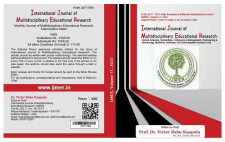

Cover Page

DOI: http://ijmer.in.doi./2022/11.03.132

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY EDUCATIONAL RESEARCH
ISSN:2277-7881; IMPACT FACTOR :7.816(2022); IC VALUE:5.16; ISI VALUE:2.286
Peer Reviewed and Refereed Journal: VOLUME:11, ISSUE:3(7), March: 2022
Online Copy of Article Publication Available (2022 Issues): www.ijmer.in
Digital Certificate of Publication: http://ijmer.in/pdf/e-Certificate%20of%20Publication-IJMER.pdf
Scopus Review ID: A2B96D3ACF3FEA2A
Article Received: 2nd March 2022
Publication Date:10th April 2022
Publisher: Sucharitha Publication, India

THE ROLE OF CRYPTOGRAPHY TOWARDS NETWORK SECURITY

Moumita Biswas
Assistant Professor
Department of Computer Science, Charuchandra College
Kolkata, West Bengal, India

Abstract: Since last several decades of civilization with the advent of internet our society is moving towards digital information age. While this information or data is transmitted over several networks it requires some kind of security such as confidentiality, integrity, authenticity etc. Cryptography and network security is the vast area which deals with various techniques and methods in order to accomplish this level of security and the techniques are in an evolutionary stage. Cryptography can be defined as techniques that encrypts the original data into unreadable format and the data can only be transformed back to its original form after decryption by an authorized person. The main purpose of cryptography is to achieve the essential security goals of network security. Network security is gaining importance day by day with the digital application of e-commerce, banking transactions, military services etc. This paper discusses the concept of cryptography, types of cryptography and its algorithms and provides an overview on network security. Cryptography in digital signatures is also presented. Digital signature demonstrates the integrity and authenticity of a digital document and the signer's identity.

Keywords: Cryptography, Network Security, Encryption, Decryption, Digital Signature.

1. INTRODUCTION

In recent times with the progress of civilization our entire globe is highly dependent on internet and its application such as communication, transmission of data, files, videos etc. During transmission of these data over internet, we need safeguard method to prevent duplication of data and redistribution of these data by intruders or unauthorized persons. We need to secure our data while it flows over the networks. Financial service is an early use case of computer communication, so it is necessary to find a way to retain the secrecy of information. Security is the method by which information is kept safe from unintended or unauthorized access, alteration or destruction.

Network security can be accomplished by Cryptography, the science and art of message transformation to make them safe and resistant to attack. Cryptography deals with writing in secret code. This method is used to ensure that the contents of a message are very confidentiality transmitted and would not be altered [3]. The idea of encryption and encryption algorithm by which we can encode our data in secret code and make it unintelligible to the hackers or unauthorized person even it is hacked. The authorized user should provide user ID and password or any other unique data to access secured data.

Historical roots of cryptography can be observed back to 2000 B.C., when the ancient Egyptians used "secret" hieroglyphics [6]. Other historical evidence of cryptography includes secret writings in ancient Greece or the famous Caesar cipher [9] of ancient Rome.

Some of the Cryptographic applications are computer passwords, financial transactions, e-commerce, business applications, etc. Cryptography is universally used by billions of people on a regular basis to protect data and information, even though most of them are unaware that they are using it.

Many cryptosystems have been introduced for promoting the information security. Everyday new method for encryption/decryption techniques is discovered. Modern cryptography is heavily based on mathematical theory and computer science implementation. This paper defines some of the terms and concepts behind basic cryptographic methods and different types of cryptographic techniques which is suitable for many applications where security is main concern.

2. LITERATURE REVIEW

Dr. Sandeep Tayal [7] has demonstrated the importance of key management in the cloud. Both encryption and key administration are essential to help secure applications and communicate them through the wireless medium. The key itself should be stored in a shielded manner beyond the reach of harmful clients to avoid misuse of data. There are two types of techniques that are commonly used to encrypt or decrypt the confidential data namely asymmetric and symmetric encryption technique. In symmetric cryptographic technique a common secret key is used by both the sender and the receiver. But in asymmetric cryptographic technique a pair of keys are used that is a public key and a private key which are used for encryption and decryption respectively.

