International Journal of Mathematics And its Applications
Volume 4, Issue 3–B (2016), 81–85.
ISSN: 2347-1557
Available Online: http://ijmaa.in/

International Journal of Mathematics And its Applications

# Cryptographic Protocol

**Research Article**

**Dr.S.Vasundhara[1]***

[1] Department Mathematics, G.Narayanamma Institute of Technology & Science For Women, Shaikpet, Hyderabad, India.

**Abstract:** Theoretical research in number theory has a long tradition. Since many centuries the main goal of these investigations is a better understanding of the abstract theory. Numbers are basic not only mathematics, but more generally for all sciences, a deeper knowledge of their properties is fundamental for further progress. Remarkable achievements have been obtained. Among the unexpected features of the recent developments in technology are the connections between classical arithmetic and on the one hand, and new methods for reaching a better security of data transmission on the other. In this paper we illustrate the aspect of the subject by showing the modern cryptography and its types like public key cryptography and private key cryptography its properties.

**Keywords:** Number theory, Cryptography.

## 1. Introduction

Information security [1] nowadays is a very important subject Governments, commercial businesses, and individuals are all demanding secure information in electronic documents, which is becoming preferred over traditional documents (paper and microfilm, for example). Documents in electronic form require less storage space, its transfer is almost instantaneous, and it is accessible via simplified databases. The ability to make use of information more efficiently has resulted in a rapid increase in the value of information.

However, information in electronic form faces potentially more damaging security threats. Unlike information printed on paper, information in electronic form can virtually be stolen from a remote location. It is much easier to alter and intercept electronic communication than its paper-based predecessors. Information security is described as the set of measures taken to prevent unauthorized use of electronic data, whether this unauthorized use takes the form of disclosure, alteration, substitution, or destruction of the data.

Several measures have been considered to provide these services but no single measure can ensure complete security. Of the various proposed measures, the use of cryptographic systems offers the highest level of security, together with maximum Flexibility. A cryptographic system transforms electronic data into a modified form. The owner of the information in modified form is now assured of its security features. Depending on the security services required, the assurance may be that the data cannot be altered without detection, or it may be that the data is unintelligible to all but authorized parties According to Koblitz [7], cryptography is the study of methods of sending messages in disguised form so that only the intended recipients can remove the disguise and read the message. The message we want to send is called the plain text

[*] *E-mail: vasucall123@gmail.com*

and the disguised message is called the cipher text. The plain text and the cipher text are written in some alphabet consisting of a certain number N of letters. The term letter can refer not only to the familiar A-Z, but also to numerals, blanks, punctuation marks, or any other symbols that we allow ourselves to use when writing the message. The process of converting a plaintext to a cipher text is called enciphering or encryption, and the reverse process is called deciphering or decryption. Historically much of this study focused on private key cryptosystem where the sender and receiver agreed on private keys for sending messages and receiving messages, and was primarily used for military and diplomatic reasons. However with these cryptosystems, anyone who knew enough to decipher messages could not only break a code but also determine the enciphering key. Enciphering and deciphering were considered equivalent sciences in a cryptosystem until the 1970 are when Whitefield Diffie and Martin Hellman invented public key cryptography

Cryptography [4] uses mathematics to encrypt and decrypt data. It enables people to store or transmit sensitive information via insecure network. On the other hand, cryptanalysis is the science of breaking secure communication. There are two persons, Alice and Bob, (the beginning of cryptography, A and B are used as (handy abbreviations of the names) communicate via an insecure channel in a secure way. The third person who is eavesdropper (Eve, abbreviated as E) should not be able to read the clear text or change it.

The goal of cryptography is to achieve the aim of allowing two people to exchange messages using cryptography which are not understood by other people (Wang, et al.). Figure 1 provides a sample model of a two-party communication using encryption. In this simple party, an entity is a person that sends, receives or manipulates data. Sender is an entity that legitimately transmits the information. On the other hand, a receiver is an entity that is the recipient of information. A receiver may be one of the entities that attempt to crush the information security service provided between the sender and receiver. An adversary plays the role either as the sender or the receiver. The other synonymous names for adversary are attacker, enemy, eavesdropper, opponent and intruder (Jesper2006 be able to read the clear text or change it.

