IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 5, May 2016

Over View of Cryptographic Algorithms for Information Security

Dr. D. Vimal Kumar[1], Mrs. J. Divya jose[2]

Professor, PG Department of Computer science, Nehru Arts & Science College, Coimbatore, India[1]

M.Phil Research Scholar, Nehru Arts & Science College, Coimbatore, India[2]

Abstract: It is used to ensure that the contents of a message are confidentially transmitted and would not be altered. Network security is most vital component of information security as it refer to all hardware and software function, characteristic, feature, operational procedures, accountability, access control, and administrative and management policy. Cryptography is central to IT security challenges, since it underpins privacy, confidentiality and identity, which to gather provide the fundamental for trusted e-commence and secure communication. There is a board range of Cryptographic algorithms that are used for securing network and presently continuous researcher on the new cryptography algorithm are going on for evolving more advanced techniques for secure communication.

Keywords: Cryptography, plain text, cipher text, encryption, decryption, network security.

I. INTRODUCTION

The building blocks of computer security are cryptographically based mechanism. Cryptography can be applied anywhere in the TCP/IP stack, though it is not common at physical layer. Cryptography is also used in complicated protocols that help to achieve different security services, thus called security protocols. The main feature of the encryption/decryption program implementation is the generation of the encryption key. Cryptography is about constructing and analyzing protocols that prevent third parties or the public from reading private messages various aspects like data integrity, data confidentiality and repudiation are central to modern cryptography. It exists in the discipline of Computer Science, Mathematics, and electrical engineering. The different applications of cryptography include ATM cards, Computer Passwords and electronic commerce

1.1 Basic Terms Used in Cryptography

1.1.1 Plain Text

The original message that the person wishes to communicate with the other is defined as Plain Text. In cryptography the actual message that has to be send to the other end is given a special name as Plain Text.

For example, Alice is a person wishes to send “Hello Friend how are you” message to the person Bob. Here “Hello Friend how are you” is a plain text message.

1.1.2 Cipher Text

The message that cannot be understood by anyone or meaningless message is what we call as Cipher Text. In Cryptography the original message is transformed into non readable message before the transmission of actual message.

For example, “Ajd672#@91ukl8*^5%” is a Cipher Text produced for “Hello Friend how are you”.

1.1.3 Key

A specific string of data that is used to encrypt and decrypt messages, documents or other types of electronic data. Keys have varying levels of strength. Keys having higher numbers of bits are theoretically tougher to break because there are more possible permutations of data bits. (Since bits are binary, the number of possible permutations for a key of x bits is 2x.) The specific way a key is used depends on whether it's used with asymmetric or symmetric cryptography..

1.1.4 Encryption

A process of converting Plain Text into Cipher Text is called as Encryption. Cryptography uses the encryption technique to send confidential messages through an insecure channel. The process of encryption requires two things- an encryption algorithm and a key. An encryption algorithm means the technique that has been used in encryption. Encryption takes place at the sender side.

1.1.5 Decryption

A reverse process of encryption is called as Decryption. It is a process of converting Cipher Text into Plain Text. Cryptography uses the decryption technique at the receiver side to obtain the original message from non-readable message (Cipher Text). The process of decryption requires two things- a Decryption algorithm and a key.

A Decryption algorithm means the technique that has been used in Decryption. Generally the encryption and decryption algorithm are same. Now a day, cryptography has many commercial applications. If we are protecting confidential information then cryptography is provide high level of privacy of individuals and groups. However, the main purpose of the cryptography is used not only to provide confidentiality, but also to provide solutions for other problems like: data integrity, authentication, non-repudiation. Cryptography is the methods that allow

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 5, May 2016

information to be sent in a secure from in such a way that the only receiver able to retrieve this information. Cryptography not only protects data from theft or alteration, but can also be used for user authentication. It is necessary to apply effective encryption/decryption methods to enhance data security.

Cryptography provides a number of security goals to ensure the privacy of data, non-alteration of data.

