iJRASET
International Journal For Research in Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 9 **Issue:** VIII **Month of publication:** August 2021

DOI: https://doi.org/10.22214/ijraset.2021.37431

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 9 Issue VIII Aug 2021- Available at www.ijraset.com

Cryptography – An Overview

Mahasweta Das[1], Debrupa Pal[2]
[1]*Student MCA 3rd year Computer Applications Department, Narula Institute of Technology, Kolkata, India*
[2] *Assistant Professor Computer Applications Department, Narula Institute of Technology, Kolkata, India*

Abstract: With the day-by-day advancement of the Internet throughout the world, online marketing sites and applications are growing rapidly. More and more social networking sites are emerging almost every day connecting people from various parts of the world. These situations demand the organizers behind those networks to generate and store a huge amount of data regularly. Nonetheless to say, the more the data, the more is the risk of losing it. Hackers, phishers, or breachers are there at every nook and corner of the World Wide Web to steal and abuse the data of users. To protect the data from breaches, it is a necessity to secure the network. The general method of network protection is known as "Cryptography". Users are generally given a unique User ID and authentication code known as Password under which their data are stored individually. In this paper, we will discuss the overall idea of cryptography along with its methods and techniques.
Keywords: Internet, Network, Data, Security, Cryptography

I. INTRODUCTION

The rapid growth of Internet technology has attracted individuals and organizations to itself. Today it is possible to find everything and everyone on the World Wide Web. Persons, banks, offices, groceries, hospitals, even local security like the police station have their social media sites where people can connect with them. The current situation of the global pandemic has increased social media access more than it was before.

Schools, Colleges are compelled to conduct classes and official works through online mode. Similarly, most of the offices are getting their employees' work from home. So not only office workers, but teachers, as well as students, are getting involved in the Internet every second. And this situation lures unethical entities. They try to access any individual's data and exploit it. These malicious adversaries are known as 'Hackers', or 'Phishers', or 'Breachers'. They may steal our data and ask for a ransom to return it. Sometimes, they can sell highly confidential information like national security to other countries. Here comes the concept of securing the network. The vast spread of computerized data storage, processing, and transmission generates sensitive data. These data are prone to unauthorized access during transmission and even when they are in storage too. Cryptography aims to protect them by following some methods and algorithms.

Modern-Day-Cryptography is a mathematical and scientific approach to conceal any readable information into some cryptic form consisting of alphanumeric characters and symbols. But in ancient times, cryptography was more of an art than science. Julius Caesar used to encrypt his messages. The method followed there was simple as it replaced each letter of the alphabet with a specific letter of the cipher or encoding text. It is named "Caesar Cipher" [1]. However, day-by-day the concept of cryptography is becoming more popular and it increases the risk of advanced methods from the attackers' side. Quantum Cryptography [2] is used to prevent those cases. It is the first commercial application of the principles of quantum information methods, based on quantum physics. In 1949, Claude Shannon proposed the idea of Confusion and Diffusion in cryptography [3]. He referred to confusion as a method to make the relationship between the plain and cipher text as involving as possible. Whereas diffusion, defined by him, dissolves the structural plain text over the block of ciphertext.

Nonetheless, to say, the confusion is used by both block and stream ciphers and diffusion is only suitable for and used by stream ciphers. The relationship between the ciphertext and the key is hidden in confusion whereas diffusion hides the same between ciphertext and plaintext.

The idea of cryptography is scrambling an understandable set of information into some undecipherable string of characters. That particular string is sent from one end, through the medium or channel, and then is received on the other end. Now in the recipient's end, after the message delivery, the string is decoded to its original form and then only the communication is said to be successful. Generally, in cryptography, users are given their unique user id and password to get individual authentication on any site. They may update their passcode from time to time, but their user ID remains the same. No two users, under any circumstances, can use or get the same user id to log into their private windows.

©IJRASET: All Rights are Reserved

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 9 Issue VIII Aug 2021- Available at www.ijraset.com

II. PRINCIPLES OF CRYPTOGRAPHY

The aim to protect a cloud or network is to provide secure communication between two entities. It means that data transferred between two parties should never be accessed and exploited by any third party. To make sure it never happens, cryptography has some core principles to follow.

