Data Encryption on Cryptography – A Review

Dr. Manish Pandey[1], Rakesh Kumar[2]
[1]Professor, Himalayan University, Itanagar, Arunachal Pradesh
[2]Assistant Professor, Department of Computer Applications, Tula's Institute, Dehradun

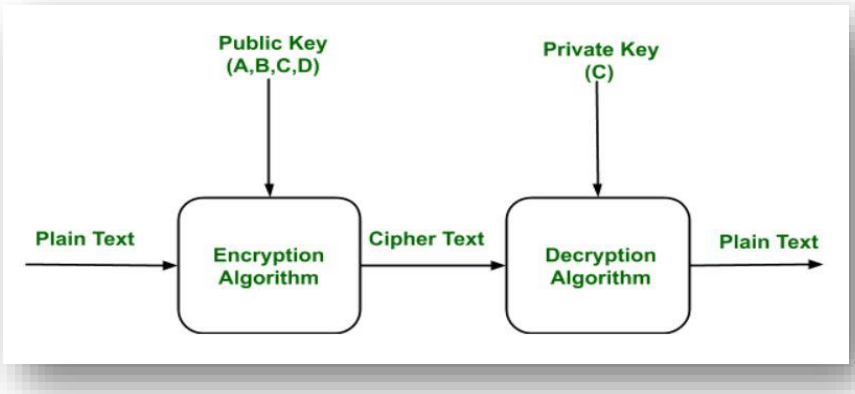
ABSTRACT

With the advent of the internet and the pace of our lives, which has grown significantly over the last few decades, data security has become a major issue for anyone connected to the web. Data security ensures that our data is accessible only to the intended recipient and prevents any modification or alteration of the data. To achieve this level of security, various algorithms and methods have been developed. Cryptography can be defined as data encryption, depending on the specific algorithms that make the data unreadable to the human eye unless the encryption algorithms are specified by the sender.

Keywords: Cryptography, Security, Algorithm, Cipher, Encryption, Data security.

1. INTRODUCTION

Every user while communicating seeks a secure network so that data communication is secure and no criminal can read his or her data. Cryptography is attempted on a both the wireless and wired network, where it converts plane text into cipher text and again cipher text into plain text and this process provides secure data communication. On the sender side the blank text is converted into a cipher text known as encryption and the cipher text on the recipient side is converted into a blank text known as decryption. Troubleshooting is a way to effectively share hidden information. Enter the code a message with a securely secure key known for sending once. Beneficiary conclusion is a remarkable concept for secure security in sensory planning. Secure trading of keys between sender and receiver is a lot of hard work in it critical sensor planning of the property. The information must be resolved first by the customer before it is released to the remote storagebenefit and information both security and information that comes with security should be ensured in such a way that organizations that specialize in distributed storage do not have the capacity to extract information, even when the client needs to pursue a few stages of the even when the client needs to pursue a few stages of the whole information, distributed storage framework will provide external access to see what part of the coded information returned to the client about. This paper examines the security of different systems and cryptographic methods.



2. CRYPTOGRAPHY MECHANISM

Cryptography is a strategy for setting aside and transferring information to a specific framework for those who are expected to read and processes it. This word is often associated with ripping a blank text message into a cipher text, next I'm back again. There are, as a rule, purposes: the secret key cryptography, cryptography of open keys, and hash functions, each is shown below:

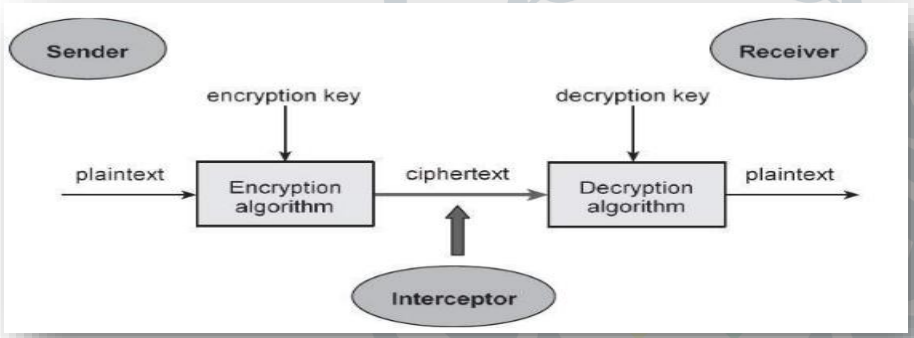
KEYS: A key is a numeric or alpha handwriting text or it may be a different image.