1.2 Goals of Cryptography

1.2.1 Confidentiality

The term ensures that no one can read the message except the intended receiver. The meaning of a message is concealed by encoding it. The sender encrypts the message using a cryptographic key.

The recipient decrypts the message using a cryptographic key that may or may not be the same as the one used by the sender.

1.2.2 Authentication

Mechanism which helps to enable authentic communication. It is the process of proving one's identity. A user or system can prove their identity to another who does not have personal knowledge of their identity accomplished using digital certificates. Kerberos is a common cryptographic authentication system.

1.2.3 Integrity

Assuming the receiver that the received message has not been altered in any way from the original. Integrity Ensures that the message received is the same as the message that was sent .Uses hashing to create a unique message digest from the message that is sent along with the message.

Recipient uses the same technique to create a second digest from the message to compare to the original one. This technique only protects against unintentional alteration of the message. A variation is used to create digital signatures to protect against malicious alteration.

1.2.4 Non-Repudiation

Ensures that neither the sender nor the receiver of message should be able to deny the transmission.

1.2.5 Access Control

Only the authorized parties are able to access the given information. Network security involves the authorization of access to data in a network, which is controlled by the network administrator.

The initial encrypted data is referred to as plain text. It is encrypted into cipher text, which will in turn be decrypted into usable plain text.

Cryptographic algorithms are categorized based on the number of key that are employed for encryption and decryption.

1.3 Types of Cryptography

1.3.1 Symmetric Key Cryptography

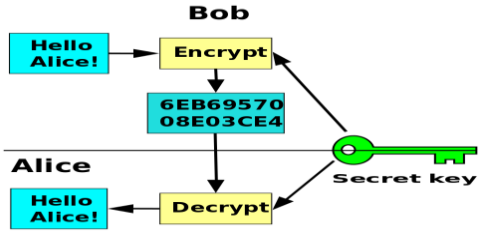

Fig: Symmetric Key Cryptography

An encryption system in which the sender and receiver share a single common key for encrypting and decrypting the message. They are simple and faster. It is sometimes called secret key cryptography. The most popular is the data encryption standard.

1.3.2 Public Key Cryptography

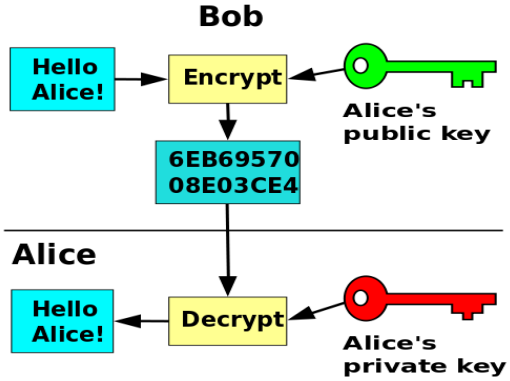

Fig : Public Key Cryptography

Public key cryptography utlilizes two keys, Public Key to encrypt the messages and a private key to decrypt them. The private key is never transmitted

2.2 Classification of Encryption Schemes

Algorithm	Key Size(s)	Speed	Speed Depends On Key?	Security
DES	56 bits	Slow	Yes	Insecure
3DES	112/168 bits	Very Slow	No	Moderately Secure
AES	128, 192, 256 bits	Fast	Yes	Secure
BLOWFISH	32-448 bits	Fast	No	Believed secured, but less Attempted cryptanalysis than other algorithms
RC4	256 Bytes	Very Fast	No	Moderately Secure
RSA	1024 bits and above	Fast	Yes	Secure

2.2.1 Symmetric Key Encryption

2.2.1.1 DES (Data Encryption Standard)

DES is a symmetric block cipher developed by IBM. The algorithm uses a 56-bit key to encipher/decipher a 64-bit block of data. The key is always presented as a 64-bit block, every 8th bit of which is ignored. However, it is usual to set each 8th bit so that each group of 8 bits has an odd number of bits set to 1.

2.2.1.2 Triple DES (3DES)

3DES is an enhancement of DES; it is 64 bit block size with 192 bits key size. In this standard the encryption method is similar to the one in the original DES but applied 3 times to increase the encryption level and the

DOI 10.17148/IJARCCE.2016.5506

average safe time. It is a known fact that 3DES is slower than other block cipher methods.

