A Review on Cryptography Mechanisms

Prof ML Sharma
Department of Electronics & Communication
Bhai Gurdas Institute of Engineering & Technology, Sangrur, India
madansharma.20@gmail.com

Er. Sheetal Atri
Department of Electronics & Communication
Bhai Gurdas Institute of Engineering & Technology, Sangrur India
atri.sheetal@gmail.com

Abstract
In today’s information age, communications play an important role which 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. Cryptography can be classified into symmetric and asymmetric encryption algorithms as shown in Figure. A symmetric encryption algorithm consists of a pair of functions, encrypt and decrypt. If plaintext is encrypted with key K and the resulting cipher text is decrypted with key K then the original plaintext 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. 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.

Index Terms: Cryptography, Encryption, Decryption.

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. 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 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 cryptosystem (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. It was produced in 1978 in response to a challenge in 1976 to find PKS.

2. Cryptography Objectives
Cryptography is the science of writing in secret code within the context of any application-to-application communication, there are some specific security requirements, including:
- **Authentication**: The process of proving one’s identity.
- **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 referred to as plaintext.

3. Cryptographic Algorithms
Cryptography has several differences from pure mathematics. While a mathematician may use A and B to explain a algorithm, a cryptographer may use the fictitious names A and B. Suppose A wants to send a message to his bank to transfer money. He could 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 intended. When encrypted, the message can only be interpreted through the use of a key corresponding to the original text that it isn't worth their effort. Some of Encryption Algorithm is shown in Table. Some of the categories of cryptographic algorithms are conventional and public key cryptography. Also known as symmetric cryptography requires that the sender and receiver share a secret piece of information that is used to encrypt or decrypt a message. If the receiver is the only other than the sender or receiver can read the message. If A has a secret key that he can send to the bank, each have a Secret key. Then he may send each other private messages. The task of privately choosing a key before communicating is called asymmetric cryptography. Anyone can use the public key, but only the owner of the private key is able to read it.

4. Data Encryption Standard (DES)
Goal of DES is to completely scramble the data and key so that every bit of ciphertext depends on every bit of data and every 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. It was adopted as a standard by the U.S. National Bureau of Standards for commercial and classified government use in 1993. DES is an
iterated block cipher, iterated means multiple repetitions of a simple encryption algorithm. DES has 16 rounds. Where a block cipher encrypts in fixed-size blocks, DES uses 64-bit (and byte) blocks. At its simplest level, DES is a combination of two basic techniques of cryptography: confusion and diffusion. DES follows strict avalanche criteria. Every bit of the key and every bit of the plaintext affects every bit of the cipher text. It has different keys for encryption and decryption. An eavesdropper sees the ciphertext and one of the keys. All of the security is in one key; there is no security in the second key.

5. Discussions and Conclusions
Cryptography is a particularly interesting field because it amounts to work that is done in secret. The irony is that today, secrecy is not the key to the goodness of an algorithm. Regardless of it being mathematical, t heory behind an algorithm, one has to use smart algorithms a t hose that are well known and well documented because they are also well-tested and well-studied! In fact, time is the only Vu e test of a cryptographic scheme that stays in use year after year is most likely a goo d 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 at tractive as a potential platform to implement cryptographic algorithms.

6. References

Author’s Profile
Madan Lal received his three years Diploma from the Department of Electronics and Telecommunication Engineering of Bo ard of Technical Education, New Delhi in 1990. He received his B.Tech (ame) from D Department of Electronics and Communication Engineering of the Institution of Engineers (India) Kolkata in 1996. He received his Master of Technology from N ational Institute of Technology, Bhopal in 1999. He is currently pursing his further study from University Kurukshetra University Kurukshetra in 2008. He is presently Professor and Head, Department of Electronics and Telecommunication Engineering. He is a Chartered Engineer; He was the Chief of the Department of Electronics and Communication Engineering of Bh al Gurdas Institute of Engineering and Technology, Sangrur, India. His area of interest is wireless communication and circuit theory. He has contributed over 75 papers published in referred journals and presented in various international & national conferences.

Sheetal Atri received her four years Bachelor of Technology from the Department of Electronics Engineering from K. P. University Kurukshetra in 2008. She is currently pursuing her Masters in Electronics Engineering from Bhai Gurdas Institute of Engineering & Technology, Sangrur. She has contributed to some papers in international & national conferences. Her areas of interest are security in computer Networks, Fuzzy Logic System, and VHDL System. Now she is doing her thesis work on security in Computer Networks.