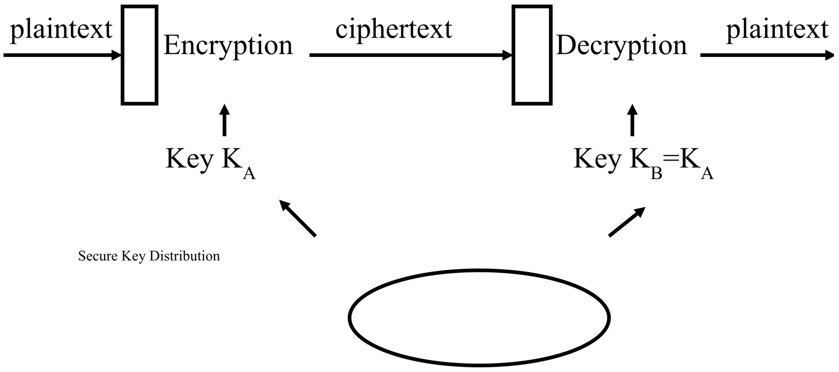

**Figure 1.** **Two party communications.**

The cryptographic strength can be measured by the needed resources and time in recovering the plain text. In order to encrypt the plaintext, cryptographic algorithm works in a combination with a key (private key) to resolve the cipher text. The cipher text differs from one to another because of different values used in each time. The security of encrypted data depends on the strength of the cryptographic algorithm and the confidentiality of the key [1].

## 1.1. Cryptographic Components

In order to secure messages, there are mathematical techniques that provide security services such as confidentiality, integrity, authentication and non-repudiation [2].

**Confidentiality:** Data is kept privately in an electronic communication. It is typically provided by encryption. It contains both protections of the transmitted data between two ends. It similarly secures the traffic flow analysis.

**Integrity:** Data is not changed in an unauthorized manner. It is typically provided by digital signature and encryption as well.

**Authentication:** Receiver determines its source to confirm the sender's identity by using something that you have or you know. Normally, it is done by using the sender public key. It is the same integrity provided by digital signature.

**Non-repudiation:** It ensures the sender and receiver from denying the sending or receiving of a message and the authenticity of their signature. Typically, it is provided by digital signature.

**Symmetric-key:** Symmetric-key [4] is a form of cryptography based on the sharing of a secret key between the parties who want to make communications. It is also called as secret-key. Secret-key is used in the both encryption and decryption process. In this form of cryptography, each party must trust each other and not tell the secret-key to anyone else.

The efficient encryption of large amount of data is the advantage of the symmetric-key, however, the problem appears when key management is over the large number of user needs Figure 2 is a sample of the symmetric-key. One method of secure communications is **symmetric key encryption**. The encryption key can be calculated from the decryption key and the decryption key can be calculated from the encryption key. A diagram of the cryptosystem is presented below:

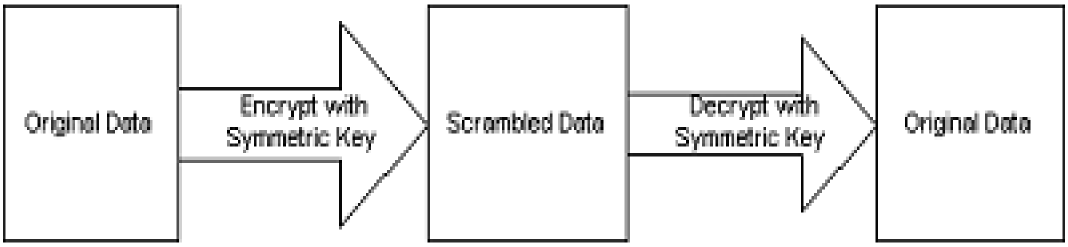

**Figure 2.** **Symmetric key Encryption.**

The protocol is described below:

(1). The sender and receiver agree on a how the key will encrypt / decrypt data.

(2). The sender and receiver agree on a symmetric key.

(3). The sender uses the key to encrypt a message.

(4). The sender sends the encrypted message to the receiver.

(5). The receiver uses the symmetric key to decrypt the message.

Symmetric key encryption is used for authentication and exchange of secret data on the World Wide Web. The World Wide Web uses this application because:

(1). People want to keep their data confidential. They don't want to advertise personal information like their credit card number.

(2). Hackers are out there and they will try to take your data and use it for their evil purposes.

(3). Anyone can tap into the communications on the World Wide Web, so it is open to attacks.

## 2. Advantages of Symmetric-key Cryptography

(1). Symmetric-key ciphers can be considered in order to have high rates of data throughput. Some hardware implementations get hundreds of megabytes per second for encryption rate. Software implementations get megabytes per second in the range.

(2). Symmetric-key ciphers contain keys that are relatively short.

(3). Symmetric-key encryption is noticed to have an extensive history. The knowledge in this area is obtained due to the success of the development of the digital computer, especially the design of the Data Encryption Standard (DES) in the early 1970s.

(4). Strong ciphers can be obtained by composing symmetric-key ciphers. Strong product ciphers can be constructed using simple transformations that are easy to analyze.

## 3. Disadvantages of Symmetric-key Cryptography

(1). The key must remain secret at both ends in communication.

(2). Key management is one of the big problems in large networks.