Priyank Sanghavi [10] has showcased the current developments in network security. Biometrics have added a great dimension to network security. It imparts a better method of authentication than passwords. This might considerably turn down the unauthorized access of secure systems. The software exposure of network security is very vast. Continuously new firewalls, antivirus and encryption schemes are being implemented.

Prof. Mukund R. Joshi [13] pointed two major principles used in cryptography - Redundancy and Freshness. The first principle is that all encoded messages must contain some redundancy. Here redundancy means the information that is not required for understanding the message reducing the chances for a passive intruder to make attacks. In case of passive attacks, the intruder stoles some information and makes some abuse without recognizing it. If some redundancy is included, then the redundancy prevents the active intruders from sending garbage values and then getting it verified as some valid message. With the absence of redundancy, the attackers would simply send junk messages and the recipient will decode it as a valid message. The second cryptographic principle is that measures must be taken to guarantee that every message received can be checked as being fresh, that is, sent very recently. This measure prevents passive intruders from playing back old messages. The timestamp is used for freshness and time is set for every received message. The message is accepted only within the time limit, messages beyond the time limit is thrown out.

Shyam Nandan Kumar [14] discussed the types of network security attacks in his paper. An active attack is to gain unauthorized access to modify data, either deleting, encrypting or otherwise harming it. Masquerade, Modification of Message, Denial of Service, Replay and Repudiation are the types of active attacks. Masquerade attack occurs when one entity pretends to be a different entity. Modification of Message makes some alterations in the message format or reorder the message to produce an unauthorized effect. Passive attack includes observation or monitoring of communication from the system but does not affect system resources. The eavesdropper tries to obtain information that is being transmitted. Types of passive attacks include Traffic Analysis and Release of Message Contents. In traffic analysis the location and identity of communicating host could be determined by the opponent. The sender and the receiver are unaware that a third party has detected the traffic pattern of the messages.

3. CONCEPT OF CRYPTOGRAPHY

Crytography: The origin of the word cryptography came from a Greek word called “Kryptos” which means “Hidden Secrets” [7]. It is the Art or Science of converting the secret data or information into an unreadable or scrambled form and again retransforming that message into its original form. It is a method of storing and dispatching data in a particular form so that only the intended receiver can read and process it. Cryptography not only protects data from theft or modification, but can also be used for user verification.

Plain text: It is the original message that we want to send secretly. Plain text is written in a form that is intelligible to everyone. Some security measure must be taken before sending the message to the intended recipients over the internet.
Cipher text: This is the scrambled or unreadable form of information or message that would seem like a gibberish to an unintended eavesdropper.
Encryption: Encryption is the process of converting plaintext into ciphertext which looks like a meaningless and random sequence of bits.
Decryption: The process of turning ciphertext back into plaintext is called decryption.
Key: The Key is an input to the encryption algorithm, and this value must be independent of the plaintext [4]. This secret material is used to transform the plaintext into cipher text and different keys will yield different cipher text.
Cryptanalysis: Cryptanalysis is the study of how to inverse cryptography. It is concerned with deciphering messages without knowledge of the cryptosystem [2].
Cryptology: The study of both cryptanalysis and cryptography is known as cryptology.
Cryptosystem: A system which converts plain text to cipher text or cipher text to plain text by the application of encryption or decryption algorithm [8]. The key generation for encryption and decryption algorithms is also part of a cryptosystem.
Cipher: An algorithm used in a cryptosystem.

