International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2018 IJSRCSEIT | Volume 3 | Issue 5 | ISSN : 2456-3307

Network Security with Cryptography

Pragya Sharma*[1], Shashank Dahiya[2]
[1]Department of Computer Technology and Application, SGSITS, Indore, Madhya Pradesh, India
[2]Computer Science Department , IET DAVV, Indore, Madhya Pradesh, India

ABSTRACT

In the present tech-savvy world, the growth in computer systems and their interconnections through networks has increased. With this the dependence of both organizations and the individuals on the information stored and communicated using these systems has also increased. This, in turn, has led to the reinforcement in security attacks and electronic frauds. Hence, there is indeed no time at which security does not matter and to protect systems from network based attacks. Network security refers to all hardware and software functions, characteristics, features, operational procedures, accountability, measures, access control and administrative and management policy required to provide an acceptable level of protection for hardware and software and information in a network. Cryptography is a technique that is used to enhance the network security. It protects users by providing functionality for the encryption of data and authentication of other users. There are many cryptographic techniques available and among them Advanced Encryption Standards (AES) is one of the most powerful techniques. In this paper a study on cryptography and its dimensions is done. Cryptographic systems with ciphers are described. The cryptographic models and algorithms are outlined.

Keywords : Network Security, Cryptography, Cryptosystem.

I. INTRODUCTION

In recent years, a lot of applications based on internet have come up such as online shopping, stock trading, internet banking and electronic bill payment, etc. Such transactions, over wired or wireless public networks demand end to end secure connections. These connections must ensure data confidentiality, availability and integrity, also known as CIA triad. Data Security is a challenging issue of data communications today that touches many areas including secure communication channel, strong data encryption technique and trusted third party to maintain the database. The rapid development in information technology, the secure transmission of confidential data herewith gets a great deal of attention. The conventional methods of encryption can only maintain the data security. The information could be accessed by the unauthorized user for malicious purpose. Therefore, it is necessary to apply effective encryption/decryption methods to enhance data security. Network security covers a variety of computer networks, both public and private, that are used in everyday jobs conducting transactions and communications among businesses, government agencies and individuals. Networks can be private, such as within a company, and others which might be open to public access. Network security is involved in organizations, enterprises, and other types of institutions. It does as its title explains: It secures the network, as well as protecting and overseeing operations being done. It involves the authorization of access to data in a network, which is controlled by the network administrator. The most common and simple way of protecting a network resource is by assigning it a unique name and a corresponding password [1]. Users choose or are assigned an ID and password or other authenticating information that allows them access to information and programs within their authority. Data encryption is known for protecting information from eavesdropping. It transforms current data of a given format, called plaintext, to another format, called cipher text, using an encryption key. Cryptography prior to the modern age was effectively synonymous with encryption, the conversion of information from a readable state to apparent nonsense. Modern cryptography is heavily based on mathematical theory and computer science practice; cryptographic algorithms are designed around computational hardness assumptions, making such algorithms hard to break in practice by any adversary. It is theoretically possible to break such a system, but it is infeasible to do so by any known practical means. This growth of cryptographic technology has raised a number of legal issues in the information age [2]. The security of quantum cryptography maintains in its ability to exchange the encryption key with absolute security. Cryptography has its origin in the ancient world. According to [3], the Julius Caesar used simple cryptography to hide the meaning of his messages. According to, The Caesar cipher is a monoalphabetic cryptosystem, since it replaces each given plain text letter, wherever in the original message it occurs, by the same letter of the cipher text alphabet. However the concepts of source and receiver, and channel codes are modern notions that have their roots in the information theory. Claude Shannon, in the 1948 provided the information theory basis for secrecy, which defines that the amount of uncertainty that can be introduced into an encoded message can't be greater than that of the cryptographic key used to encode it [8]. Claude Shannon presented this concept of security in communications in 1949; it implies that an encryption scheme is perfectly secure if, for any two messages M 1 and M 2, any cipher - text C has the same probability of being the encryption of M 1 as being the encryption of M 2. Shannon was developed two important cryptographic concepts: confusion and diffusion. According to Salomon[7], the term confusion means to any method that makes the statistical relationship between the cipher - text and the key as difficult as possible, and diffusion is a general term for any encryption technique that expands the statistical properties of the plaintext over a range of bits of the cipher-text.

II. METHODS AND MATERIAL

SECURITY REQUIREMENTS FOR TRANSMITTING INFORMATION

X.800 divides these services into following five services: [5]

1. AUTHENTICATION

The authentication service is concerned with assuring that a communication is authentic. It is the process of providing the identity that assures the communicating entity is the one that it claims to be.

- PEER ENTITY AUTHENTICATION

It provides for the corroboration of the identity of a peer entity in an association. Used in association with a logical connection to provide confidence in the identity of the entities connected.

