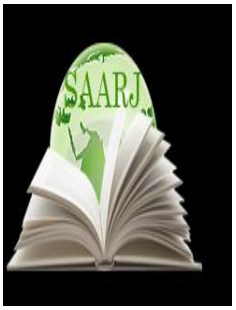
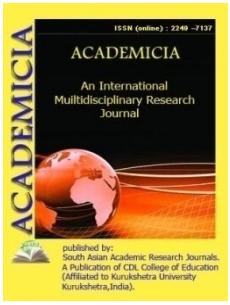


ACADEMICIA
An International Multidisciplinary Research Journal
(Double Blind Refereed & Peer Reviewed Journal)



DOI: 10.5958/2249-7137.2021.02108.X

A BRIEF STUDY ON CRYPTOGRAPHY

Dr. Ajay Rana*; Mridul**

*Shobhit Institute of Engineering and Technology,
(Deemed to be University), Meerut, INDIA
Email id: ajay.rana@shobhituniversity.ac.in,

**School of Computer Science and Engineering,
Faculty of Engineering and Technology,
Shobhit Institute of Engineering and Technology,
(Deemed to be University), Meerut, INDIA
Email id: mridul@shobhituniversity.ac.in

ABSTRACT

Data security has become a top worry for everyone linked to the internet, as it has merged with our lives and grown at a breakneck pace over the past few decades. Data security guarantees that only the intended recipients have access to our information and prohibits any data modification or change. Various techniques and approaches have been developed to attain this degree of security. Cryptography is a set of methods for encrypting data using particular algorithms that render the data unreadable to the naked eye until decoded using preset procedures by the sender. In order to secure personal, financial, medical, and ecommerce data while maintaining a reasonable degree of privacy, cryptography will continue to be used in IT and business strategies. Cryptography is an ancient technology that is continuously being explored, with historical origins.

KEYWORDS: *Cryptography, Security, Algorithm, Cipher, Decryption, Data Security.*

1. INTRODUCTION

Cryptography is a method of ensuring message secrecy. In Greek, the word has a particular meaning: "hidden writing." Nowadays, however, people and organizations' privacy is protected by high-level encryption, which ensures that information transmitted is safe and only the authorized recipient has access to it. Examples date back to 2000 B.C., when the ancient

Egyptians employed "secret" hieroglyphics, as well as other evidence from ancient Greece and Rome, such as hidden inscriptions and the renowned Caesar cipher[1]–[3].

Hundreds of millions of individuals use cryptography on a regular basis to secure data and information, but the majorities are unaware of it. Cryptographic systems, in addition to being very valuable, are also exceedingly fragile, since a single programming or specification mistake may undermine them. Figure 1 illustrates the concept of cryptography.

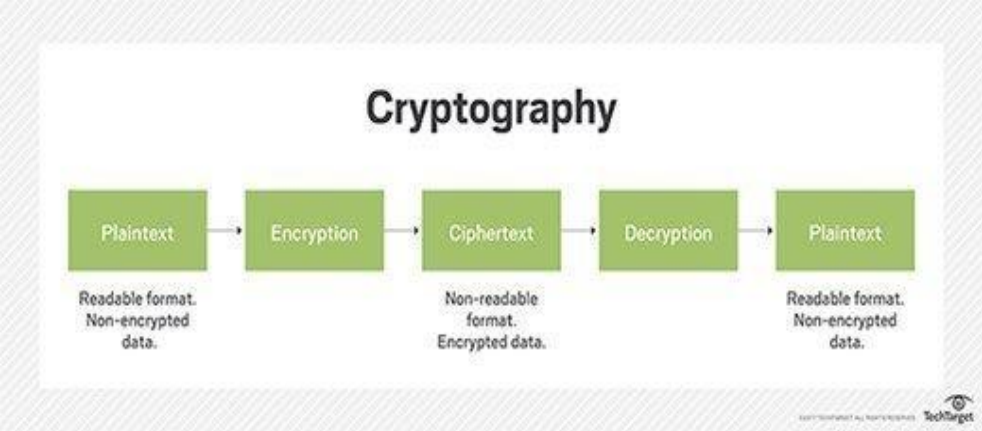


Figure 1: Illustrates the Concept of Cryptography[4]**.**

1.1 Historical Algorithms:

This part will present a few historical algorithms, as well as pencil and paper examples for the non-mathematical reader. Long before public key cryptography was introduced, these methods were developed and deployed.

