International Journal of Trend in Scientific Research and Development (IJTSRD)
Volume 6 Issue 6, September-October 2022 Available Online: www.ijtsrd.com e-ISSN: 2456 – 6470

Cryptography Methodologies

Devendra Kumar Meena[1], Dr. A. Rengarajan[2]

[1] MCA Scholar, [2]Professor,

[1,2]School of CS and IT, Dept of MCA, Jain (Deemed-to-be University), Bangalore, Karnataka, India

ABSTRACT

From the last several years data and Security has become a main concern for anyone who connected to the internet. Data security prevents any modification in our data and ensures that our data is only accessible by the intended receiver. We have redeveloped methods and algorithm to achieve this level of security. Cryptography Is a technique for securing data, information and communication using some algorithms that make the data unreadable for human eye. We can decrypt the data using algorithm that is predefined by the sender.

KEYWORDS: *Mothers, quality of life, normal vaginal delivery, caesarean section*

How to cite this paper: Devendra Kumar Meena | Dr. A. Rengarajan "Cryptography Methodologies" Published in International Journal of Trend in Scientific Research and Development (ijtsrd), ISSN: 2456-6470, Volume-6 | Issue-6, October 2022, pp.2030-2032, URL: www.ijtsrd.com/papers/ijtsrd52232.pdf

IJTSRD52232

Objective

To understand the concept and techniques of cryptography used in communication, information and data transfer.

Literature Review

What is cryptography, how cryptography works, where we use the concept of cryptography, how algorithm is used in securing the data, working of AES and DES algorithm.

Introduction

Cryptography is a technique to achieve confidentiality of data. Cryptography term has a specific meaning in Greek: “secret writing”. Nowadays the privacy of organizations and individuals is provided by cryptography and making sure that data or information sent is secure in a way that the authorized receiver can access this information. Cryptography is very old technique, back to 2000 B.C. Egyptians used “secret” hieroglyphics.

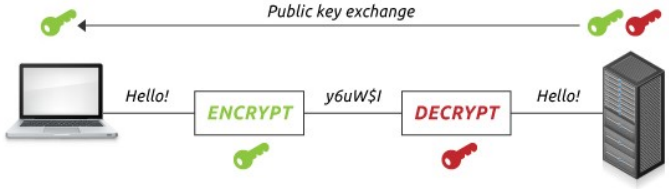

Figure 1: Cryptography

We need to know something about following terminology before start with cryptography:

Encryption: encryption process converts a plain text into a cipher text.

Decryption: decryption is inverse process of encryption; it converts a cipher text into a plain text

Cipher: Cipher is an algorithm for encrypting and decrypting data.

Classification of Cryptography

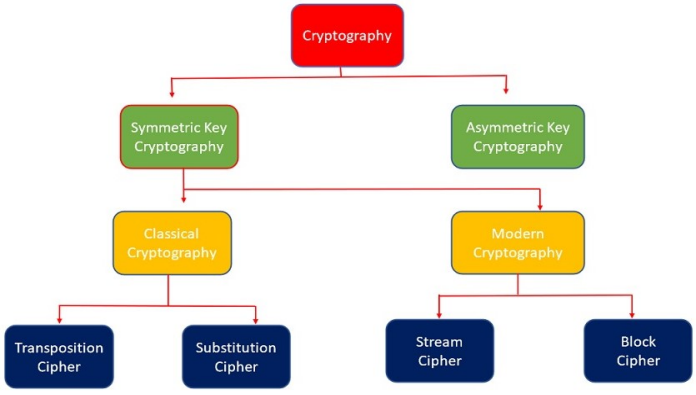

Figure 2: Classification of Cryptography

Symmetric Key Cryptography

Symmetric key cryptography is a type of encryption scheme in which the sender and receiver of a message share a single, common key that is used for both encryption and decryption the message. Symmetric key cryptography also known as private-kay, single-key and secret-key cryptography. Data Encryptions Standards (DES) is the most popular symmetric key system. Symmetric key cryptography Mostly used in banking application where personal information's need to be encrypted. Symmetric cryptography helps in detecting bank frauds. Symmetric key cryptography also helps in protecting data that is not in transit and dress on servers and data centers.

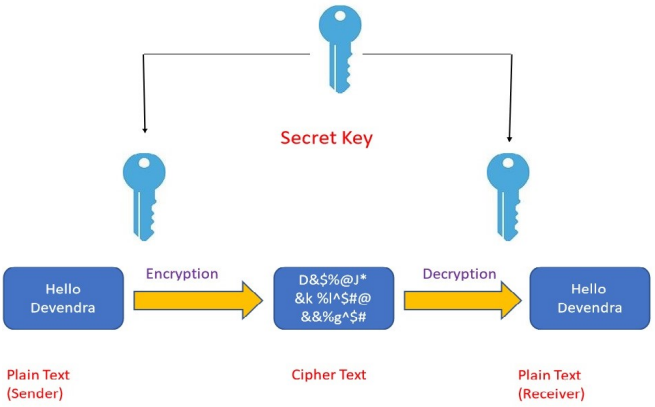

Figure 3: Symmetric Key Cryptography

Asymmetric Key cryptography

Asymmetric key cryptography also known as public-key cryptography. Two different keys are used in asymmetric key cryptography. Private key is used for encrypting the data and public key is used for decrypting the same data.

