Communications Cryptography

Othman O. Khalifa*, MD Rafiqul Islam*, S. Khan* and Mohammed S. Shebani**

*International Islamic University Malaysia
Kulliyyah of Engineering
Electrical and Computer department
Jalan Gombak
E-mail: khalifa@iiu.edu.my

**Higher Electronic Institute
Beniwalid, Libya

Abstract- In today's information age, communications play an important role which is contributed to the growth of technologies. Electronic security is increasingly involved in making communications more prevalent. Therefore, a mechanism is needed to assure the security and privacy of information that is sent over the electronic communications media is in need. Whether the communications media is wired or wireless, both can be not protected from unauthorized reception or interception of transmission. The method of transforming the original information into the unreadable format is called encryption and decryption of information. The study of encryption and decryption is known as Cryptography. Cryptography or communication by using secret code was used by the Egyptians some 4000 years ago. However, the science of cryptography was initiated by Arabs since 600s. Cryptography becomes vital in the twentieth century where it played a crucial role in the World War I and II. This paper focuses on the analysis of the two types of key cryptography exists, based on the availability of the key publicly: Private key Cryptography, and Public Key Cryptography. Both the sender and the recipient share a key that must be kept private. In the former case the sender and recipient share a private key between the two of them which must be distributed first before actual communications take place. This analysis shows how much complicated and difficult to do properly. The most famous example of this type of cryptography is the Data Encryption Standard (DES). In the Public Key Cryptography, each party has two sets of keys; one key is known to the public while the other is kept secret to the owner

1. Introduction

Cryptography, in Greek, literally means hidden writing, or the art of changing plain text message [1][4][5]. Cryptography is used increasingly by businesses, individuals and the government for ensuring the security and privacy of information and communications. Cryptography's use by criminals is becoming widespread as well. The same aspects of cryptography that make it useful for security and privacy make it particularly troublesome for law enforcement. The use of cryptography by criminals can prevent law enforcement from obtaining information needed for the prevention and prosecution of crime. The international organizations have acted to regulate cryptography and protect the legitimate interests of law enforcement, while attempting to balance the needs of legitimate users of cryptography. Given the international nature of many crimes, such international protection of law enforcement interests will be necessary to make domestic protections of these interests meaningful. While modern cryptography is a vast and complicated field, the basics are easy to understand. Cryptography includes four commonly used tools: a cipher, a key exchange mechanism, a hashing core and a random-number generator. Communications Cryptography may be in wire-based networks, physical security was often adequate. A wire running from points A to B would be good enough to defeat eavesdroppers, and cryptography would be added if it was felt that anybody else had access to that wire. However, for wireless applications where data are beamed, it is difficult to ensure that only the intended recipient receives the data. For many cases, it does not matter if you are just playing a wireless game between two telephones, which cares if other people can intercept the data. In addition, if you are beaming sensitive documents or carrying out personal conversations, the situation is different, especially with the merging of 3G and e-commerce [1][2][11]. In general, without cryptography, that is essentially what would happen within e-commerce and wireless networks. The situation is not that bad many different cryptographic methods are used in conjunction with wireless networks to preserve users' privacy.

Cryptography can be classifies into Symmetric and asymmetric encryption algorithms as shown in Figure 1. A symmetric encryption algorithm consists of a pair of functions, encrypt and decrypt. If plaintext is encrypted with key K and the resulting ciphertext is decrypted with key K then the original plaintext is

0-7803-8671-X/04/$20.00 ©2004 IEEE.

recovered. The most popular symmetric encryption algorithm is the Data Encryption Standard (DES). It was developed by IBM in 1976 in response to the challenge to produce an encryption [6][7][8]. Algorithm that could be made public and still is secure. Even though repeated attempts have been made to replace it, remains secure when properly used. Asymmetric encryption algorithm, also known as a public key crytosystem (PKS), the keys used for the encrypt and decrypt functions are different, and it is computationally infeasible to obtain the decryption key from the encryption key. This allows the encryption key to be made public while the decryption key is kept private. The keys are known as the public key and the private key. The corresponding terminology for a key in a symmetric cryptosystem is secret key. Thus anyone can encrypt messages, but only the holder of the private key can read them. The most popular public key cryptosystem is RSA, named after its inventors Rivest, Shamir, and Adleman [9][10][11]. It was produced in 1978 in response to a challenge in 1976 to find a PKS.