PLAIN TEXT: The first message one wishes to share with another which appears as a blank text.

CIPHER TEXT: A message that cannot be understood by any person or small group message is something we call Cipher content.

ENCRYPTION: The process of converting empty content into image content is called as encryption. This process requires two things - the number of encryption and a key. Calculation refers to the system used as part of encryption. Encryption occurs on the sender's side.

DECRYPTION: The decryption process goes back to encryption. In this process Cipher Content is converted to Empty Content. The recording process requires two items - a fixed number and a key. Counting means the method used as part of Decryption.

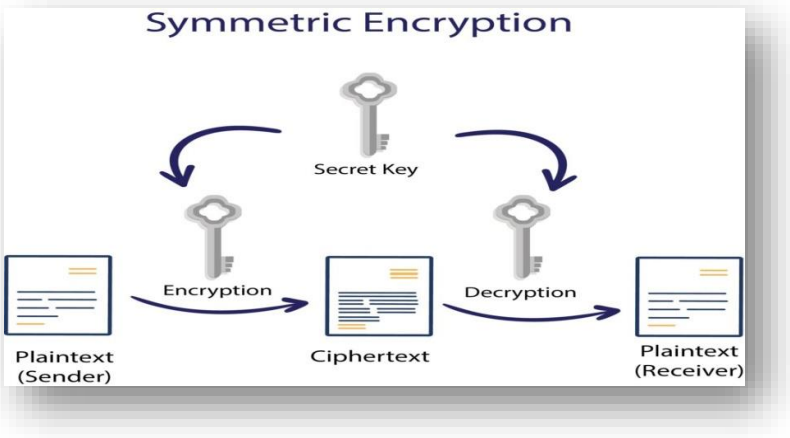


3. TYPES OF CRYPTOGRAPHY

Cryptography can be divided into three distinct categories:

1. Secret Key Cryptography
2. Public Key Cryptography
3. Hash Functions

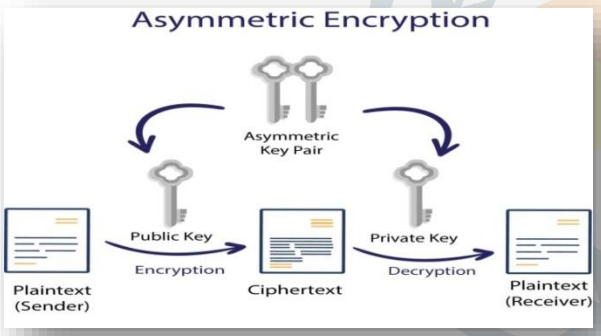
SECRET KEY CRYPTOGRAPHY: Encryption key cryptography is used to encrypt an empty text message using a series of bits called a secret key. It usually uses the same key to understand the corresponding encryption message and to get the first empty text because both encryption and deleting data encryption are accessed with the same key; the secret key is often called the symmetric key.



EXAMPLE

AES
DES
Caesar cipher

PUBLIC KEY CRYPTOGRAPHY: Public key encryption, or public key cryptography, is a way to encrypt data with two different keys and make one key, public key, available for anyone to use. Another key is known as the secret key. Public encrypted data can only be cleared of private encryption, and encrypted data can be cleared of public encryption.



Examples:

ECC:

The ECC works by focusing on certain pairs of public and private keys to encrypt and decrypt web traffic encryption.

There are other encryption methods available such as Diffie-Hellman and RSA scripts. These methods are based on the construction of keys that use large numbers that include a lot of compound strength.

ECC cryptography is a key-based method that uses a public key encryption method to encrypt data based on elliptic curve view. With the application of elliptic curve theory, faster, smaller, more efficient cryptographic keys are created.

With elliptical curve encryption, complex and mathematically complex keys are produced by the elements of the elliptic curve equation in the transformation of the conventional method as a product of large numbers. The elliptic curve cryptosystem technology can be used simultaneously with multiple public key encryption methods, including RSA and Diffie-Hellman. Various studies and studies suggest that ECC systems can achieve the same level of security with a 164-bit key if other strategies require a 1,024-bit key. This is because the elliptic curve system supports the creation of a security equivalent to a small computer power supply and reduced battery usage due to its widespread use in various mobile applications.

Daffier-Hellman:

The Daffier-Hellman algorithm is used to create a shared secret that can be used for private communication while exchanging data on a social network using an elliptic curve to generate points and obtain private key using restrictions.

To facilitate the practical application of the algorithm, we will consider only 4 variables, the main one being P and G (the original P-source) and the two secret values a and b.

P and G are both numbers that are publicly available. Users (say Alice and Bob) choose secret numbers a and b and generate a key and exchange it publicly. The hacker gets the key and produces the secret key, after which they have the same secret encryption key.

DSS:

Digital Signature is a method of verifying the authenticity and integrity of a message or digital or electronic document. Authentication means checking whether the data comes from a valid source or not to the recipient i.e. verifying the sender's identity and integrity means checking whether the data or message should not be changed during the transfer.

DSS or Digital Signature Standard was introduced by the National Institute of Standards and Technology (NIST) in 1994. It has become the standard for the United States government for electronic document certification. Federal Information Processing Standard (FIPS) 186 specifies DSS. It was first proposed in 1991 and revised in 1993 due to public concerns about the safety of the system. DSS uses SHA (Secure Hash Algorithm) to create digital signatures and provides a new digital signature method known as the Digital Signature Algorithm.

HASH FUNCTION: Hash functions are mathematical functions that convert or "map" a specific set of data into a small unit of fixed size, also known as "hash value.

4. SERVICES OF CRYPTOGRAPHY

Following are the features of cryptography:

4.1. **Confidentiality:** If information is read or copied by an unauthorized person, the result is a loss of privacy. Data is kept confidential for those who do not have the right pieces, even if that data passes through an unsafe area.

4.2. **Integrity:** Integrity means that the data or information in your system is stored so that it cannot be edited or deleted by unauthorized organizations. To maintain data integrity, easy ways to make a backup copy of your data, using access controls, monitor your testing and encryption.

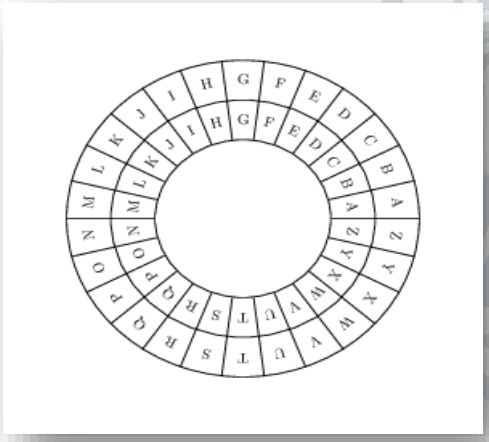
4.3. Non-repudiation: Rejection is an asset acquired through encryption that prevents a person or business from disclosing certain actions related to the data (such as the means of refusal or authority origin); for evidence of obligation, purpose, or commitment; or for proof of ownership.**4. Authentication:** Cryptography can help to identify you for authentication purposes. Proof of identity. (The main ways to prove the authenticity of an online host today are based on a name or based on an address, both of which are notoriously weak.)

5. HISTORICAL ALGORITHMS

In this section we will learn about cryptographic algorithms that were designed and used long before the public key for encryption was used.

CAESAR CIPHER

This cipher instead, known as Caesar cipher, is probably the most historical cipher most mentioned in textbooks. Caesar Cipher also known as substitution techniques. In cipher instead, each letter of a blank text (blank text is a message to be encrypted) instead of another letter to create a cipher text (cipher text is a hidden message). One of Caesar's uses was a 3cipher switch. Each letter has been replaced by 3 letters, so the letter 'A' has been replaced by 'D','B' has been replaced by 'E', and so on. The characters will eventually collapse, so 'X' will be replaced by 'A'.



SIMPLE SUBSTITUTION METHOD

Simple Substitution Ciphers Take the Simple Substitutions Cipher, also known as the Mono alphabetic Cipher, for example. In the cipher Substitution Cipher, we take the letters of the alphabet and place them in random order under well-written letters, as shown here.

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

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

The encryption rule here is that “each letter is replaced by a lower case letter” and the code rule may be the opposite. FOR EXAMPLE, the corresponding ciphertext for the blank text TULAS says UYGMI.

TRANSPOSITION METHOD

Conversion can be defined as the transformation of characters into a blank text using rules and specific keys. The columnar transposition cipher can be considered as one of the simplest forms of transposition cipher and has two forms: the first is called "complete column conversion", and the second is "incomplete column". Regardless of the form used, the rectangular shape is used to represent the blank text horizontally, and its width should correspond to the length of the key used. There can be as many lines as needed to write a message. When full column conversion is used, blank text is written, and all blank columns are filled in blank so that each column is the same length. for example

s e c o n

di v i s o

n a d v a n

ci n g t o

ni g h t x

The cipher text is then taken from the columns depending on the key. In this example, if we use the key “321654”, the cipher text will be:

cvdngeiaiisdncndonoxnsattoivgh

However, when it comes to incomplete column change for the column, the columns do not need to be filled in, so blank letters are left out. This causes columns of varying lengths, which can make the cipher text much harder to define without keys

DIGITAL SIGNATURE

Unlike cryptography, digital signatures did not exist before the invention of computers. With the introduction of electronic communications, there was a need to negotiate digital signatures, especially in the business environment where multiple organizations take place and each one should be committed to keeping their announcements and / or suggestions. The theme of the memorable signatures was first discussed hundreds of years ago, with the exception of those that were handwritten signatures. The concept of digital signing was first introduced in a paper by Daffier and Hellman entitled "New Guidelines for Cryptography".

DIGITAL SIGNATURE REQUIREMENT

The relationship that generates the link between the signature and the encryption emerged during the “digitalization” we now see and live on. Requirements for a memorable signature system will be:

• Each user must have the ability to create their own signature. In any selected document of their choice.

• Each user must have the ability to successfully verify whether the given series or not is another user's signature.

• No one should be able to produce signatures on documents that the original owner did not sign.

FUTURE SCOPE

Many researchers, industrial laboratories and governments are actively working to develop a quantum computer that can handle large-scale calculations such as the work at the Q station. Three critical emerging areas of privacy and encryption:

- Confidential computing, and
- Quantum-safe cryptography

Confidential computing: Confidential computing helps in performing in-memory data encryption without exposing the cloud data to the entire system.

There are currently several approaches to protecting data at rest and in transit, where protecting sensitive data in use is a confidential computation.

Quantum-safe cryptography: Quantum safe cryptographyidentifies algorithms that secure information from attacks from both classical and quantum computers, so that information is safe even after a large commercial quantum computer is built.

Quantum safe cryptography is used for:

1. It protects the communication between military and government.
2. Soothing the confidentiality of medical data and healthcare records.
3. Restricting access to confidential corporate networks.
4. Security of personal data storage in the cloud.
5. Protects the transactions records of banking and finance.

6. CONCLUSION

Cryptography plays a vital and important role in achieving the main objectives of security principles, such as security, integrity, confidentiality, and non-compliance. Cryptographic algorithms are being developed to achieve these goals. Cryptography aims to provide a reliable, robust, and secure data security network. In this paper, we have reviewed some of the research that has been done in the field of cryptography and how the various algorithms used in encryption for different security purposes have worked. Cryptography will continue to emerge through IT and business plans regarding the protection of personal, financial, medical, and ecommerce data as well as providing a decent level of privacy.

REFERENCES:

1. (PDF) A Review Paper on Cryptography (researchgate.net)
2. Cryptography : Different Types, Tools and its Applications (elprocus.com)
3. (PDF) A Review Paper on Cryptography (researchgate.net)
4. Paper2883.pdf (ijarsct.co.in)
5. acstv10n5_10.pdf (ripublication.com)
6. Secret Key Cryptography: A Beginner's Guide In 4 Easy Points (jigsawacademy.com)
7. https://www.researchgate.net/publication/334418542_A_Review_Paper_on_Cryptography
8. https://www.jigsawacademy.com/blogs/cyber-security/elliptic-curve-cryptography/sssss