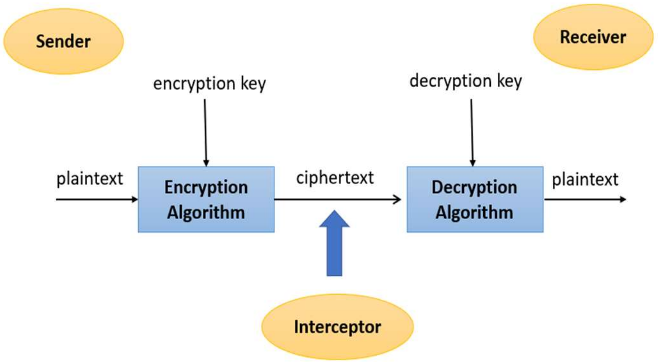


Fig 1: Cryptosystem

4. NETWORK SECURITY

Network security attempts to take physical and software precautionary measures to protect the underlying networking framework from unauthorized access, misuse, malfunction, alteration, destruction, or illegitimate disclosure, thus creating a reliable platform for computers, users, and programs to conduct their permitted critical tasks within a secure domain [12]. Computer networks that are engaged in frequent transactions and communication within the government, individuals, or business requires security. Most security problems are intentionally caused by malicious people [10] trying to gain some benefit, get attention, or to harm someone. A possible hacker could attack the communication channel, obtain the encrypted data, and decrypt it and send back a false message. Hence securing the middle network is just as important as securing the computers and encrypting the message. The main goals of cryptography are to overcome the main challenges associated with network security [1]. Network security problems can be divided roughly these following closely intertwined areas:

- **Authentication:** This is the process of providing one’s identity. This property ensures that the origin of the message is correctly identified.
- **Confidentiality:** It ensures that no one other than the intended receiver can read the message. With this property, information is unavailable to unauthorized individuals, entities, or processes.
- **Integrity:** The integrity mechanism ensures that the contents of the message is not altered any way from the original, as send by the sender when it reaches the intended recipient.
- **Non-repudiation**: non-repudiation means the sender cannot deny sending the message sent at a later time. This mechanism proves that the sender really sent this message.
- **Access Control:** Authorized users are provided the means to communicate to and from a particular network

5. TYPES OF CRYPTOGRAPHY

Symmetric Key Cryptography

Symmetric key cryptography is a type of cryptography in which the single common key is used by both sender and receiver to encrypt and decrypt messages. This system is also known as private or secret key cryptography. AES (Advanced Encryption System) is a commonly used symmetric key cryptographic method. The symmetric key system has one major drawback that the two parties must somehow exchange the key in a secret [5] manner as there is only one single key for encryption as well as decryption process.

Examples: AES (Advanced Encryption Standard), DES, Triple DES, RC2, RC4, RC5, IDEA, Blowfish, Stream cipher, Block cipher etc. are some widely used symmetric key cryptography techniques.

DOI: http://ijmer.in.doi./2022/11.03.132

Article Received: 2nd March 2022
Publication Date:10th April 2022
Publisher: Sucharitha Publication, India

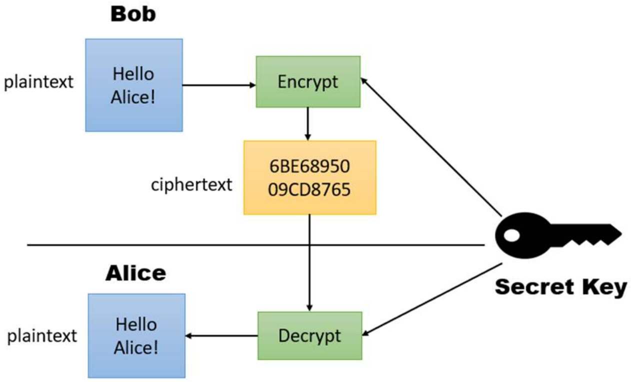


Fig 2: Symmetric Key Cryptography

Asymmetric Key Cryptography

This is also termed as Public-key cryptography. It uses a different kind of protective method for the transmission of information. In this system, every user uses two keys [11] or a pair of keys (private key and public key) for encryption and decryption process. The private key is kept as a secret with every user and public key is distributed over the network so if anyone wants to send messages to any user can use those public keys. Even if the public key is known by everyone the intended receiver can only decode it because he alone knows the private key. It is more secure than symmetric key. RSA is the most commonly used asymmetric key cryptography.

Examples: RSA, DSA, PKCs, Elliptic Curve techniques, etc. are the common types of asymmetric key cryptography.

