International Journal of Scientific Research in Computer Science, Engineering and Information Technology

ISSN : 2456-3307

OPEN ACCESS

Available Online at : www.ijsrcseit.com
doi : https://doi.org/10.32628/CSEIT2410290

Research on Various Cryptography Techniques

Bharati A. Patil, Prajakta R. Toke, Sharyu S. Naiknavare
Dr. D. Y. Patil Arts, Commerce & Science College, Pimpri, Pune, Maharashtra, India

ARTICLEINFO

Article History:

Accepted: 10 April 2024
Published: 22 April 2024

Publication Issue
Volume 10, Issue 2
March-April-2024

Page Number
685-692

ABSTRACT

Cryptography is utilized to make secure data transmission over networks. The algorithm called for cryptography should meet the conditions of authentication, confidentiality, integrity and non-repudiation. Cryptography is a technique used from decenniums to secure and forfend the information and send the data from one place to another without the trepidation of having been read out by some unauthorized and unauthenticated denotes. Several ways has been developed in this field to make the information more secure and evade trespassing. However these methods may have some loopholes or shortcoming which leads to the leakage of information and thus raising a question of information security. The cryptographic technique is utilized not only to provide the security but additionally it deals with data integrity, confidentiality and non-repudiation issues.

To safeguard data during transmission or storage, sundry algorithms and methods have been developed in the field of security. A wide range of cryptography approaches are employed, each with its own set of strengths and inhibitions that are acclimated to provide data security. Cryptography can be defined as techniques that cipher data, depending on categorical algorithms that make the data unreadable to the human ocular perceiver unless decrypted by algorithms that are predefined by the sender. It encrypts data utilizing a set of algorithms such as symmetric and asymmetric algorithms. These encryption methods vary in terms of vitality, celerity, and utilization of resources (CPU utilization, recollection, and power).

It is utilized to bulwark personal identifiable information (PII) and other confidential data, authenticate identities, avert document tampering, and build trust between servers. Cryptography is one of the most paramount techniques utilized by digital businesses to safeguard the systems that store their most valuable asset – data – whether it is at rest or in kinetic Customer PII, employee PII, perspicacious property, company strategies, and any other confidential information are examples of data. As a result, cryptography is a vital infrastructure, as the aegis of sensitive data increasingly relies on cryptographic solutions. In this paper I have discussed various cryptographic techniques and the inhibitions of those techniques as well. Some cryptographic algorithms are briefly described and their impact on the information is additionally mentioned.

Keywords : Cryptography, Information Security, Encryption, Decryption, Symmetric Cryptography, Asymmetric Cryptography Private Key, Public Key

I. INTRODUCTION

Security is a consequential in for fending data against intruders. One of the most consequential methods for ascertaining data secrecy is cryptography. Cryptography is secret inscribing for data security auspice. Well-masked data cannot facilely be read, modified or fabricated. Now a day's all works cognate to banking, ATM card, credit card, marketing, E commerce etc. is doing with the avail of internet. So there must be aegis provided over the network. Consequently for secure communication we have several cryptography techniques are utilized. We apply these cryptographic techniques to sensitive information in order to provide bulwark from an unauthorized access. In cryptosystem, data are bulwarked via encryption method for keeping communication is private. Every one send the private message by encrypting the message and intended receiver decrypts it by its key. Cryptography peradventure the most paramount element of communication's security and is becoming increasingly paramount as a rudimentary building block for computer security. Encryption is the process of encoding a message in such a way as to hide its contents. Modern cryptography includes several secure algorithms for encrypting and decrypting messages. These are all fixated on the utilization of secrets called keys. A cryptographic key is a parameter utilized in an encryption algorithm in such a way that the encryption cannot be broken without the cognizance of the key. Encryption is the method of encoding a message in order to encrypt its contents.

In the presence of an adversary, cryptographic procedures are habituated to ascertain data secrecy and integrity. Sundry cryptographic approaches, such as symmetric-key cryptography or public-key cryptography, can be utilized during data conveyance and storage depending on the security demands and hazards involved.

Furthermore, cryptography enables sundry computations on encrypted data without the desideratum to decode the data for processing. These approaches are consequential for protect personal information from being leaked during conveyance and from storage servers from a privacy standpoint. A multi-layered security plan should include cryptographic approaches. Some security measures, such as the utilization of a firewall and access sanctions, endeavour to keep intruders out of the network or computer entirely, homogeneous to how fences and door locks endeavour to keep purloiners off the property or out of the house. An inner line of bulwark is provided by cryptography.