2.2.1.3 AES

AES is a block cipher .It has variable key length of 128, 192, or 256 bits; default 256. It encrypts data blocks of 128 bits in 10, 12 and 14 round pending on the key size[16]. AES encryption is fast and flexible; it can be implemented on various platforms especially in small devices. Also, AES has been carefully tested for many security applications.

2.2.1.4 BlowFish

Blowfish algorithm is the important type of the symmetric key encryption that has a 64 bit block size and a variable key length from 32 bits to 448 bits in general. Since the key size is larger it is complex to break the code in the blowfish algorithm. Moreover it is vulnerable to all the attacks except the weak key class attack.

2.2.1.5 RC4

RC4 is recognized as the most commonly utilized stream cipher in the world of cryptography. RC4 has a use in both encryption and decryption while the data stream undergoes XOR together with a series of generated keys.

It takes in keys of random lengths and this is known as a producer of pseudo arbitrary numbers. The output is then XORed together with the stream of data in order to generate a newly-encrypted data.

2.2.2 Asymmetric Key Encryption

2.2.2.1 RSA

Rivest-Shamir-Adelman is the most commonly used public key encryption algorithm. It can be used to send an encrypted message without a separate exchange of secret keys. It can also be used to sign a message. In RSA, this asymmetry is based on the practical difficulty of factoring the product of two large prime numbers, the factoring problem. RSA computation occurs with integers modulo n = p * q, for two large secret primes p, q.

To encrypt a message m, it is exponentiated with a small public exponent e. For decryption, the recipient of the cipher text c = me (mod n) computes the multiplicative reverse d = e-1 (mod (p-1)*(q-1)) (we require that e is selected suitably for it to exist) and obtains cd = m e * d = m (mod n). The key size should be greater than 1024 bits for a reasonable level of security.

2.2.2.2 Diffie-Hellman Algorithm

The Diffie–Hellman key exchange method allows two parties that have no prior knowledge of each other to jointly establish a shared secret key over an insecure communications channel.

This key can then be used to encrypt subsequent communications using a symmetric key cipher. The Diffie-Hellman protocol is generally considered to be secure when an appropriate mathematical group is used

CONCLUSION

Cryptography is an emerging technology which is important for network security. Some well-known cryptographic algorithms have been analyzed in this paper to demonstrate the basic differences between the existing encryption techniques. Regardless of the mathematical theory behind an algorithm, the best algorithm are those that are well-known and well-documented because they are well-tested and well studied. In-fact time is the only true test of good cryptography, any cryptographic scheme that stays in use year after year is most likely good one. The strength of cryptography lies in the choice of the key; longer key resist attack better than shorter keys.

REFERENCES

[1]. William Stallings “Network Security Essentials (Applications and Standards)”, Pearson Education, 2004.
[2]. W. Stallings. “Cryptography and Network Security”, Prentice Hall, 1995.
[3]. National Bureau of Standards, “Data Encryption Standard,” FIPS Publication 46, 1977.
[4]. E. Thambiraja, G. Ramesh, Dr. R. Umarani, “A Survey on Various Most Common Encryption Techniques” International Journal of Advanced Research in Computer Science and Software Engineering, VOL. 2
[5]. Sumedha Kaushik, Ankur Singhal, “Network Security Using Cryptographic Techniques” International Journal of Advanced Research in Computer Science and Software Engineering, VOL.2, Issue 12 December 2012, Page 105-107.
[6]. Vishwa gupta, Gajendra Singh, Ravindra Gupta, “Advance cryptography algorithm for improving data security” International Journal of Advanced Research in Computer Science and Software Engineering, VOL.2, Issue 1 January 2012.
[7]. “Comparative Analysis of Performance Efficiency and Security Measures of Some Encryption Algorithms” International Journal of Engineering Research and Applications (IJERA), VOL.2, Issue 3,May- Jun 2012, Page 3033-3037.