International Journal of Enhanced Research in Management & Computer Applications
ISSN: 2319-7471, Vol. 4 Issue 10, October-2015

Analysis of Symmetric and Asymmetric Cryptography and their Issues

Anil Kumar
Programmer-Cum-Networking Engineer,
Transport Department, Govt of Haryana, India

ABSTRACT

Cryptography plays a major role in securing data. 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 in information security as it refers to all hardware and software function, characteristics, features, 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 together provide the fundamentals for trusted e-commerce and secure communication. There is a broad range of cryptographic algorithms that are used for securing networks and presently continuous researches on the new cryptographic algorithms are going on for evolving more advanced techniques for secures communication.

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

1. INTRODUCTION

Cryptography is the scientific study of secret writing. The history of Cryptography dates back to about 2000 B.C. Cryptography is considered as one of the oldest methods employed by ancient civilizations for secret communications. The Egyptians in particular is known to have used cryptography on the tombs of deceased kings and rulers. The Caesar Cipher, which was invented by Julius Caesar to send confidential messages to his generals during wars , is known to be one of the famous methods in the history of Cryptography . The Caesar cipher was very simple and fast which implemented the substitution cipher method with alphabet shifts of 3 , which would for example shift an “A” to “D” or a “B” to “E”. In modern times, cryptography follows complex scientific approach and the algorithms are designed for cryptosystems based on computational hardness which makes it difficult for adversary to break into the system. More generally a modern cryptosystem is about the design and analysis of various methods that are related to various aspects in data security, integrity and authentication. The following figure illustrates the working of a crypto-system in general –

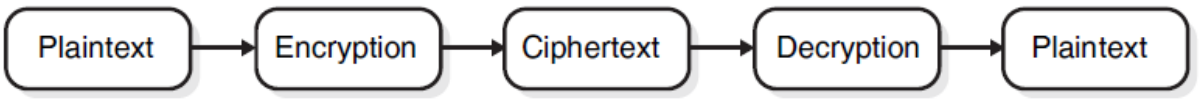

Fig 1: Working principle of a cryptosystem

To assure that a particular system is secure , Cryptanalysts try to break the methods used in building the system. Cryptography and Cryptanalysis together constitute to define what is known as „Cryptology“. This paper will discuss some of the most popular crypto algorithms in modern era, their working principle , their security levels and the attacks that could possibly break a certain system.

2. TERMS USED IN CRYPTOGRAPHY

2.1 Plain Text

The original message that the person wishes to communicate with the other is defined as Plain 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.

2.2 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".

2.3 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.

2.4 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.

2.5 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 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 etc[2].

3. GOALS OF CRYPTOGRAPHY

A. Confidentiality: Renders the information unintelligible except by authorized entities
B. Integrity : Data has not been altered in an unauthorized manner since it was created, transmitted, or stored
C. Authentication :Verifies the identity of the user or system that created information
D. Authorization : Upon proving identity, the individual is then provided with the key or password that will allow access to some resource
E. Nonrepudiation : Ensures that the sender cannot deny sending the message.

4. TYPES OF CRYPTOGRAPHY

The modern cryptography is classified into two types –Symmetric Key Cryptography and Asymmetric Key Cryptography.

A. Symmetric Key Cryptography: In Symmetric Key algorithms, a single key is used for both encryption and decryption process. Both the parties must agree on the secret key before the actual exchange of data takes place. The sender uses this key and an encryption algorithm to encrypt data; the receiver uses the same key and the corresponding decryption algorithm to decrypt the data. Symmetric Key Ciphers are broadly classified into two categories –Stream Ciphers and Block Ciphers. A stream cipher breaks the plaintext X into successive characters or bits x1, x2,.. and enciphers each xi with the ith element ki of a key stream K = k1,k2. . . whereas , a block cipher breaks X into successive blocks (each block is typically several characters long.) X1,X2 . . . . . and enciphers each Xi with the same key K; that is , EK(X) = EK(X1)EK(X2) . . .