A. Confidentiality

It means that data or message transferred between two parties is restricted to them only.

B. Integrity

It assures that the data exchanged remains intact and accessible by authenticated parties throughout its entire life cycle.

C. Authentication

If a user claims a certain piece of data, it is cross-checked whether that particular data belongs to the user or not.

D. Non-repudiation

If an individual is associated with a certain communication or contract, he/she can never deny their authenticity over that data.

III. MECHANISM OF CRYPTOGRAPHY

Cryptography is simply a strategy that ensures that the data is sent from and received by only the intended users. It transmits data in a certain manner where a piece of normal information is scrambled into some unintelligible pattern, then gets transmitted, and then again gets back to its original form after being received by the expected user. The general terms associated with cryptography [4] are:

A. Key

A key refers to a string of integers or characters or a mixture of both which alters data to make it appear random.

B. Plaintext

Plaintext refers to any readable data, be it binary or any other language we use on daily basis. Users can easily read & understand these without needing any special technique. For instance, if user A wants to send “Good Morning” to user B, then “Good Morning” is said to be the Plaintext.

C. Ciphertext

Ciphertext refers to the randomly arranged unintelligible string of numeric, characters, and symbols which is encoded and decoded only through keys. And thus, only the intended users can use the data and not any third-party user or outsider. Let’s assume “Good Morning” is encoded as “2#@9_kl8*^5%”. Then the latter one is said to be the ciphertext.

D. Encryption

Encryption is the method of converting plaintext or readable data into an incomprehensible string of literals known as ciphertext. Data is encrypted at the sender’s side. It needs an encryption calculation and an encryption key to change the form of the data.

E. Decryption

Decryption is the method of changing the data to its original readable form from its cryptic form. It is the reverse method of encryption. A decryption key along with an unscrambling algorithm is needed to decipher the ciphertext into a plaintext. Data Decryption occurs at the receiver’s end.

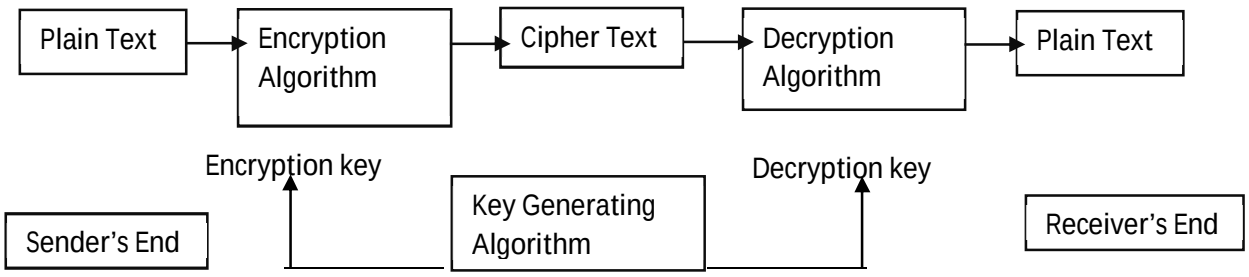


Fig 1. Cryptography Mechanism

©IJRASET: All Rights are Reserved

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 9 Issue VIII Aug 2021- Available at www.ijraset.com

IV. VARIOUS CRYPTOGRAPHY TECHNIQUES

There are commonly three types of Cryptography techniques, Symmetric, Asymmetric, and Hash Functions. [5]

A. Symmetric Cryptography

In Symmetric Encryption, same key is used to cipher and decipher the text. It means that the key used with the encryption algorithm to generate the ciphertext at the sender's end is re-used with the unscrambling or decryption algorithm at the receiver's end to get back the text in its normal form. That said, the key must be exchanged between the data users to have a seamless communication.