- DATA ORIGIN AUTHENTICATION

It provides for the corroboration of the source of a data unit. It does not provide protection against the duplication or modification of data units. This type of service supports applications like electronic mail where there are no prior interactions between the communicating entities.

2. ACCESS CONTROL

Access control is the ability to limit and control the access to host systems and applications via communications links. To achieve this, each entity trying to gain access must first be identified, or authenticated, so that access rights can be tailored to the individual.

3. DATA CONFIDENTIALITY

Confidentiality is the protection of transmitted data from passive attacks. With respect to the content of a data transmission, several levels of protection can be identified.

- *CONNECTION* CONFIDENTIALITY
  The protection of all user data is on a connection.
- *CONNECTIONLESS* CONFIDENTIALITY
  The protection of all user data is in a single data block.
- *SELECTIVE-FIELD* CONFIDENTIALITY
  The confidentiality of selected fields within the user data is on a connection or in a single data block.
- *TRAFFIC-FLOW* CONFIDENTIALITY
  The protection of the information can be derived from observation of traffic flows.

4. DATA INTEGRITY

The assurance that data received are exactly as sent by an authorized entity (i.e., contain no modification, insertion, deletion, or replay). Integrity can apply to a stream of messages, a single message, or selected fields within a message.

- CONNECTION INTEGRITY *WITH* RECOVERY

Provides for the integrity of all user data on a connection and detects any modification, insertion, deletion, or replay of any data within an entire data sequence, with recovery attempted.

- CONNECTION INTEGRITY *WITHOUT* RECOVERY

As above, but provides only detection without recovery. Selective-Field Connection Integrity Provides for the integrity of selected fields within the user data of a data block transferred over a connection and takes the form of determination of whether the selected fields have been modified, inserted, deleted, or replayed.

- *CONNECTIONLESS* INTEGRITY

Provides for the integrity of a single connectionless data block and may take the form of detection of data modification. Additionally, a limited form of replay detection may be provided.

- *SELECTIVE FIELD* CONNECTIONLESS INTEGRITY

Provides for the integrity of selected fields within a single connectionless data block; takes the form of determination of whether the selected fields have been modified.

5. NONREPUDIATION

Nonrepudiation prevents either sender or receiver from denying a transmitted message. Thus, when a message is sent, the receiver can prove that the alleged sender in fact sent the message. Similarly, when a message is received, the sender can prove that the alleged receiver in fact received the message.

- *NONREPUDIATION, ORIGIN*

Proof that the message was sent by the specified party.

- *NONREPUDIATION, DESTINATION*

Proof that the message was received by the specified party.

III. RESULTS AND DISCUSSION

CRYPTOGRAPHIC DIMENSIONS

Cryptographic systems are characterized along three independent dimensions:

1. **The type of operations used for transforming plaintext to cipher text.**

All encryption algorithms are based on two general principles: substitution, in which each element in the plaintext (bit, letter, group of bits or letters) is mapped into another element, and transposition, in which elements in the plaintext are rearranged. The fundamental requirement is that no information be lost (that is, that all operations are reversible). Most systems, referred to as product systems, involve multiple stages of substitutions and transpositions [5].

2. The number of keys used.

If both sender and receiver use the same key, the system is referred to as symmetric, single-key, secret-key, or conventional encryption. If the sender and receiver use different keys, the system is referred to as asymmetric, two-key, or public-key encryption [5].

3. The way in which the plaintext is processed.

A block cipher processes the input one block of elements at a time, producing an output block for each input block. A stream cipher processes the input elements continuously, producing output one element at a time, as it goes along [5].

CRYPTOSYSTEM TYPES

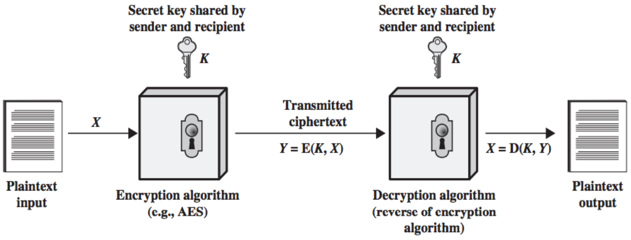
In general cryptosystems can be classified into two encryption types, symmetric or asymmetric, depending on whether the keys at the transmitter and receiver are easily computed from each other.

1. Symmetric Cryptography

Symmetric encryption is a conventional method of Encryption. It is also the simplest technique of encryption. Symmetric encryption is executed by means of only one secret key known as ‘Symmetric Key’ that is possessed by both parties and is unknown to the attacker.. This key is applied to encode and decode the information. The sender uses this key before sending the message and the receiver uses it to decipher the encoded message.

In symmetric cryptosystems (also called conventional, secret-key or one-key cryptosystems), the enciphering and deciphering keys are either identical or simply related, i.e. 684 IEE *PROCEEDINGS, Vol. 131, Pt. F, No. 7, DECEMBER 1984* one of them can be easily derived from the other. Both keys must be kept secret, and if either is compromised further secure communication is impossible. Keys need to be exchanged between users, often over a slow secure channel, for example a private courier, and the number of keys can be very large, if every pair of users requires a different key, even for a moderate number of users, i.e.