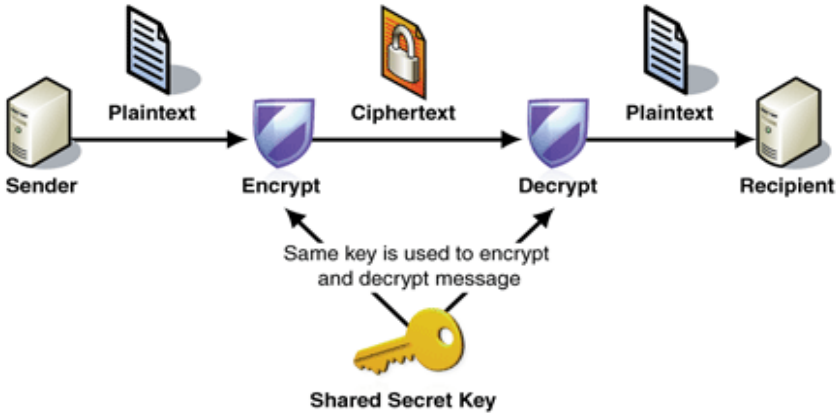

Fig 2 : Symmetric Key Cryptography

Strengths

- Much faster (less computationally intensive) than asymmetric systems
- Hard to break if using a large key size

Weaknesses

- Requires a secure mechanism to deliver keys properly
- Each pair of users needs a unique key, so as the number of individuals increases, so does the number of keys, possibly making key management overwhelming
- Provides confidentiality but not authenticity or nonrepudiation

Examples of Symmetric Algorithms

- Data Encryption Standard (DES)
- Triple-DES (3DES)
- Blowfish
- IDEA (International Data Encryption Algorithm)
- RC4, RC5, and RC6
- Advanced Encryption Standard (AES)

B. Asymmetric or Public-key cryptography: Asymmetric Cryptography refers to a cryptographic system requiring two separate keys, one to encrypt the plaintext, and one decrypt the cipher text. One of these keys is published or public and the other is kept private. Public key algorithms, unlike symmetric key algorithms, do not require a secure initial exchange of secret keys between the parties. Public-key cryptography is used as a method of assuring the confidentiality, authenticity and non-repudiability of electronic communications and data storage.

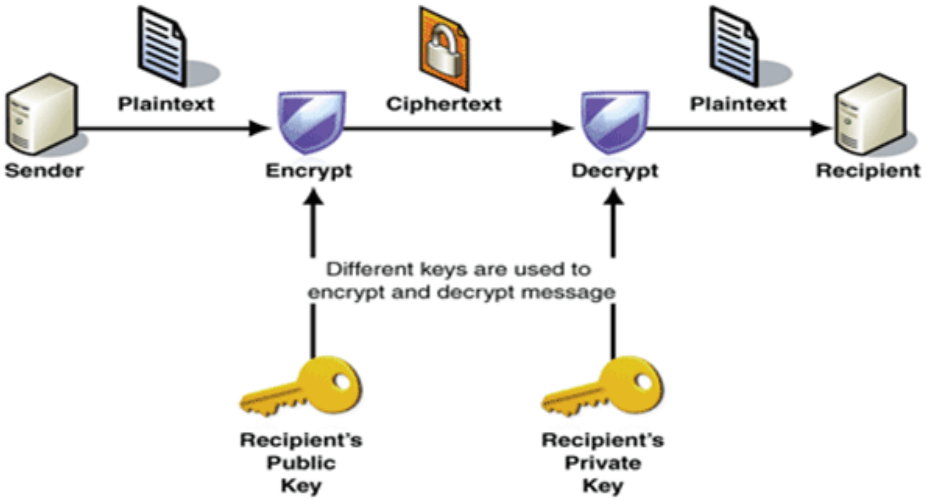

Fig 3 : Asymmetric Key Cryptography

Strengths

- Better key distribution than symmetric systems
- Better scalability than symmetric systems
- Can provide authentication and nonrepudiation

Weaknesses

- Works much more slowly than symmetric systems
- Mathematically intensive tasks

Examples of Asymmetric Key Algorithms

- Diffie-Hellman
- RSA (Rivest-Shamir-Adleman)
- El Gamal
- Elliptic curve cryptosystem (ECC)
- Digital Signature Algorithm (DSA)
- Merkle-Hellman Knapsack

SUMMARIZATION

Attribute	Symmetric	Asymmetric
Keys	One key is shared between two or more entities.	One entity has a public key, and the other entity has the corresponding private key.
Key exchange	Out-of-band through secure mechanisms.	A public key is made available to everyone, and a private key is kept secret by the owner.
Speed	Algorithm is less complex and faster.	The algorithm is more complex and slower.
Use	Bulk encryption, which means encrypting files and communication paths.	Key distribution and digital signatures.
Security service provided	Confidentiality.	Authentication and nonrepudiation.