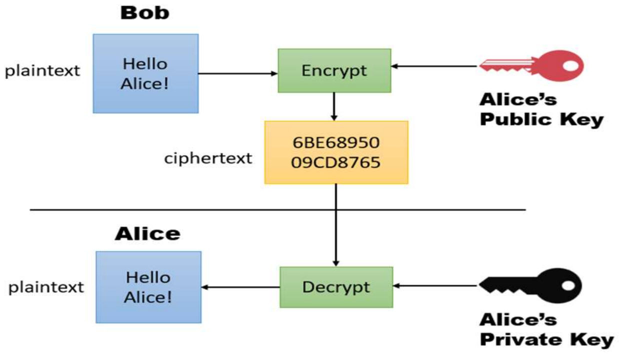


Fig 3: Asymmetric Key Cryptography

6. DIGITAL SIGNATURE

The authenticity and integrity of a message, software or digital document can be ensured with the help of a mathematical technique called digital signature. A valid digital gives the recipient reason to believe that the message was generated by a well-known sender, such that the sender cannot refuse having sent the message (authentication and non-repudiation) and that the message was not changed during transmission (integrity). Digital signatures are frequently used for software distribution, financial services, and in other cases where it is necessary to detect falsification or tampering.

Digital signatures are often used to perform a digital analog to handwritten signatures. More broadly, this refers to any electronic data that bears the intent of a signature. Digital signatures employ a type of asymmetric cryptography [9]. For messages sent through an insecure medium, a properly implemented digital signature ensures the recipient that the message was sent by the legitimate sender. Digital signatures are similar to traditional handwritten signatures in many ways, but it is harder to forge well implemented digital signatures than the handwritten type. The process of digital signature used here, are cryptographic based, and must be implemented properly to be effective. Digital signatures can also provide non-repudiation, means the signer cannot deny of signing a message, while also asserting their private key remains secret.

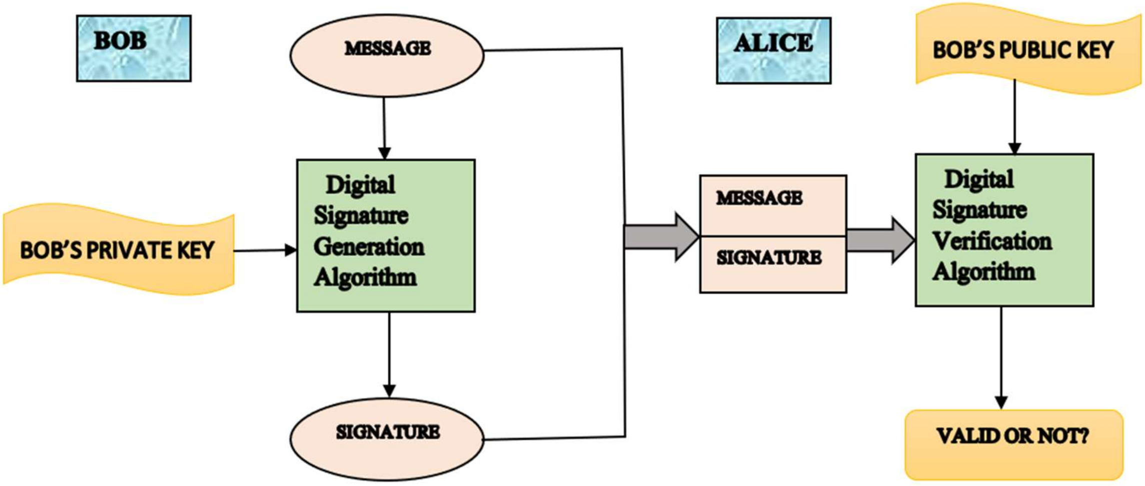


Fig 4: Digital Signature Cryptography

A digital signature process consists of three algorithms

- A key generation algorithm that produces a private and public key.
- A digital signature generation algorithm that generates a signature when the private key and the message is provided.
- A digital signature verification algorithm that, given a message, public key and a signature, either validate or rejects the message's claim to be authentic.