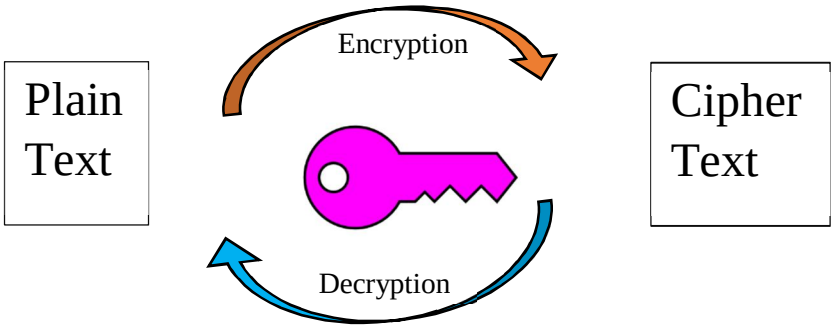


Fig 2. Symmetric Cryptography

There are two types of algorithms used in Symmetric key encryption. They are:

1) *Block Algorithm:* Data is encrypted in blocks of electronic data. The system holds the data in memory until it gets the complete block of data before encryption.
2) *Stream Algorithm:* Data is encrypted byte per byte. That means, system ciphers each byte of message separately.

B. Asymmetric Cryptography

Unlike Symmetric Encryption, Asymmetric Encryption does not use the same key in both sender's and receiver's end. The two keys used in this type of encryption are very different. They are known as public-key and private-key. The public key may be known to anyone and is used to encrypt the message. The private key, on the other hand, is known to the intended recipient only and is used to decrypt the message. This type of encryption is used in one-way communication.

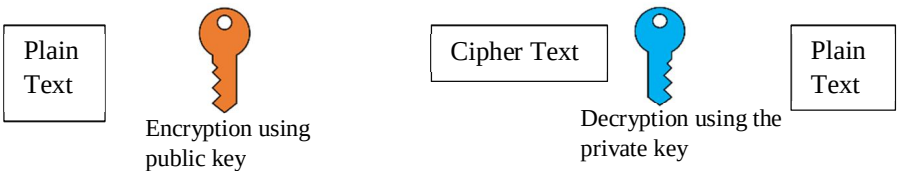


Fig 3. Asymmetric Cryptography

C. Hash Function

Hash Function is a basic concept of modern-day cryptography. It is a mathematical algorithm which maps any message to a fixed size bit-array known as the hash value. The process is infeasible to revert i.e., it is practically impossible to go back and decipher a message from a certain hash value. Any small change in a message can bring drastic changes to the hash value, making it completely different than the previous one. No two messages can map to the same hash value. Similarly, the same message will always map to one hash value. However, the method of finding the hash value of a message is quite fast.

©IJRASET: All Rights are Reserved

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 9 Issue VIII Aug 2021- Available at www.ijraset.com

V. DIFFERENT ALGORITHMS

There are various kinds of cryptographic algorithms available [6]. Among them, some of the most popular algorithms are:

1) *DES*: Short for Data Encryption Standard, this algorithm uses a 56-bit key to operate on a 64-bit block of data. It is a 'private key' system.
2) *Triple DES*: This was designed to replace the DES algorithm, which was eventually breached by malicious entities. Triple DES uses 3 individual 56-bit keys, summing up to 168-bits. Though experts assure that 112-bit key strength is more accurate.
3) *AES*: Advanced Encryption System or AES replaced Triple-DES in no time. It is highly efficient in 128-bit form. Although for heavy encryption purpose, it uses 192 and 256-bit forms.
4) *Blowfish*: One of the most flexible encryption methods is Blowfish. It, too, was designed to replace DES. It uses a block algorithm to encrypt messages into 64-bit blocks. This algorithm is available in public domain for free of cost. It is popular for its speed and overall effect.
5) *Twofish*: It is the successor of Blowfish. This algorithm uses keys having lengths up to 256-bits. This is one of the fastest symmetric algorithms and is ideal for use in any environment. It is also accessible for free.
6) *RSA Security*: Unlike the previous ones discussed, RSA does not use a single key for both the sender and receiver. It uses a pair of keys to encrypt and decrypt the message separately. The encrypted text generated by this algorithm is extensively large and it takes attackers a lot more time and effort to decipher the original data. This asymmetric algorithm is also used in PGP and GPG programs.