(3). Symmetric-key encryption typically requires a large key for the public verification function in Digital signature mechanisms (Menezes, et al. 1996)

In 1976, Diffie and Hellman presented Asymmetric-key cryptography which is commonly known as public-key cryptography.

### 3.1. Public-key Cryptography (Asymmetric-key)

In 1976, Diffie and Hellman presented public key cryptography (PKC), which is unlike traditional public-key. Diffie Hellman keys are not used to encrypt or decrypt the message. They are used to create a single shared secret key between the units.

Public key cryptography contains two keys, which are public and private keys. A situation is assumed where Alice wants to send a message to Bob. Alice uses Bob's Public key to encrypt a message and her private key to sign the message. Bob (receiver) uses his Private Key to decrypt the message and he uses Alice's Public Key to verify the signature. The standard bodies have set the key size of the encryption key, in order to provide the desired security. The key size decides the hardship of recovering the encrypted data computationally without the use of the secret key. A scenario of a public key is depicted in Figure 3. The key pair *(e, d)* is selected by Bob. 'e' is the public key that Bob sends to Alice over any channel but the private key 'd' is kept. Alice encrypts the sending message to Bob using Bob's public-key. Bob decrypts the ciphertext *'c'* using the *'d'*.

**Public Key Encryption** involves a pair of keys. One key is public, the other key is private. The public key is published and can be easily found. The private key is kept secret. However, there is a special relationship between the public key and the private key that is shown by the following two drawings:

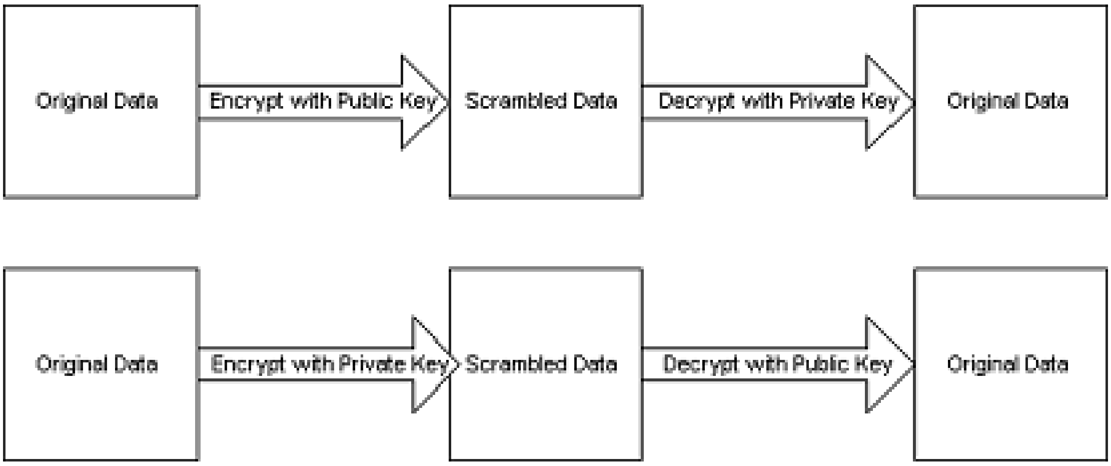

**Figure 3.**

The original data can be encrypted with one key and decrypted with the other key. While it is mathematically possible to use either key to encrypt or decrypt, there are definite reasons to use one method instead of the other. If the top method is used, data will be encrypted with a public key, and only the individual that has the corresponding private key can decode the information. Since the private key is a secret, there is only one individual that can decode the information. If the bottom method is used, then anyone can decode the message. The public keys are published and readily available. The keys can be published into a database on a server that is accessible from the internet. Therefore, more secure transmissions should use public key encryption.

## References

[1] Certicom, Standards for Efficient Cryptography, SEC 1: Elliptic curve

[2] Cole, Eric, Jason Fossen, Stephen Northcutt and Hal Pomeranz, *SANS Security Essentials with CISSPCBK*, Version 2.1. USA: SANS Press, (2003).

[3] W.Diffie and M.E.Hellman, *New Directions in Cryptography*, IEEE Transactions on Information Theory, 22(6)(1976), 644-654.

[4] Federal Information Processing Standards, Advanced Encryption Standard (AES), FIPS PUB 197, (2001).

[5] N.Koblitz, *CM-Curves with Good Cryptographic Properties*, Advances in Cryptology-CRYPTO'91, Springer-Verlag Berlin Heidelberg, (1992), 279-287

[6] Joan Feigenbau, *An introduction to elliptic curve, cryptography.*

[7] N.Koblitz, *A course in Number theory and cryptography*, $2^{nd}$Ed., Springer-Verlag New York, (1994).

[8] W.Stalling, *Network and Internet work Scurity*, IEEE Press, (1995).

[9] B.Schneier, *Applied Cryptography*, New York: Wiley Publishing, (1996).