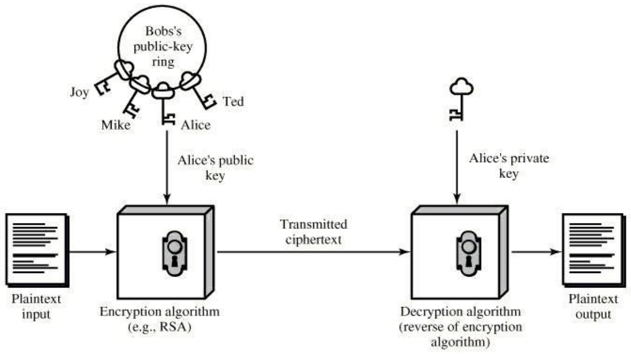
$n(n — 1)/2$ for n users. This creates a key-distribution problem which is partially solved in the asymmetric systems. Examples of symmetric systems are the data encryption standard (DES) [4] and rotor ciphers.


Secret key shared by sender and recipient
K
Secret key shared by sender and recipient
K
X
Transmitted ciphertext
Y = E(K, X)
X = D(K, Y)
Plaintext input
Encryption algorithm (e.g., AES)
Decryption algorithm (reverse of encryption algorithm)
Plaintext output

2. Asymmetric Cryptography

Asymmetric Encryption is a relatively new and complex mode of Encryption. It is complex because it incorporates two cryptographic keys to implement data security. These keys are called a Public Key and a Private Key. The Public key is available to everyone who wishes to send a message. On the other hand, the private key is kept at a secure place by the owner of the public key.

There are practical problems associated with the generation, distribution and protection of a large number of keys. A solution to this key distribution was suggested by Diffie and Hellman in 1976 [6]. A type of cipher was proposed which uses two different keys: one key used for enciphering can be made public, while the other, used for deciphering, is kept secret. The two keys are generated such that it is computationally infeasible to find the secret key from the public key. If user A wants to communicate with user B, A can use B's public key (from a public directory) to encipher the data. Only B can decipher the ciphertext since he alone possesses the secret deciphering key. The scheme described above is called a public-key cryptosystem or an asymmetric cryptosystem [9]. If asymmetric algorithms satisfy certain restrictions, they can also be used for generating so-called digital signatures [10].



IV. CONCLUSION

With such a massive growth and dependency over inter-networking comes enormous data transmission. And this give rise to security of network. Techniques of Cryptography schemes are versatile and highly involved. The paper presented various services of transmission informations and its security which varies by its use over type of data send over. All have discrete advantage over other. Though no scheme has been discovered that can work with complete colours of data. Cryptographic dimensions are explained with all processing of conversions and methods independently used. Result of which are based on type of data or plain text needed to be enciphered. The secure exchange of key between sender and receiver is an important task. Network security covers the use of cryptosystem, depending on flexibility and range of transmission to senders. Its types and functionalities are comprehended. Working with symmetric and asymmetric key are two different ranges to encipher and decipher transmission. It covers brief concepts of network security, underlines security method, cryptography.
In the future it opens work for transmission services and its management as well as finding way to optimize cryptosystem without symmetric bias.

V. REFERENCES

[1]. Simmonds, A; Sandilands, P; van Ekert, L (2004) Ontology for Network Security Attacks". Lecture Notes in Computer Science. Lecture Notes in Computer Science 3285, pp.317-323.

[2]. Swarnalata Bollavarapu and Ruchita Sharma-? Data Security using Compression and Cryptography Techniques

[3]. Pfleeger, C. P., & Pfleeger, S. L., Security in Computing, Upper Saddle River, NJ: Prentice Hall.2003.

[4]. 'Data encryption standard', FIPS PUB 46, National Bureau of Standards,Washington, DC Jan. 1977

[5]. William Stallings, Cryptography and Network Security Principles and Practices, Fourth Edition

[6]. DIFFIE, W., and HELLMAN, M.: 'New directions in cryptography', IEEE Trans., 1976, IT-22, pp. 644-654

[7]. Salomon, D., “Coding for Data and Computer Communications”, New York, NY: Spring Science and Business Media. 2005.

[8]. Shannon, E. C., Communication theory of secrecy system, Bell System Technical Journal, Vol.28, No.4, 1949, pp.656- 715.

[9]. SIMMONS, G.J.: 'Symmetric and asymmetric encryption', ACM Comput. Surveys, 1979, 11, pp. 305-330

[10]. RIVEST, R.L., SHAMIR, A., and ADLEMAN, L: 'A method for obtaining digital signatures and public-key cryptosystems', CACM, 1978, 21, pp. 120-126

[11]. https://www.rapidsslonline.com