# Chapter 61
# Network Security Approaches in Distributed Environment

**Keshav Sinha**
*Birla Institute of Technology, India*

**Partha Paul**
*Birla Institute of Technology, India*

**Amritanjali**
*Birla Institute of Technology, India*

## ABSTRACT

*Distributed computing is one of the thrust areas in the field of computer science, but when we are concerned about security a question arises, "Can it be secure?" From this note, the authors start this chapter. In the distributed environment, when the system is connected to a network, and the operating system firewall is active, it will take care of all the authentication and access control requests. There are several traditional cryptographic approaches which implement authentication and access control. The encryption algorithms such as Rijndael, RSA, A3, and A5 is used for providing data secrecy. Some of the key distribution techniques have been discussed such as Diffie Hellman key exchange for symmetric key, and random key generation (LCG) technique is used in red-black tree traversal which provides the security of the digital contents. The chapter deals with the advanced versions of the network security techniques and cryptographic algorithms for the security of multimedia contents over the internet.*

## INTRODUCTION

Cryptology is defined from Greek word kryptós and lógos which means hidden word. Cryptography and Cryptanalysis is an amalgamation of cryptology. The art of hiding the readable data (according to the perception of a human being) into a non-readable format is known as cryptography. Cryptanalysis is the opposite of cryptography, where it converts the non-readable data into readable form, without knowing the algorithm of encryption. The word cryptography is originated from the Greek word "kryptós", which

DOI: 10.4018/978-1-7998-7705-9.ch061

means the art of writing or solving codes secretly. The first citation of the cryptography technique was in the form of hieroglyphics, dated back to 1900 B.C, that is during the time of Egyptian. In the year 1799, a French soldier found a black basalt slab, which was inscribed with the ancient script. The stone was in the form of irregular shape which contains three different types of scripts (i) Greek, (ii) Egyptian hieroglyphics, and (iii) Egyptian demotic. In the year 1790-1832, Jean-Francois Champollion was the first person who cracked the hieroglyphics code by using a Greek guide. Since the year 1802, the Rosetta stone has been kept in the British Museum, London. Modern day's cryptography is very different from ancient cryptography. Now the encryption algorithm is very complicated and require huge computational time. Cryptography algorithm uses the number of shift rounds and XOR operation for decipherment. Due to the advancement in computing power, the future cryptographic algorithm works on quantum computation speed allowing use of large key size. The DNA cryptography is one of the kind of cryptographic technique which uses the perplexing genetic data for hiding and improve the genetic secrecy in the sequencing process. The term cryptology is offend used in the field of data transmission and storage.

## Principles of Security

There are several types of security attacks are performed by hackers in real life. To tackle those attacks, there are sets of security principles which will help us to understand and find the possible solutions to those problems which is caused by the attackers. There are six principles of cryptography and security.

1. **Confidentiality:** It specifies that only the sender and the authentic user should be able to access the data. No third party will access the data without authorization.
2. **Authentication:** It is the mechanism to establishing a secure (authentic) connection between sender and receiver. It is mainly used in electronic transactions, and network handshaking.
3. **Data Integrity:** When the sender sends a message to the recipient, and in between the communication channel the contents of a message is lost. Then it say that the integrity of the message is lost.
4. **Non-Repudiation:** This refers to the situation when a user sends the data and at a later stage it denies.
5. **Access Control:** It defines as what to access and who has given the right to access the data.
6. **Availability:** It specifies that all resources are available to the legitimate users at all time.

## Cryptographic Techniques

Cryptography provides a secure data communication environment for the user. Where Encryption and decryption play a major role. Encryption algorithm uses a key to transform an original message into an encrypted cipher message. If the key is the same for encryption and decryption then the algorithm will always transform the plaintext into the ciphertext. The message is secure if an attacker cannot determine any properties of plaintext or key. There are different types of key selection techniques such as:

1. **Symmetric-Key Cryptography:** In this, both sender and receiver use a single key for encryption and decryption of the original message.
2. **Public-Key Cryptography:** It is also known as asymmetric key cryptography. Where it uses a pair of keys for encryption and decryption.