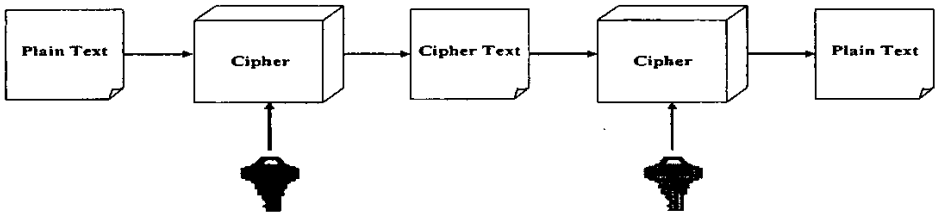

Figure 1, Asymmetric Encryption

2. Security Risks

In recent years, more and more businesses make use of communication networks. Share potential information and therefore sensitive data is located in communications network transmissions that are connected all over the world [2][4][7][11]. This commitment to data communication has increased the vulnerability of organization assets. Computer fraud is becoming one of the most popular crimes in our days. Since a network without security mechanisms is like an office building with open doors, the network owner has to make sure to lock those doors and give keys only to those people whom he wants to share the information with. For many people, communications security just means preventing unauthorized access, such as preventing a hacker from breaching into a network. Security is more than that.

3. Cryptography Objectives

Cryptography is the science of writing in secret code and is an ancient art; the first documented use of cryptography in writing dates back to circa 1900 B.C. when an Egyptian scribe used non-standard hieroglyphs in an inscription. Some experts argue that cryptography appeared spontaneously sometime after writing was invented, with applications ranging from diplomatic missives to war-time battle plans [5][6][8]. It is no surprise, then, that new forms of cryptography came soon after the widespread development of computer communications. In data and telecommunications,

cryptography is necessary when communicating over any untrusted medium, which includes just about *any* network, particularly the Internet.

Within the context of any application-to-application communication, there are some specific security requirements, including:

- *Authentication:* The process of proving one's identity. (The primary forms of host-to-host authentication on the Internet today are name-based or address-based, both of which are notoriously weak.)
- *Privacy/confidentiality:* Ensuring that no one can read the message except the intended receiver.
- *Integrity:* Assuring the receiver that the received message has not been altered in any way from the original.
- *Non-repudiation:* A mechanism to prove that the sender really sent this message.

Cryptography, then, not only protects data from theft or alteration, but can also be used for user authentication. There are, in general, three types of cryptographic schemes typically used to accomplish these goals: secret key (or symmetric) cryptography, public-key (or asymmetric) cryptography, and hash functions, each of which is described below. In all cases, the initial unencrypted data is referred to as *plaintext*. It is encrypted into *ciphertext*, which will in turn (usually) be decrypted into usable plaintext [10][11][12].

In many of the descriptions below, two communicating parties will be referred to as Alice and Bob; this is the common nomenclature in the crypto field and literature. If there is a third or fourth party to the communication, they will be referred to as Carol and Dave. Mallory is a malicious party and Eve is an eavesdropper.

3. Cryptography and Communications

Communication is an essential part of life; it marks the progress of human beings. Traditional media for communication are the sending of letters through the Post Office, talking over the phone through the Telecommunications Company, or more commonly to speak directly with the other person. These traditional media have existed for a long period of time and special provisions have been made so that people can communicate in a secure way, either for personal or for business communication [11][12]. For face to face communication, people can recognize each other's physical characteristics or they can compare hand written signatures with that of official documents like an ID card. Mimicking all of the physical characteristics of a person is difficult. People can accept with a high level of certainty the identity of their colleague. The bottom line is that for each communication medium, there is a transitional period when specific laws and technologies are set in order for people to communicate securely and transparently. The Internet, as a network that interconnects networks of computers around the world, is a new communication medium that is substantially different from existing ones. For example, on the Internet, the communicating parties do not have physical contact. It is rather more difficult for one to disguise oneself to someone else, imitates the voice and other aspects behavior and gets information on prior common experiences. On-line transactions do not impose such barriers for illegitimate transactions. Additionally, on the Internet, one can automate the same type of fraud bringing higher gains and a bigger incentive. The law and the technologies to let transparent and secure communication have not been fully defined or set yet. Cryptography has provided us with digital signatures that resemble in functionality the hand-written signatures and digital certificates that relate to an ID card or some other official document. However, in order to use these technologies, we need to make the necessary provisions so that their usage is equally transparent and secure.