Each user has two keys (private key and pubic key) in asymmetric key cryptography. Both keys (private and public) are mathematically related. Public key and private key together are called the key pair. The public key is available for everyone but the private key is not available for everyone. Private key is secret key. Both private and public key are required to perform an operation e.g., data encrypted with the public key is decrypted with the private key. Encrypting the data with the private key creates a digital signature. This digital signature ensures the message has come from stated sender.

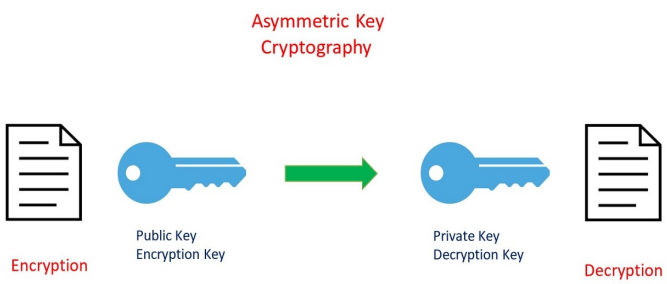

Figure 4: Asymmetric Key Cryptography

Classical Cryptography

1. Transposition Cipher

Transposition cipher is a cryptographic algorithm. In this algorithm the order of alphabets in the pain text is rearranged to form of a plaintext. In this algorithm process the actual plain text alphabets are not included.

An example for a transposition cipher algorithm is columnar transposition cipher where each character in the pain text is written horizontally with the specified alphabet width. The cipher code is written vertically, which creates an entirely different cipher text.

The plain text hello devendra, and let us apply the simple columnar transposition technique as shown below.

h	e	l	l
o	d	e	v
e	n	d	r
a			

The plain text characters are placed horizontally and the cipher text is created with vertical format as: hoeaedn led lvr . The receiver has to use the same table to decrypt the cipher code to plain text.

2. Substitution Cipher

Substitution cipher is a cryptographic algorithm. It is the most commonly used cipher. It includes an algorithm of substituting every plain text character for every cipher text character. In this algorithm process, alphabets are jumbled in comparison with Caesar cipher algorithm.

Keys for a simple substitution cipher usually consists of 26 letters. An example key is -

plain alphabet: abcdefghijklmnopqrstuvwxyz
cipher alphabet: pqowieurytalskdjfhgmznxbcv

An example using the above key
Plaintext: hello devendra Ciphertext: rilld winikwhp

Modern Cryptography

1. Stream cipher

Stream cipher encrypt one bite at a time. Stream ciphers operate on pseudorandom bits generated from the key, and the plaintext is encrypted by XORing both the plaintext and the pseudorandom bits.

Stream Cipher follows the sequence of pseudorandom number stream. One of the best benefits of following stream cipher is to make cryptanalysis more difficult, so the number of bits chosen in the Keystream must be long in order to make cryptanalysis more difficult.

The longer key achieved the stronger security and it helps in preventing any attack.

2. Block Cipher

Block cipher consists an algorithm for encryption and another algorithm for decryption. Block cipher takes a block of plaintext and generates a block of ciphertext, generally of same size. Block size is fixed in given scheme.

Pseudorandom permutation is used in order to make the block cipher more secure. That means if the key is kept secret, the attacker will not be able to decrypt the block cipher and compute the output from any input. In a block cipher two values are generally referred to the size of the block and the size of the key. Most of the block ciphers use a 64-bit block or a 128-bit block.

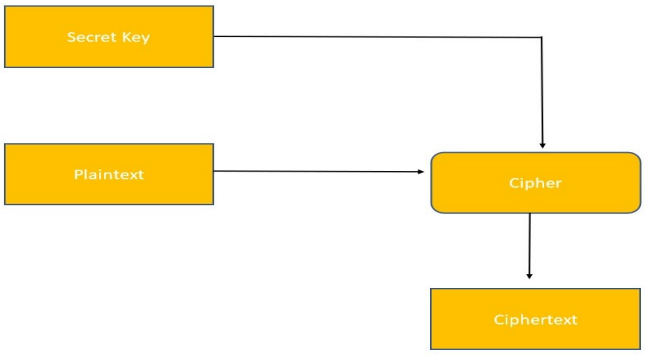

Figure 5: Block Cipher Diagram

CONCLUSION

Cryptography plays a important and critical role in achieving the primary aims of security goals such as authentication, integrity, confidentiality, etc. Cryptographic algorithms are developed in order to successfully achieve these goals. Cryptography has the important purpose of providing strong, reliable, and robust data and network security. In this paper, we demonstrated a review of some of the research that has been conducted in the field of cryptography as well as of how the various algorithms used in cryptography for different security purposes work. Cryptography will continue to emerge with business plans and IT in regard to protecting financial, personal, ecommerce, and medical data and providing a respectable level of privacy.

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

[3] Vipin Kumar Gupta, A Literature Review on The Concept of Cryptography and RSA Algorithm

[4] https://www.researchgate.net/publication/360175324_A_LITERATURE_REVIEW_ON_THE_CONCEPT_OF_CRYPTOGRAPHY_AND_RSA_ALGORITHM, International Journal of Advance and Innovative Research, IISN:2394-7780, volume 9, issue- march 2022

[5] https://www.tutorialspoint.com/cryptography/

[6] https://www.geeksforgeeks.org/cryptography-and-its-types/