund R. Joshi, RenukaAvinashKarkade, network security with cryptography

[2] RIVEST, R.L., SHAMIR, A., and ADLEMAN, L: 'A method for obtaining digital signatures and public-key cryptosystems', CACM, 1978, 21, pp. 120-126

[3] Dr. Sandeep Tayal1, Dr. Nipin Gupta2, Dr. Pankaj Gupta3, Deepak Goyal4, Monika Goyal5, A review paper on network security and cryptography.
[4] Coron, J. S. , " What is cryptography?", IEEE Security & Privacy Journal, 12(8), 2006, p. 70-73.
[5] R.Aparna ,Dr.P.l.Chithra,"A Review on Cryptographic Algorithms for Speech Signal Security" International Journal of Emerging Trends & Technology in Computer Science(IJETTCS), Volume 5, Issue 5, September - October 2016,pp 84-88.
[6] KritikaAcharya, ManishaSajwan, Sanjay Bhargava, Analysis of Cryptographic Algorithms for Network Security
[7] Aparna R.,Dr.P.L.Chithra,Role of Windowing Techniques in Speech Signal Processing For Enhanced Signal Cryptography,Chapter 28,Advanced Engineering Research and Applications.
[8] M. Shashanka and P. Smaragdis, "Secure sound classification: Gaussian mixture models," in Proc. ICASSP, vol. 3, Toulouse, France, 2006, p. 3.
[9] Laura Savu, Cryptography Role in Information Security, Recent Researches in Communication and IT,pg 36-41
[10] M. Quisquater, L. Genelle, and E. Prouff, "Thwarting higher-order side channelanalysis with additive and multiplicative maskings," in Cryptographic Hardwareand Embedded Systems 2011, Nara, Japan, 2011, pp. 240–255.