Core Cryptographic Processes

	Confidentiality	Authentication
Symmetric Key Encryption	Applicable. Sender encrypts with key shared with the receiver.	Not applicable.
Public Key Encryption	Applicable. Sender encrypts with receiver's public key. Receiver decrypts with the receiver's own private key.	Applicable. Sender (supplicant) encrypts with own private key. Receiver (verifier) decrypts with the public key of the true party, usually obtained from the true party's digital certificate.

CONCLUSION

Actually, it's difficult to compare the cryptographic strengths of symmetric and asymmetric key encryptions. Even though asymmetric key lengths are generally much longer (e.g. 1024 and 2048) than symmetric key lengths (e.g. 128 and 256), it doesn't, for example, necessarily follow that a file encrypted with a 2048-bit RSA key (an asymmetric key) is already tougher to crack than a file encrypted with a 256-bit AES key (a symmetric key). Instead, it would be more appropriate to compare asymmetric and symmetric encryptions on the basis of two properties:

- Their computational requirements, and
- Their ease of distribution

Symmetric key encryption doesn't require as many CPU cycles as asymmetric key encryption, so you can say it's generally faster. Thus, when it comes to speed, symmetric trumps asymmetric. However, symmetric keys have a major disadvantage especially if you're going to use them for securing file transfers. Because the same key has to be used for encryption and decryption, you will need to find a way to get the key to your recipient if he doesn't have it yet. Otherwise, your recipient won't be able to decrypt the files you send him. However way you do it, it has to be done in a secure manner or else anyone who gets a hold of that key can simply intercept your encrypted file and decrypt it with the key. The issue of key distribution becomes even more pronounced in a file transfer environment, which can involve a large number of users and likely distributed over a vast geographical area. Some users, most of whom you may never have met, might even be located halfway around the world. Distributing a symmetric key in a secure manner to each of these users would be nearly impossible.

Asymmetric key encryption doesn't have this problem. For as long as you keep your private key secret, no one would be able to decrypt your encrypted file. So you can easily distribute the corresponding public key without worrying about who gets a hold of it (well, actually, there are spoofing attacks on public keys but that's for another story). Anyone who holds a copy of that public key can encrypt a file prior to uploading to your server. Then once the file gets uploaded, you can decrypt it with your private key.

Getting the best of both worlds with hybrid cryptosystems

Because both symmetric and asymmetric key cryptography have their own advantages, modern file transfer systems typically employ a hybrid of the two. Some hybrid cryptosystems are: SSL (used in FTPS and HTTPS), SSH (used in SFTP), and OpenPGP, all of which are supported by JSCAPE MFT Server. Hybrid cryptosystems employed in an SFTP or FTPS server use asymmetric keys to initially encrypt symmetric keys known as session keys. The session keys are then the ones used to encrypt the actual data. As its name implies, a session key is only used in one session. After the session, the key is simply discarded. That's a good thing because even if a session key is compromised, only data sent within that particular session will be at risk.

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,Issue 7 July 2012, Page 226-233.
[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 December2012, Page 105-107.
[6]. Vishwagupta, 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]. Nagamalleswara Rao. Dasari, Vuda Sreenivasarao, “Performance of Multi Server authentication and Key Agreement Withuser Protection In Network Security” International Journal on Computer Science and Engineering, VOL.2, Issue 05 2010, Page 1705-1712.
[8]. AL. Jeeva, Dr. V. Palanisamy, K. Kanagaram, “Comparative Analysis of Performance efficiency And Security Measures Ofsome Encryption Algorithms” International Journal of Engineering Research and Applications(IJERA), VOL.2, Issue 3,May-Jun 2012, Page 3033-3037.
[9]. G. Ramesh, R. Umarani, “Performance Analysis of Most Common Encryption Algorithms on Different Web Browsers “I.J. Information Technology and Computer Science, Issue Nov 2012, Page 60-66.
[10]. Zirra Peter Buba& Gregory Maksha Wajiga “Cryptographic Algorithms for Secure Data Communication “in International Journal of Computer Science and Security IJCSS, Volume no 5, Issue 2.
[11]. Daemen, J., and Rijmen, V. "Rijndael: The Advanced Encryption Standard." Dr. Dobb's Journal, March 2001.
[12]. http://en.wikipedia.org/wiki/Symmetric-key_algorithm
[13]. http://en.wikipedia.org/wiki/Public-key_cryptography
[14]. http://www.laits.utexas.edu/~anorman/BUS.FOR/course.mat /SSim/history.html
[15]. http://www.queen.clara.net/pgp/art6.html
[16]. http://resources.infosecinstitute.com/role-of-cryptography/
[17]. http://www.idga.org/communications-engineering-and-it/articles /understanding-cryptography-in-modern-military-comm/