iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 10 **Issue:** XI **Month of publication:** November 2022

DOI: https://doi.org/10.22214/ijraset.2022.47761

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: 7.538
Volume 10 Issue XI Nov 2022- Available at www.ijraset.com

Cryptography: A Smart Technique to Secure Data (Review Paper)

Amarja Deshmukh[1]
BIT College of engineering Barshi, Solapur University

Abstract: ***In order to secure our data, Cryptography can guarantee the confidentiality and integrity of both data at rest and data in transit in order to secure our data. Additionally, it can prevent repudiation and authenticate senders and recipients to one another. Several endpoints, often multiple clients, and one or more back-end servers are common features of software systems.***
Keywords: Encryption, Decryption, cyphertext, plaintext

I. INTRODUCTION

The study and application of methods for secure communication in the presence of outside parties known as cryptography.
It focuses on creating and analysing procedures that stop nefarious third parties from obtaining information communicated between two entities, hence adhering to the many information security components.
Secure communication describes a situation in which a third party cannot access a message or piece of data shared between two parties. An adversary is a malevolent entity that attempts to retrieve valuable information or data with the intention of weakening the information security principles. Authentication, non-repudiation, data confidentiality, and data integrity are the four main tenets of contemporary cryptography.

II. BACKGROUND OF STUDY

It's a way to protect information and communication through use of some codes so that the only person can decipher it with whom you want to share .The word has formed with prefix "Crypt" which means "hidden" and it's suffix is "Graphy" which means "Writing". In Cryptography there are various methods to make code harder to decode and some of those methods are mathematical equation and algorithm. And it's useful in web communication, web Browsing and to secure some confidential transaction.

III.LITERATURE REVIEW

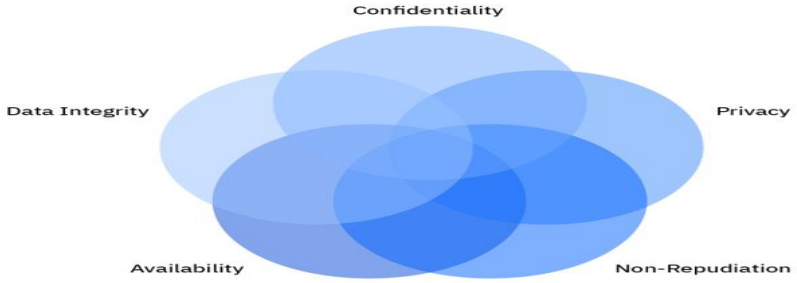
What is cryptography, where in concept of cryptography are been used, how cryptography works and which all algorithm are used in securing the private messages

IV.IMPLEMENTATION

A. Techniques for Cryptography

In the age of computers, cryptography is frequently connected with the transformation of plain text into cypher text, which is text that can only be decoded by the intended recipient. This process is known as encryption. Decryption is the process of converting encrypted text into plain text.

B. The Following list of Cryptographic Features



C. Confidentiality

Information can only be accessed by the intended recipient and no one else. This is known as confidentiality.

D. Integrity

Information cannot be changed while being stored or sent between a sender and the intended recipient without the addition of new information being noticed.

E. Non-repudiation

The information creator/sender is unable to later retract his desire to send information.

F. Authentication

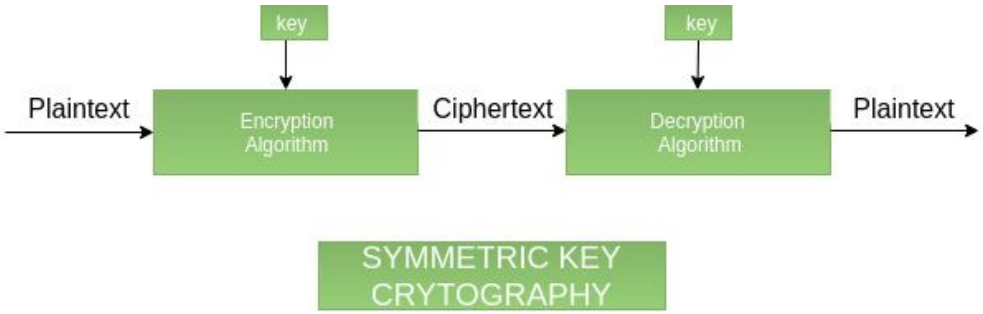
The sender's and receiver's identities are verified. Additionally, the information's origin and destination are verified.