VI. COMPARISON OF VARIOUS ENCRYPTION ALGORITHMS

The following table compares [7][8] the popular encryption algorithms discussed before:

TABLE I

Parameters	DES	Triple DES	AES	Blowfish	RSA
Structure	Secret Key Encryption	Secret Key Encryption	Secret Key Encryption	Secret Key Encryption	Public Key Encryption
Key Size	64 bits	112 or 168 bits	128, 192, or 256 bits	64 bits	1024 to 4096 bits
Block Size	64 bits	64 bits	128 bits	64 bits	128 bits
Attacks	Brute force attack	Differential and Related-key attacks	Side-channel attacks	No attack	Plain text attack, Chosen Cipher attack, and Factorization attack
Level of Security	Adequate Security	Adequate Security	Excellent Security	Highly Secure	Excellent Security
Encryption Speed	Very Slow	Very Slow	Fast	Very Fast	Slower

©IJRASET: All Rights are Reserved

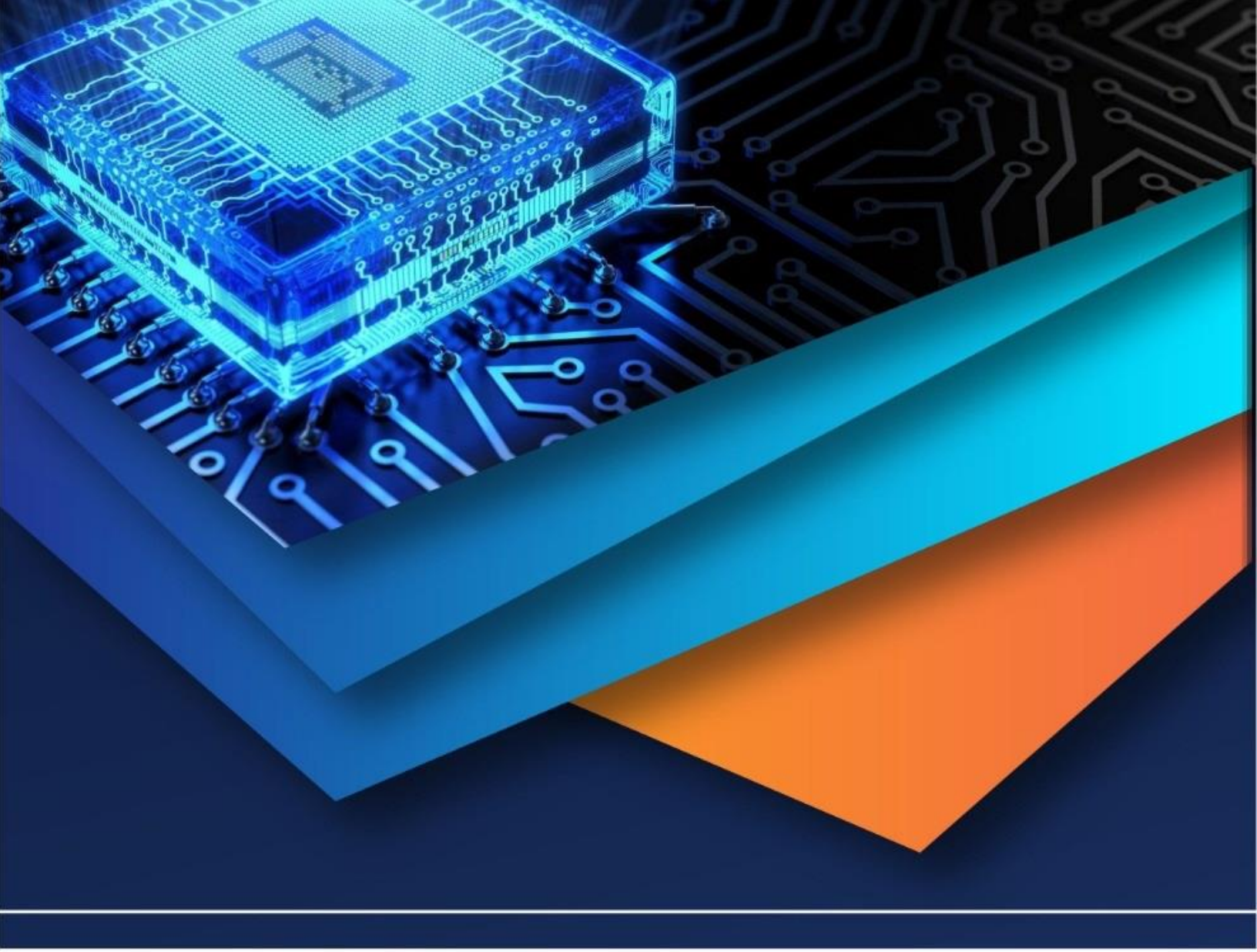
VII. CONCLUSION

Cryptography is a vital concept as it protects the data from breaching over the networks. The base is a singular or double key(s) which encodes and decodes the data. Only the authenticated users are supposed to have access to the key. However, to prevent the possibility of getting the key misplaced to any adversary, it should be exchanged carefully and securely. Network security depends on: what are the amenities done in the network, how the network administrator protects the network and its accessible resources from unauthorized access, and whether the network is under continuous observation or not. The cost for communication can be reduced if the data is compressed while transmitting. [9] There are generally two types of data compression over a network: Lossy and Lossless. [10] Lossy methods like Block Truncation and Transform coding are used to compress an Image while Lossless methods are used to compress text messages. Lossless methods of compression used over the network are, Run Length Coding, Huffman Coding, LZW, and Arithmetic Coding.

REFERENCES