Cryptography forfends data from intruders who are able to perforate the outer network bulwarks and from those who are sanctioned to access the network but not this particular data, much homogeneous to a wall safe bulwarks valuables from people who are sanctioned to enter your house but not this particular data.

A plain or mundane text sent over the network is converted into cipher text so that the information can only be utilized by the sender and the receiver. The method of converting plain text messages into cipher text messages is called encryption, in technical terms. The method of converting cipher text into plain text again is kenned as decryption. Decryption is precisely diametrical to encryption. The computer at the cessation of the sender customarily converts a plain text message into cipher text messages in computer to computer communications by performing encryption. Then, this message is sent over the network to the receiver. To get plain text, the receiver's computer takes the encrypted message and performs the decryption method. The encryption and decryption process is called cryptography. Cryptography in general is the art and science of achieving aegis by encoding messages to make them unreadable. It can be utilized in any way to mask the important of the information. It can additionally be applied to software, graphics or voice. The encryption inceptions date back to the days of the great Julius Caesar. Caesar utilized this strategy to send his messages confidentially. One of the most facile methods of encryption is the Caesar's form, commonly kenned as Caesar's Cipher. The encryption methods of today are much more involute and advanced compared with it. In order to convert sensible information into an incomprehensible format, prodigiously intricate algorithms are being applied today. When encrypted; only the felicitous keys, kenned as' Cryptographic Keys,' can decrypt the data. A cryptographic key is simply a password which is utilized to encrypt and decrypt information.

Supersession technique and Transposition technique are the types of operation utilized for converting plain text into cipher text. A supersession technique is one in which plain text letters are superseded with other letters, numbers or symbols. In Transposition Technique the plaintext letters perform some kind of permutation. Cryptographic process is show in Fig 1.

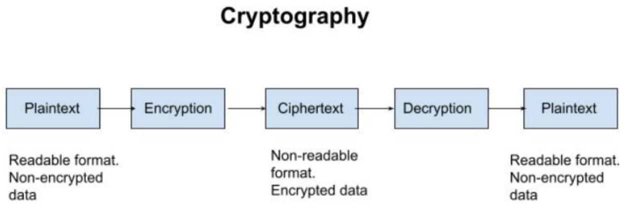
Cryptography
Plaintext
Encryption
Ciphertext
Decryption
Plaintext
Readable format. Non-encrypted data
Non-readable format. Encrypted data
Readable format. Non-encrypted data

Fig 1. Cryptographic process

II. TERMINOLOGY

1. **Plaintext:** The original and understandable text. As an instance, 'Y' needs to transmit a “Computer” message to 'Z'. Here, “Computer” is the plaintext or the original message.
2. **Cipher text:** The text that cannot be understood by way of anybody or a gibberish text, example “A@$&J9.”
3. **Encryption:** A process of changing clear text into unclear text. The manner of encipherment needs an encipherment algorithm and a key. Encipherment occurs on the sender side.
4. **Decryption:** A reverse method of encode. It is a manner of converting cipher text into plaintext.
5. **Key:** A key is character, number, or a special character. It is used at the time of encipherment on the original text and at the time of decode on the cipher text.
6. **Steganography:** It is actually the science of hiding information from people who would snoop on you. The difference between Steganography and encryption is that the would-be snoopers may not be able to tell there’s any hidden information in the first place.
7. **Cryptography:** The study of both encryption and decryption.

Purpose of Cryptography

1. Authentication: The potential of a system to test the identity of the sender.
2. Confidentiality: Information transmitted ought to be accessed handiest by using legal parties and not through anyone else.

3. Integrity: Only the authorized parties are permitted to alter on transmitted information.
4. Non-repudiation: Is the guarantee that someone cannot deny the validity of something.
5. Access Control: Just the authorized persons are capable to get right of entry to the given information.

Evaluation Parameters

Each encryption algorithm presents strengths and weaknesses in terms of their parameters. Some parameters that determine encryption performance are described as follows.