V. TYPES OF CRYPTOGRAPHY

In general there are three types Of cryptography

A. Symmetric Key Cryptography

It is a method of encryption where both the message's sender and recipient utilise the same key to encrypt and decrypt communications. Symmetric Key Systems are quicker and easier, but the issue is that the sender and receiver must securely exchange keys. Synchronized Key Today's Internet uses cryptography extensively, which mostly consists of two types of algorithms called Block and Stream. The Advanced Encryption Standard (AES) and the Data Encryption Standard (DES) are two popular encryption methods (DES). Although this type of encryption is typically faster than asymmetric encryption, it necessitates the possession of a secret key by both the sender and the recipient of the material. The FIDO authentication system is built on asymmetric cryptography, which does not rely on the exchange of a secret key.



B. Hash Functions

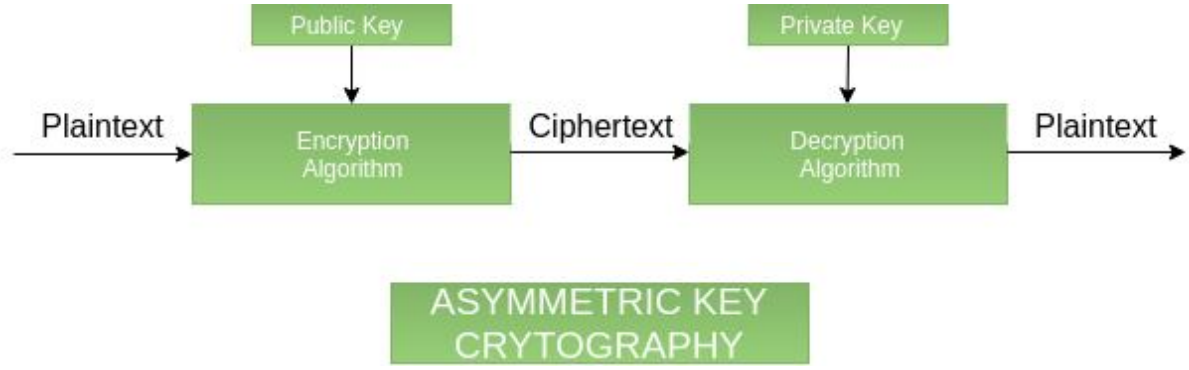
This algorithm uses no keys at all. It is impossible to reconstruct the contents of plain text since a fixed-length hash value is computed based on the plain text. Hash functions are widely used in operating systems to secure passwords.

There are modifications that can strengthen your hash function and give you more protection against attacks.

1) *Hashes With Salt:* Each plaintext credential is salted by adding random data. The end result is that two identical plaintext passwords are now distinguished in enciphered text form, making it impossible to identify duplicates.
2) *Keyed hashing Procedures:* A cryptographic key AND a cryptographic hash function are used by a keyed hash function, sometimes referred to as an HMAC, to create a message authentication code that is both keyed and hashed.
3) *Adaptive Hashing Algorithms:* Any function that is intended to iterate on its internal operations, feeding the output back as input, in a way that ultimately causes it to take longer to run, is considered to be an adaptive one-way function. Because the developer can control how many iterations take place, it is adaptive. Adaptive design has been used by architects to safeguard passwords stored in hash algorithms (like PBKDF2) and encryption techniques (such as bcrypt).
4) *Hash functions used in cryptography and their trade-offs:* Attackers do face obstacles from cryptographic hash functions, much like how speed bumps slow down a motorcycle going too fast. But it's important to keep in mind that the motorcycle will eventually continue to travel down the street. But your adversaries—regular users and your server—will also be slowed down by these barriers.

C. *Asymmetric key Cryptography*

In this approach, information is encrypted and decrypted using a pair of keys. When encrypting data, a public key is used, and when decrypting data, a private key is used. Private Key and Public Key are distinct. Even if everyone knows the public key, only the intended recipient can decode the message because only he has right to possession.



1) Cryptography used for:

Computer passwords
Digital Currencies
Secure web browsing
Electronic Signatures
Authentication
Cryptocurrencies
End-to-end encryption

2) Caesar Cipher Technique

One of the earliest and most basic encryption techniques is the Caesar Cipher. It is merely a sort of substitution cypher in which each letter of a given text is substituted with a letter that is located a certain number of positions farther down the alphabet. As an illustration, if there was a shift of 1, A would be replaced by B, B by C, and so on. Julius Caesar, who reportedly employed it to communicate with his officials, is said to be the inspiration for the method's moniker**.**

Therefore, in order to cypher a given text, we require an integer value, or "shift," that represents the number of positions down which each letter in the text has been moved.