[1] Programmer Enas Ismael Imran, Programmer Farah abdulameerabdulkareem, "Enhancement Caesar Cipher for Better Security", IOSR Journal of Computer Engineering (IOSR-JCE), e-ISSN: 2278-0661, p- ISSN: 2278-8727 Volume 16, Issue 3, Ver. V (May-Jun. 2014), PP 01-05
[2] "Quantum Information Processing with Diamond - Principles and Applications", Edited by Steven Prawer and Igor Aharonovich, 2014, ISBN 978-0-85709-656-2, chapter 2 (Principles of quantum cryptography/quantum key distribution (QKD) using attenuated light pulses by H. Weinfurter)
[3] Shannon, E. C., "Communication theory of secrecy system", Bell System Technical Journal, Vol.28, No.4, 1949, pp.656-715
[4] 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, © Research India Publications
[5] Prof. Mukund R. Joshi, Renuka Avinash Karkade, "Network Security with Cryptography", International Journal of Computer Science and Mobile Computing, Vol.4 Issue.1, January- 2015, pg. 201-204
[6] Algorithms: https://blog.storagecraft.com/5-common-encryption-algorithms/
[7] "Embedded System design with implementation of a cryptographic algorithm for the development of Nadjibi's Pay as You Go platform", Audrey Jean-Martial KAKPOHOUE (audrey.j.m.kakpohoue@aims-senegal.org), African Institute for Mathematical Sciences (AIMS), Senegal, supervised by: Mr Julien POTRON and Dr Amadou Lamine TOURE, Nadjibi, AIMS, Senegal, March 7, 2018, Submitted in Partial Fulfillment of a Masters at AIMS
[8] Omar G. Abood, Shawkat K. Guirguis,"A Survey on Cryptography Algorithms", International Journal of Scientific and Research Publications, Volume 8, Issue 7, July 2018 495, ISSN 2250-3153, DOI: 10.29322/IJSRP.8.7.2018.p7978
[9] 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, ISSN: 1314-3395, Special Issue
[10] Ruchita Sharma, Swarnalata Bollavarapu, "Data Security using Compression and Cryptography Techniques", International Journal of Computer Applications (0975 – 8887), Volume 117 – No.14, May 2015

©IJRASET: All Rights are Reserved



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)