4. Cryptographic Algorithms

Cryptography has several differences from pure mathematics. While a mathematician may use A and B to explain an algorithm, a cryptographer may use the fictious names Alpha and Beta. Suppose Alpha wants to send a message to his bank to transfer money. He would like the message to be private, since it includes information such as his account number and transfer amount. One solution is to use a cryptographic algorithm, a technique that would transform his message into an encrypted form, unreadable except by those for whom it is intended. When encrypted, the message can only be interpreted through the use of the corresponding secret key. Without the key the message is useless: good cryptographic algorithms make it so difficult for intruders to decode the original text that it isn't worth their effort [8][9][11]. Some of Encryption Algorithm is shown in Tble.1. There are two categories of cryptographic algorithms: conventional and public key. Conventional cryptography, also known as symmetric cryptography, requires that the sender and receiver share a key: a secret piece of information that is used to encrypt or decrypt a message. If this key is secret, then nobody other than the sender or receiver can read the message. If Alpha and the bank each has a secret key, then they may send each other private messages. The task of privately choosing a key before communicating. Public key cryptography, also known as asymmetric cryptography, solves the key exchange problem by defining an algorithm which uses two keys, each of which can be used to encrypt a message. If one key is used to encrypt a message, then the other must be used to decrypt it. This makes it possible to receive secure messages by simply publishing one key (the public key) and keeping the other secret (the private key). Anyone may encrypt a message using the public key, but only the owner of the private key is able to read it. In this way, Alpha may send private messages to the owner of a key-pair (the bank) by encrypting it using their public key. Only the bank can decrypt it.

Table 1. Summary of Encryption Algorithm

Algorithm	Type	Key Size	Features
DES	Block Cipher	56 bits	Most Common, Not strong enough
TripleDES	Block Cipher	168 bits (112 effective)	Modification of DES, Adequate Security
Blowfish	Block Cipher	Variable (Up to 448 bits)	Excellent Security
AES	Block Cipher	Variable (128, 192, or 256 bits)	Replacement for DES, Excellent Security
RC4	Stream Cipher	Variable (40 or 128 bits)	Fast Stream Cipher, Used in most SSL implementations

4.1 Data Encryption Standard (DES)

Goal of DES is to completely scramble the data and key so that every bit of cipher text depends on every bit of data and ever bit of key. It is a block Cipher Algorithm, encodes plaintext in 64 bit chunks, One parity bit for each of the 8 bytes thus it reduces to

56 bits. It is the most used algorithm. DES developed by IBM in the early 1970s. Standard approved by US National Bureau of Standards for Commercial and nonclassified US government use in 1993. DES is an iterated block cipher, iterated means multiple repetitions of a simple encryption algorithm. DES has 16 rounds. Where Block cipher encrypts in fixed-size blocks. DES uses 64-bit (8-byte) blocks. At its simplest level, DES is a combination of the two basic techniques of cryptography: confusion and diffusion. DES follows a strict avalanche criteria. Every bit of the key and every bit of the plaintext affects every bit of the ciphertext. It has different keys for encryption and decryption. Eavesdropper sees the ciphertext and one of the keys. All of the security is in one key; there is none in the algorithm or in the second key.

5. Discussions and Conclusions

Cryptography is a particularly interesting field because of the amount of work that is, by necessity, done in secret. The irony is that today, secrecy is *not* the key to the goodness of a cryptographic algorithm. Regardless of the mathematical theory behind an algorithm, the best algorithms are those that are well-known and well-documented because they are also 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 a good one. The strength of cryptography lies in the choice (and management) of the keys; longer keys will resist attack better than shorter keys. The basic concepts, characteristics, and goals of various cryptographic have been discussed. The essential parts of Cryptography in communications systems are shown. How this makes them especially attractive as a potential platform to implement cryptographic algorithms.

6. References

[1] I. Vajda, *Extraction of random bits for cryptographic purposes,* Tatra Mountains Mathematical Publications, 2002, vol. 25, pp. 83-99

[2] Ferguson, N. and B. Schneier, *Practical Cryptography.* New York: John Wiley & Sons, 2003

[3] Barr, T.H. *Invitation to Cryptology.* Upper Saddle River (NJ): Prentice Hall, 2002.

[4] Bauer, F.L. *Decrypted Secrets: Methods and Maxims of Cryptology,* 2nd ed. New York: Springer Verlag, 2002.

[5] D.E.R. Denning, *Cryptography and Data Security,* Addison-Wesley, 1982.

[6] E. Kranakis, *Primality and Cryptography,* Wiley, 1986.

[7] A.G. Konheim, *Cryptography: A Primer,* John Wiley, 1981.

[8] J. Seberry and J. Pieprzyk, *Cryptography: An Introduction to Computer Security,* Prentice-Hall, 1989.

[9] D. Welsh, *Codes and Cryptography,* Oxford Science Publications, 1988.

[10] D. R. Stinson, *Cryptography: Theory and Practice,* CRC Press, 1995.

[11] B. Schneier, *Applied Cryptography,* Wiley, 1994.

[12] M. Y. Rhee, *Cryptography and Secure Communications,* McGraw-Hill, 1994.