1. Encryption time: Measured in milliseconds, depend on the data block length and key length. It directly influences the performance of the encryption algorithm. The performance of an algorithm is regarded as advanced when the encryption time is rapid.
2. Decryption time: The time period to regain the original text from cipher text; it is also measured in milliseconds. The performance of an algorithm is regarded as superior when the decryption time is rapid.
3. Memory used: A low memory usage is desirable because it affects system cost.
4. Throughput: Is computed through way of dividing the whole encoded block size on the entire encodes time. The power consumption of the algorithm will decrease, if the throughput cost increases

III.CRYPTOGRAPHIC TECHNIQUES

There are two basic information encryption techniques: symmetric encryption, which is also called secret key encryption, and asymmetric encryption, also called public key encryption.

A. Symmetric Encryption

Symmetric-key cryptography refers to methods of encryption, in which the sender and the receiver share the same key. Symmetric key ciphers are either used as block ciphers, or as stream ciphers. A block cipher enciphers the input type used by a stream cipher, in plaintext blocks as opposed to individual characters. Symmetric cryptography is much faster than asymmetric. The symmetric encryption is shown in Fig 2.

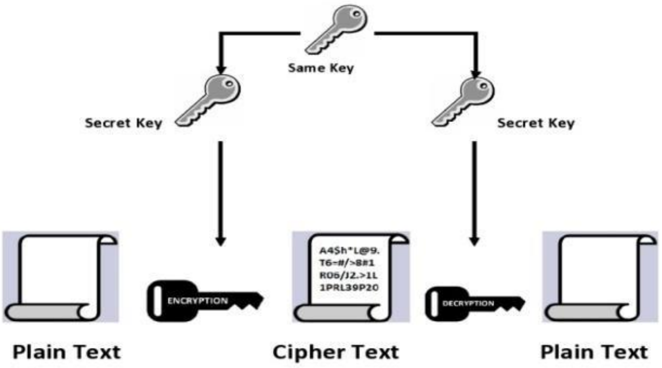

Fig 2. Symmetric Encryption

The symmetric techniques are those methods in which a

single key is used to encrypt and decrypt the data and this

secret key is shared among the sender and receiver in advance before transferring the data. We call this key as Private Key.

There are four general categories of Symmetric Cryptography

1. Ceaser Cipher
2. Playfair
3. Monoalphabetic
4. Polyalphabetic
5. Deffie Hellman Key Exchange Technique

A. Ceaser Cipher Technique

This method is one of the simplest and oldest methods of

substitution. The idea is to substitute each letter of the plaintext with 3 letters ahead of it.

For e.g.:

1. Plain: abcdefghijklmnopqrstuvwxyz
2. Key: defghijklmnopqrstuvwxyzabc

3. Plaintext: let me send you message
4. Cipher text: ohw ph vhqg brx phvvdjh
5. Loophole: In this method is that every letter has a fixed substitution and thus it is very easy to guess the key.

B. Playfair Technique

Developed by Charles Wheatstone, this method proved to be one of the best known techniques of that time during the World War II. The steps involved are:

1) Choose the Keyword

a) Rules

-No repetition of letters

2) Create Table

a) Rules

- Create a 5×5 matrix and insert the key into it and fill the remaining cell by other alphabets.

- Letter 'j' not to be included in the matrix.

3) Plaintext

a) Rules

- Split the text into pairs

- If the plaintext is of odd length then make it even by appending letter 'x' in the end string

- Replace the repeating letters with letter 'x'.

4) Insert the pairs into the matrix separately

a) Rules

- If both the letters are in same column then move each of them one letter down and if we reach the table end then wrap around

- If both the letters are in same row then move each of them one letter right and if we reach the table end then
wrap around

- If the letter forms a rectangle then swap it with the letter present at the end of the rectangle.

5) Example

Let us encrypt the plaintext "memory" and let us choose key as "security". Now we build a 5×5 matrix as

s	e	c	u	r
i	t	y	a	b
d	f	g	h	k
l	m	n	o	p
q	v	w	x	z

Table 1: 5×5 Matrix with Keyword "Security"

Now the plaintext "memory" can be break down into pair of letters as: me, xo, ry. The pair "me" is in same column, so we can move one letter down and thus we get "vt".Similarly "xo" are also in same column so we get "ux" and for the pair "ry" we get "ca". Thus, finally we get "vtuxca" as cipher text for the plaintext "memory".

a) Loophole

The letters changes itself but their frequency does not change. Thus the attacker may easily obtain the plaintext from the frequency analysis table. Another limitation of this method is that it has a five cross five matrix that can store on 25 uppercase characters or 25 lowercase characters due to which it is unable to store both uppercase and lowercase characters together in a single matrix. Apart from this, the whitespaces and other different characters are not possible to be stored.

C. Monoalphabetic Technique

This is another type of Symmetric Technique in which the letters are replaced by fixed alternates. One of the oldest monoalphabetic techniques is the ATBASH Technique in which the first alphabet is replaced by the last letter of the alphabet order.

For e.g.:

1. Plain: abcdefghijklmnopqrstuvwxyz
2. Key: zyxwvutsrqponmlkjihgfedcba
3. Plaintext: let me send you message
4. Cipher text: ovg nv kvmw blf nvhhztv
5. Loophole: Anyone can easily identify the letters as it is simply based on ascending and descending order ofalphabets. Thus even the immature in the field of

cryptography can easily identify the pattern and thus the information may get revealed.

D. Polyalphabetic Technique

This method is way better than the monoalphabetic substitution technique as it works on the concept that the

same alphabet can be altered with different alphabets. One of the oldest methods of this kind is ALBERTI Cipher. Alberti formed two rings the outer ring and the inner ring.

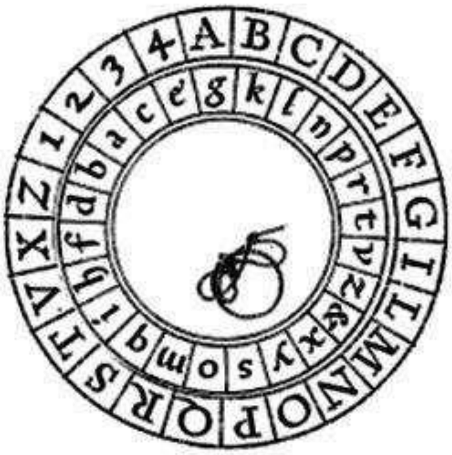

Fig. 3: Alberti formed two rings

The outer ring refers to the letters of the plaintext and the inner circle refers to the letters to be substituted. After certain conversions the inner ring is rotated and thus the corresponding substitution changes.

1) Loophole

The loophole of the Alberti Cipher the repeating key. If an expert cryptanalyst could find out the length of the key, he can treat the cipher text as a number of interwoven Caesar Ciphers, which can all individually be broken. Both Kasiski and Friedman have developed a mathematical test to determine the length of the key. A weakness of Alberti Cipher is that somehow the shifts in alphabets are necessary to be communicated to the recipient. Therefore, to enable it an index letter is chosen on the inner ring that indicates on the outer ring referring which position it corresponded to. This corresponding present in outer capital letter is then inserted in the cipher text at the position where the shift happens. The result of this is a cipher text that is primarily written in lowercase, but occasionally at some places contains an uppercase letter too. For someone unfamiliar to the Alberti cipher and trying to break the code, this cipher text would be

very hard to break. However, if the code breaker is aware of the method of the Alberti cipher, it would very obvious to recognize the pattern, and therefore extremely easy and simple to break.

B. Asymmetric Encryption

Asymmetric key cryptography refers to methods of encryption, in which the sender and the recipient share the same key. A key is used to encrypt, and the other to decrypt. It gives greater stability than the symmetrical systems. Asymmetric Encryption is a relatively new and complex Encryption style. Complex, because it uses two cryptographic keys for data security implementation. Such keys are referred to as a public key, and a private key. As the name suggests, the Public Key is open to anyone wishing to send a message. On the other hand, the public key owner keeps the private key in a secure place. The asymmetric encryption is show in Fig.4.

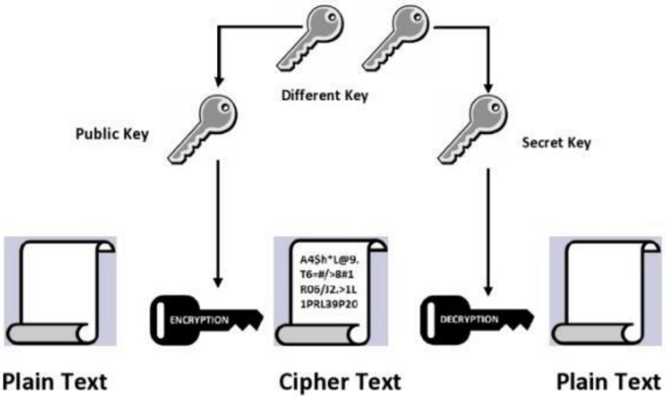

Fig. 4 Asymmetric Encryption

Asymmetric encryption is also known as public key cryptography, opposed to symmetric encryption, which is a relatively new technique. For asymmetric encryption, two keys are used to encrypt a plain text. Hidden keys are shared over a large network or over the Internet. This means the keys are not misused by malicious people. It is important to note that anyone with a secret key can decrypt the message and that is why asymmetric encryption uses two related keys to improve security. Anyone who might want to send you a message will be given a public key free. The second private key is kept a secret for you to know only. A message encrypted using a public key can only be decrypted using a private key, while using a public key can also decrypt a message encrypted using a private key. Public key protection is not needed since it is available to the public and can be transmitted over the internet. Asymmetric key has a far better power to ensure that information exchanged during communication is secure.

➢ Rivest-Shamir-Adleman (RSA)

RSA stands for the name of three inventors Rivest Shamir and Adleman. RSA is the most commonly used algorithm for the public key encryption. It can be used for both digital signatures and the encryption. RSA's protection is commonly seen as factoring. RSA is one of the first functional cryptosystems with a public key and is commonly used for secure data transmission. The encryption key is available in such a cryptosystem, which varies from the decryption key that is kept secret. In RSA this asymmetry is based on the practical complexity of factoring two large prime numbers product, the question of factoring. The problem for the attacker is that it is presumed that computing the inverse d of e is no simpler than factorizing n. For a reasonable level of safety, the key size should be greater than 1024 bits. Size keys, say, which provide 2048 bits.

a. Key Generation

(1) Select p and q both prime number, p is not equal to q.

(2) Calculate n = p x q.

(3) Calculate ø (n) = (p -1) x (q-1).

(4) Select integer e whose gcd (Ø (n), e) = 1; 1 < e

(5) Calculate private key d = e-1 (mod Ø (n)).

(6) Public key PU = {e, n}.

(7) Private Key PR = {d, n}.

b. Encryption Procedure

C= M ^e mod n.

c. Decryption Procedure

M = C ^d mod n.

Where, M is message, p and q are prime numbers, n is common modulus, e and d are public and private keys.

➢ Diffie-Hellman (DH)

It's that algorithm for public key encryption, using discrete logarithms in a finite field. Two parties allow a secret key to be shared without prior secrets over an unreliable medium. Diffie-Hellman (DH) is a key exchange algorithm that is commonly used. Two parties wish to begin communicating in many cryptographically protocols. Diffie-Hellman protocols are exchange keys and allow common secret key to be created over an unconfident communication channel. This issue is related to discrete logarithms; its name is Diffie-Hellman issue. This problem is complicated, as contrasted with the problem of the discrete logarithm. Diffie-Hellman key exchange, also known as exponential key exchange, is a digital encryption system that uses numbers raised to specific powers to generate decryption keys based on components that are never transmitted directly, thereby mathematically overcoming the task of a would-be code breaker.

IV. CONCLUSION

Cryptography is a tool which makes out data transmission secure and apart from this it also provides data integrity, nonrepudiation and confidentiality. Out of symmetric and asymmetric key cryptography, the public key cryptography or the asymmetric cryptography has become an indispensable component for our global digital communication network.

These networks support a many basic communities like mobile phones, internet, social networks, and cloud computing and distributed resources. In the world of computer science, Cryptography is a very interesting field because the amount of work performed is kept only secret. There are different techniques and algorithms researched, and various types of work have been performed. In this paper briefly discussed cryptography and its form of symmetric key cryptography and algorithms for asymmetric key cryptography.

V. REFERENCES

[1]. “Cryptography and Network Security: Principles and Practice” by William Stallings.

[2]. Hershey, J. E. Cryptography Demystified. New York: McGraw-Hill.

[3]. H.Kenneth, “Elementary Number Theory and Its Applications “Third Edition. Addison-Wesley, (1992)

[4]. Cryptography Algorithms: A guide to algorithms in blockchain, quantum cryptography, zero-knowledge protocols, and homomorphic encryption.