1.2 Caesar Cipher:

During the Gallic Wars, Julius Caesar, the Emperor of Rome, developed one of the oldest and earliest instances of cryptography. The letters A through We are encoded using the letters three positions ahead of each letter in the alphabet, while the remaining letters A, B, and C are represented by X, Y, and Z in this kind of method. This implies that a "shift" of 3 is employed, but we could have a similar effect on the encrypted text by using any value between 1 and 25. As a result, a shift is now often referred to as a Caesar Cipher.

The Caesar cipher is easy to crack since it is one of the most basic forms of encryption. The letters that were shifted must be moved three letters back to their original places in order to decode the cipher text. Despite this flaw, it may have been powerful enough for Julius Caesar to employ throughout his battles in the past. However, since the shifted letter in the Caesar Cipher is always three, anybody attempting to decode it just has to move the letters[5], [6].

1.3 Simple Substitution Ciphers:

Take, for example, the Simple Substitutions Cipher, commonly known as the Monoalphabetic Cipher. In a Simple Substitution Cipher, the alphabet letters are placed in random order beneath the correctly written alphabet, as shown here:

A B C D E F G H I J K L M D I Q M T B Z S Y K V O F N O P Q R S T U V W X Y Z E R J A U W P X H L C N G

The same key is used for encryption and decryption. The encryption rule is that "each letter is substituted by the letter underneath it," while the decryption rule is the inverse. For example, the plaintext CAN's equivalent cipher text is QDN.

1.4 Transposition Ciphers:

Other cipher families use a key and a specific rule to arrange the letters in plaintext to convert them to cipher text. Transposition is the process of changing the letters in plaintext using rules and a particular key. A columnar transposition cipher is one of the most basic kinds of transposition ciphers, and it comes in two flavors: full columnar transposition and partial columnar transposition. A rectangle shape is used to represent the written plaintext horizontally, regardless of which form is used, and its width should correspond to the length of the key being used. The message may be written in as many rows as needed[7]–[9]. When using full columnar transposition, the plaintext is transcribed and any empty columns are filled with null to ensure that each column has the same length. For example:

s e c o n d

d i v i s o n

a d v a n c i n g

t o n i g h t x

Depending on the key, the cipher text is then generated from the columns. If we use the key "321654" in this example, the cipher text will be:

cvdngeiaiisdncndonoxnsattoivgh

However, when it comes to an incomplete columnar transposition cipher, the columns are not required to be completed, so the null characters are left out. This results in columns of different lengths, which can cause the ciphertext to be more difficult to decipher without the key.

1.5 Modern Algorithms:

a. Stream Ciphers:

Stream ciphers use the key to create pseudorandom bits, and the plaintext is encrypted by XORing the plaintext with the pseudorandom bits. In the past, stream ciphers were often avoided because they were more easily cracked than block ciphers. However, after years of development, the stream cipher has improved in security and can now be used in connections, Bluetooth, communications, mobile 4G, TLS connections, and other applications.

Each bit in a stream cipher is encrypted separately. The first is the synchronous stream cipher, in which the key stream is dependent on the key; the second is the asynchronous stream cipher, in which the ciphertext is reliant on the key stream. A dotted line has been drawn. The stream cipher would be asynchronous if it was present; otherwise, it would be synchronous. An example of an asynchronous cipher is the cipher feedback (CFB).

b. Block Ciphers:

This type of cipher consists of both an algorithm for encryption and an algorithm for decryption:

- The encryption method (E) and a plaintext block (P) are given a key (K), and C is the result, which consists of a ciphertext block. C = E can be used to express the encryption operation (K, P).

The decryption method (D) is the opposite of the preceding process, which involves decrypting the ciphertext for the plaintext, P. P = D is a formula that can be written (K, C).

To make the block cipher more secure, a pseudorandom permutation (PRP) is employed. An attacker will not be able to decode the block cipher and calculate the output from any input if the key is kept secret. This is true as long as K's secrecy and randomness are guaranteed from the attacker's perspective. In a broad sense, this implies that the attacker won't be able to spot any patterns in the data that's either input to or output from the block cipher.

The size of the block and the size of the key are usually referred to in a block cipher. The value of both is crucial to the security. A 64-bit or 128-bit block is used in several block ciphers. Because it's critical that the blocks don't become too big, the memory footprint and ciphertext length are both modest. A block cipher processes blocks rather than bits when it comes to ciphertext length. To put it another way, if we wish to encrypt a 16-bit message and replace the blocks with 128-bit blocks, we must first transform the message to 128-bit blocks; only then can the block cipher begin processing and produce a 128-bit ciphertext. When it comes to memory footprint, we require at least 128-bit RAM to work with and process a 128-bit block. Most CPU registers are tiny enough to fit. Alternatively, specialized hardware circuits may be utilized to accomplish this. In most instances, 68 bits, 128 bits, and even 512-bit blocks are still small enough for efficient implementation. However, if the blocks grow in size (i.e., in kilobytes), the cost and performance of the system may suffer. Figure 2 illustrates the block diagram of cipher.

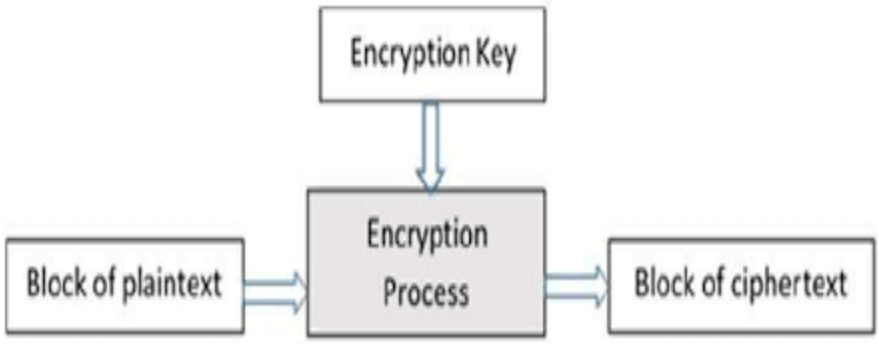


Figure 2: Illustrates the block diagram of cipher[10]**.**

1.6 Hash Functions:

They operate by translating an arbitrarily-sized input to a fixed-size output via a process termed compression, which was formerly known as pseudo random functions (PRF). However, this is

not the same as the compression found in.zip and.rar files. It is, instead, a non-invertible mapping. In order to be helpful, a hash function must satisfy two requirements:

It must have two properties: one, it must be one-way, and two, it must be collision resistant.

1.7 Public key Systems:

A cryptography revolution occurred with the introduction of public key encryption. Even in the 1970s and 1980s, broad cryptography and encryption were clearly restricted to the military and intelligence communities. Cryptography only expanded into other sectors as a result of public key systems and methods.

Because the public key may be shared without fear of being compromised, public key encryption allows us to communicate without relying on secret channels. The following is a list of the public key's characteristics:

- With the use of public key encryption, key distribution may be done via public channels, possibly simplifying the system's initial deployment and making system maintenance easier as parties join or depart.
- The use of public key encryption reduces the need to keep a large number of secret keys. Even if all parties wish to be able to communicate securely, everyone may keep their own private key in a safe manner.
- In open settings, public key cryptography is better, particularly when parties that have never interacted before wish to communicate and engage safely. For example, a business may be able to publish their public key online, and anybody who wishes to make a transaction may use the retailer's public key whenever they need their credit card information encrypted.

1.8 Digital Signatures:

Digital signatures, unlike cryptography, did not exist prior to the advent of computers. With the introduction of computer communications, the need for digital signatures to be addressed emerged, particularly in commercial settings where many parties are involved and each must agree to keeping their declarations and/or offers confidential. Unforgeable signatures were originally proposed hundreds of years ago, but they were handwritten signatures. Diffie and Hellman originally proposed the concept of digital signatures in their article "New Directions in Cryptography."

As a result, in a scenario where the sender and receiver do not have full confidence in one another, authentication alone will not be enough to bridge the gap. Something more is needed, namely a digital signature that functions similarly to a handwritten signature..

1.9 Digital Signature Requirements:

With the “digitalization” age that we are now seeing and living in, the connection that established the link between signature and encryption came into being. The following would be the criteria for an unforgeable signature schema:

- Each user should be able to create their own signature on any document they want.

- Each user should be able to quickly determine whether or not a given string is the signature of a different user.
- No one should be able to create signatures on papers that were not signed by the original owner.

1.10 Digital Signature Principles:

It is critical both within and outside the digital realm to be able to verify that a user or person delivered a message. Handwritten signatures are used to accomplish this in today's society. When it comes to creating digital signatures, public-key cryptography is used. The fundamental concept is that the person signing a document or message uses a private key (called private-key), and the person receiving the message or document must use the corresponding public-key.

1.11 Difference between Digital Signature and Message Authentication:

When communicating via an unsecured channel, parties may want to include authentication in the messages they send to the receiver so that the recipient can determine whether the message is genuine or if it has been altered. Message authentication generates an authentication tag for each message transmitted; receivers must validate it after receiving the message to guarantee that no external attacker has the capacity to create authentication tags that aren't being utilized by the communicating parties.

Message authentication is similar to digital signature in certain ways, but the distinction is that with message authentication, just the second party is needed to authenticate the message. There can be no third-party verification of the message's authenticity or if it was produced by the actual sender. However, in the case of a digital signature, other parties may verify the signature's authenticity. As a result, digital signatures have provided a message authentication method.

2. DISCUSSION

Cryptography is a technique of using codes to secure information and communications so that only those who are supposed to read and process it may do so. The prefix "crypt-" denotes "secret" or "vault," while the suffix "-graphy" denotes "writing." Secret-key cryptography, public-key cryptography, and hash function cryptography are the three kinds of cryptography. Authentication, integrity, secrecy, and no-repudiation are only a few of the main security objectives that cryptography helps to achieve. In the presence of an adversary, cryptographic methods are employed to guarantee data confidentiality and integrity. Various cryptographic techniques, such as symmetric key cryptography or public key cryptography, may be employed during data transit and storage depending on the security requirements and risks involved.

3. CONCLUSION

Authentication, integrity, secrecy, and no-repudiation are only a few of the main security objectives that cryptography helps to achieve. To accomplish these objectives, cryptographic algorithms are created. The aim of cryptography is to provide dependable, strong, and resilient network and data security. Various cryptographic techniques, such as symmetric key cryptography or public key cryptography, may be employed during data transit and storage depending on the security requirements and risks involved. We presented an overview of some of the research that has been done in the area of cryptography, as well as an explanation of how

the various algorithms used in cryptography for various security reasons function in this article. In order to secure personal, financial, medical, and ecommerce data while maintaining a reasonable degree of privacy, cryptography will continue to be used in IT and business strategies.

REFERENCES:

1. V. Mavroeidis, K. Vishi, M. D. Zych, and A. Jøsang, "The impact of quantum computing on present cryptography," *Int. J. Adv. Comput. Sci. Appl.*, 2018, doi: 10.14569/IJACSA.2018.090354.

2. W. J. Buchanan, *Cryptography*. 2017.

3. W. J. Buchanan, S. Li, and R. Asif, "Lightweight cryptography methods," *J. Cyber Secur. Technol.*, 2017, doi: 10.1080/23742917.2017.1384917.

4. "security_cissp_cryptography_mobile." https://searchsecurity.techtarget.com/definition/cryptography (accessed Aug. 02, 2017).

5. J. Buchmann, K. Lauter, and M. Mosca, "Postquantum Cryptography-State of the Art," *IEEE Security and Privacy*. 2017, doi: 10.1109/MSP.2017.3151326.

6. D. J. Bernstein and T. Lange, "Post-quantum cryptography," *Nature*. 2017, doi: 10.1038/nature23461.

7. L. Jian *et al.*, "A survey on quantum cryptography," *Chinese J. Electron.*, 2018, doi: 10.1049/cje.2018.01.017.

8. A. Nitaj, "Post quantum cryptography," *Malaysian J. Math. Sci.*, 2017, doi: 10.1201/9781351021708-9.

9. "Fault analysis in cryptography," *Int. J. Latest Trends Eng. Technol.*, 2017, doi: 10.21172/1.91.29.

10. "cipher." https://www.tutorialspoint.com/cryptography/block_cipher.htm (accessed Aug. 02, 2017).