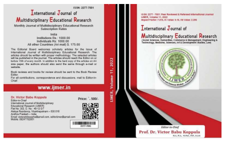
Two main properties are needed to be preserved. At first, using the corresponding public key, the legitimacy of a signature produced from a specific message and specific private key can be verified. Secondly, it should be impossible for an attacker to generate an authentic signature of a legitimate sender with having no idea about that sender's private key. Digital signature technology requires all the parties to trust that every legitimate sender is able to create and keep their own private key in a secret manner. If an unauthorized person gets the access of a private key of a legitimate party, that person could create fraudulent digital signatures in the name of the private key holder.

7. CONCLUSION

In this era of internet communication, network security is gaining attention increasingly. Information is transmitted in a digital form over different networks using different services. Security of these information against unauthorized access is on high demand. Cryptography has the important motive of providing reliable, powerful, and robust network and data security. Cryptography plays a crucial and vital role in fulfilling the primary aims of security goals, like authentication, confidentiality, integrity and no-repudiation. Cryptographic algorithms are developed in order to accomplish these goals. Cryptography will continue to emerge with IT and business plans in regard to protecting personal, financial, medical, and e-commerce data and providing a respectable level of privacy. This paper has described briefly about how cryptography works and discussed various types of cryptography mechanisms used for different network security purposes. Cryptanalysts are continuously trying to find loopholes in all these security algorithms, so researchers are continuously trying to evolve more secure algorithms that can perform well in all the scenarios. Hence, we can conclude that Network Security and Cryptography are on the leading edge of research today.

REFERENCES

1. Behrouz A. Forouzan, "Cryptography and Network Security", Tata McGraw-Hill Company Limited, Special Indian Edition 2007
2. Shashi Gautam, Shubha Mishra, Dr. Manish Shrivastava, "A Survey on Generation and Evolution of Various Cryptographic Techniques", International Research Journal of Engineering and Technology (IRJET), Volume: 04 Issue: 01 | Jan -2017
3. A. Joseph Amalraj, Dr. J. John Raybin Jose, "A Survey Paper on Cryptography Techniques", IJCSMC, Vol. 5, Issue. 8, August 2016, pg.55 – 59



4. Harpreet Kaur, Vaishali Verma, Jaya Mishra, "Survey Paper on Cryptography", Volume No 06, Special issue No. (02), September 2017, ICITTESE
5. Atul Kahate "Cryptography and Network Security", Tata McGraw-Hill Companies, Second Edition
6. Dr. R.K Gupta, "A Review Paper on Concepts of Cryptography and Cryptographic Hash Function", European Journal of Molecular & Clinical Medicine ISSN 2515-8260 Volume 07, Issue 07, 2020
7. Dr. Sandeep Tayal, Dr. Nipin Gupta, Dr. Pankaj Gupta, Deepak Goyal, Monika Goyal, "A Review paper on Network Security and Cryptography", Advances in Computational Sciences and Technology, ISSN 0973-6107 Volume 10, Number 5 (2017) pp. 763-770
8. Sujatha K, D.Ramya Devi Kala Rathinam D., "A Review Paper on Cryptography And Network Security", International Journal of Pure and Applied Mathematics -Volume 119 No. 17 2018, 1279-1284
9. Abdalbasit Mohammed Qadir, Nurhayat Varol, "A Review Paper on Cryptography", DOI: 10.1109/ISDFS.2019.8757514
10. Priyank Sanghavi, Kreena Mehta, Shikha Soni, "Network Security", International Journal of Scientific and Research Publications, Volume 3, Issue 8, August 2013, ISSN 2250-3153
11. Rajani Devi.T, "Importance of Cryptography in Network Security", 2013 International Conference on Communication Systems and Network Technologies
12. Sarita Kumari, "A research Paper on Cryptography Encryption and Compression
13. Techniques", International Journal Of Engineering And Computer Science ISSN:2319-7242, Volume 6 Issue 4 April 2017, Page No. 20915-20919
14. Prof. Mukund R. Joshi, Renuka Avinash Karkade, "Network Security with Cryptography", IJCSMC, Vol. 4, Issue. 1, January 2015, pg.201 – 204, ISSN 2320–088X
15. Shyam Nandan Kumar, "Review on Network Security and Cryptography", International Transaction of Electrical and Computer Engineers System, 2015, Vol. 3, No. 1, 1-11