Modular arithmetic can be used to depict the encryption by first turning the letters into numbers.

$$E_n(x) = (x + n) mod\ 26$$

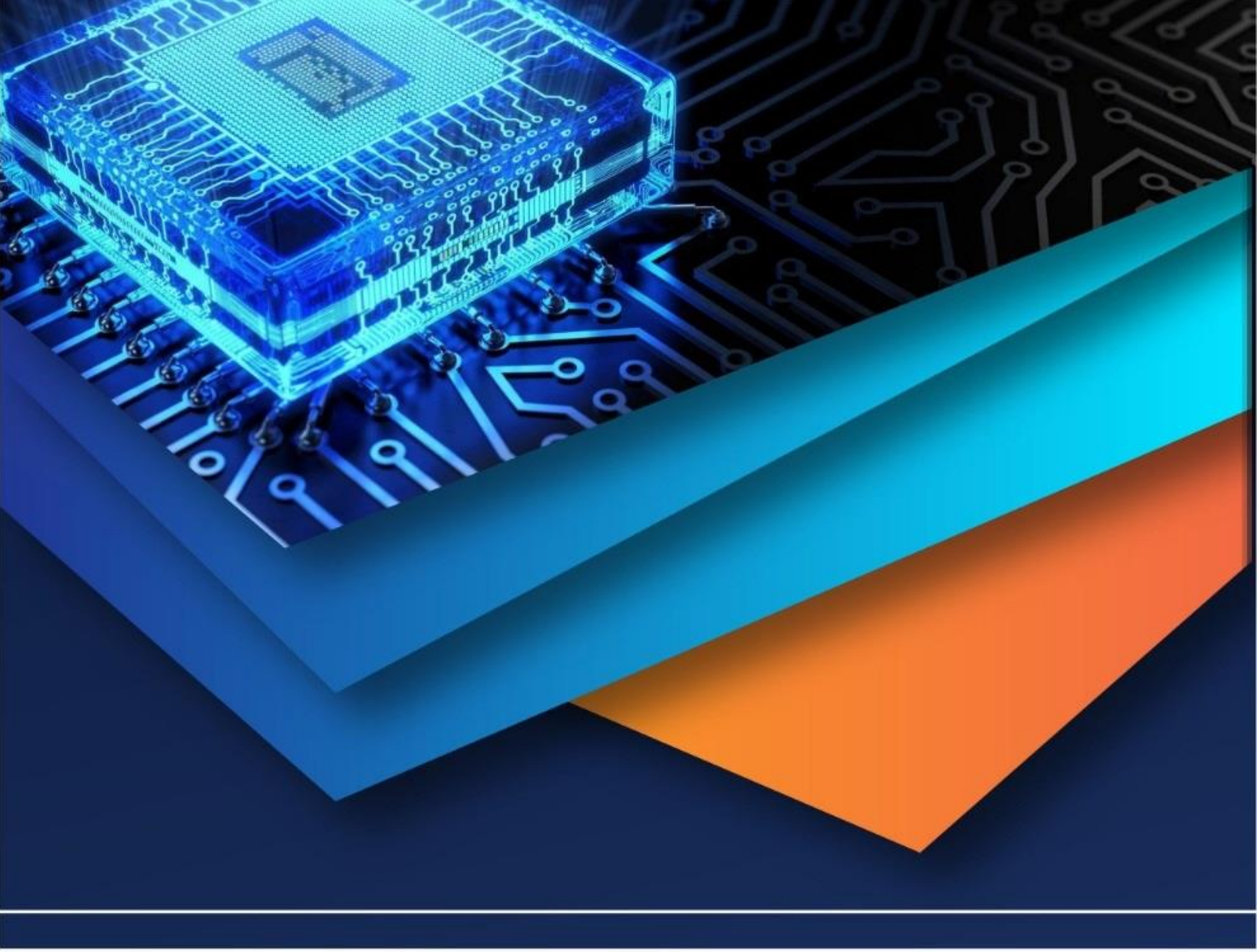
(Encryption Phase with shift n)

$$D_n(x) = (x - n) mod\ 26$$

(Decryption Phase with shift n)

REFERENCES

[1] Abdalbasit Mohammed Qadir and Nurhayat Varol, A Review Paper on Cryptography, https://www.researchgate.net/publication/334418542_A_Review_Paper_on_Cryptography, 23 october 2019
[2] Yahia Alemami, Mohamad Afendee Mohamed, Saleh Atiewi, Research on Various Cryptography Techniques, International Journal of Recent Technology and Engineering (IJRTE) ISSN: 2277-3878, Volume-8, Issue-2S3, July 2019



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY