Secure Communication Using Cryptology

Veena M [1]
Sneha C D [2]

[1] UG Student, KLE S.Nijalinagappa College, Bengaluru.
[2] UG Student, KLE S.Nijalinagappa College, Bengaluru.

ABSTRACT

Cryptography is a concept to protect data transmission over wired or wireless network. Data Security [1-2] is the main aspect of secure data transmission over insecure network. Network security involves the authorization of access to data in a network, which is controlled by authorized users only. Network security covers a variety of computer networks that are used for conducting transactions, communications among businesses, government agencies, etc. In this paper we study cryptography along with its few types. The types of cryptographic models along with examples are outlined.

Keywords: Encryption, Decryption, Cipher, OTP

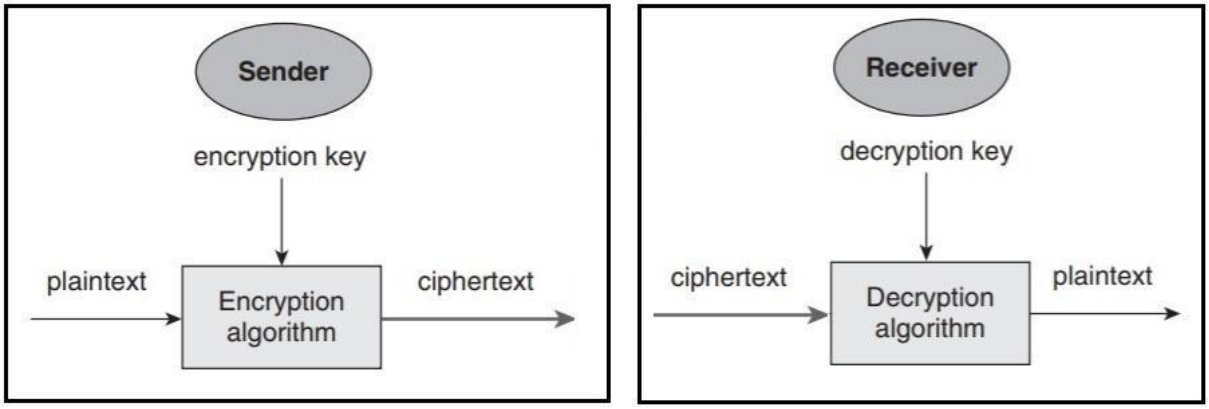
1. Introduction to Cryptography

Cryptography [3] is a method of protecting information and communications through the use of codes so that only those for whom the information is intended can read and process it.

The word “crypt” means “hidden” or “vault” and “graphy” stands for “writing”. It refers to secure information and communication techniques derived from mathematical concepts and a set of rules based on calculations called algorithms to transform messages in ways that are hard to decipher. These deterministic algorithms are used for cryptographic key generation [4] and digital signing and verification to protect data privacy, web browsing on the internet and confidential communications such as credit card transactions and email. It provides a suite of basic mechanisms for implementing the security services that protect electronic information, such as confidentiality, data integrity and authentication. It doesn’t secure information on its own, but many technical mechanisms for protecting information have cryptography at their core.

Cryptology means making and breaking of “secret codes” i.e., a set of information to transferred from one end to another end **or** Cryptography is form of making of “secret codes” which has to transmit to the receiver end **or** Cryptanalysis is a breaking of “secret codes” that has been transformed in the bandwidth through a channel for a purposeful mechanism.

Cipher is system used to encrypt data from the sender end for a protection purpose.



The process of data transmission is of the form as follows,

Plain Text: Message

Key: To encrypt the plain text.

Cipher Text: Message after encryption or secret codes.

Encryption: Converting of readable text to unreadable characters.

Decryption: Converting of unreadable characters to readable text.

2. Types of Cipher

Simple Substitution Cipher [6]

Encryption: The message is encrypted by substituting the letter of the alphabet "n" places ahead of the current letter.

Key: value of "n".

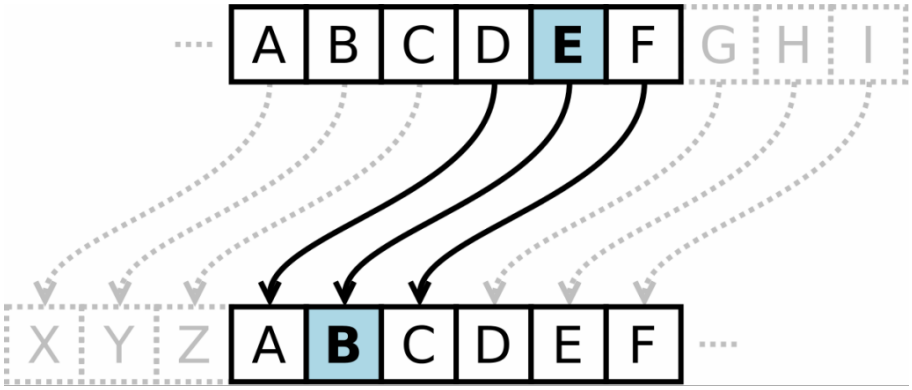
Decryption: The cipher text is decrypted to plain text by substituting each alphabet in the cipher text by "n" places behind the current letter.

Example

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

Key :n="3".

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



Using key n=”3” we can encrypt the following plain text as follows

“twothousandone”

For the given plain text cipher text can be obtained by simply substituting the corresponding letter in the cipher text that is 3 places ahead of it in the alphabet.

“**XASXMSYWDRHSRI**”

To decrypt this simple substitution we can shift each cipher text letter backward by “3”.

The simple substitution with a shift of 3 is known as the “CAESAR’S CIPHER”.

Double Transposition Cipher

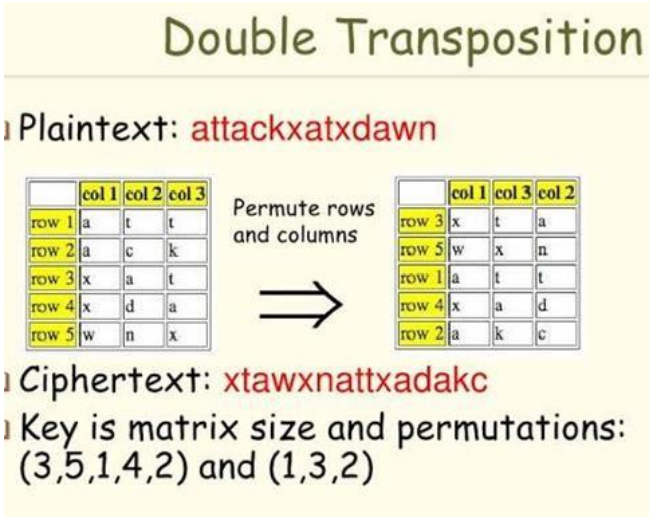
Encryption: Given plain text is represented by a matrix of order,

m*n matrix format.

Permute the rows and columns according to a specified permutations.

Keys: Consists of Size of matrix and the rows and column permutations.

Decryption: Put the cipher text into the appropriate sized matrix and undo the permutations to recover the plain text.



Example: Suppose if we write the plain text "klesncollege" in order of 3*4 arrays:

$$\begin{pmatrix} K & l & e & s \\ n & c & o & l \\ l & e & g & e \end{pmatrix}$$

Now if we transpose the rows according to **(1,2,3)->(3,2,1)** and transpose the columns according to **(1,2,3,4)->(4,2,1,3).**

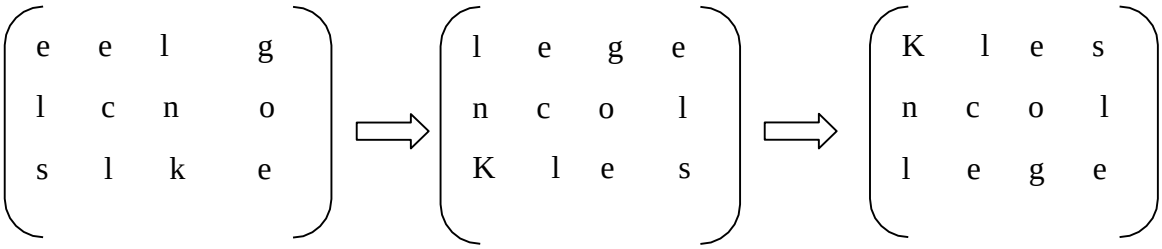
We obtain

$$\begin{pmatrix} K & l & e & s \\ n & c & o & l \\ l & e & g & e \end{pmatrix} \Rightarrow \begin{pmatrix} l & e & g & e \\ n & c & o & l \\ K & l & e & s \end{pmatrix} \Rightarrow \begin{pmatrix} e & e & l & g \\ l & c & n & o \\ s & l & k & e \end{pmatrix}$$

The cipher text is then read from the final array:

"EELGLCNOSLKE"

To decrypt the cipher text is first put into a 3*4 array. Then the columns are numbered as (4,2,1,3) and rearranged to (1,2,3,4) and the rows are numbered as(3,2,1) and rearranged into (1,2,3).



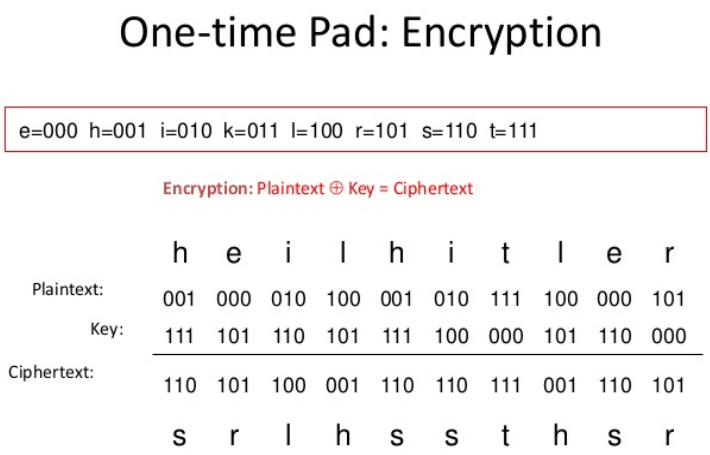
<u>One Time Pad</u>

Encryption: Convert the plain text letters into a bit string.

The key is then XORed with the plain text to yield the cipher text.

Key: The one-time pad key consists of a randomly selected string of bits that is the same length as the message.

Decryption: Accomplished by XOR-ing the same key with the cipher text.



Abbreviated alphabet:

Letter	**C**	**R**	**y**	**P**	**T**	**o**	**b**	**v**
Binary	**000**	**001**	**010**	**011**	**100**	**101**	**110**	**111**

Example: Suppose that John who recently got a job as a spy,wants to use a one-time pad to encrypt the plain text message.

“crypto”

Convert the plain text letter into the bit string

“000 001 010 011 100 101”

Now suppose that John has the key

“111 101 110 101 111 000”

Then to encrypt,John computes the cipher text as

c r y p t o

Plain text: 000 001 010 011 100 101

Key: 111 101 110 101 111 000

Cipher text:111 100 100 110 011 101

v t t b p o

When his fellow spy,Bob receives John’s message,he decrypts it using the same shared key and there by recovers the plain text:

v t t b p o

Cipher text:111 100 100 110 011 101

Key: 111 101 110 101 111 000

Plain text: 000 001 010 011 100 101

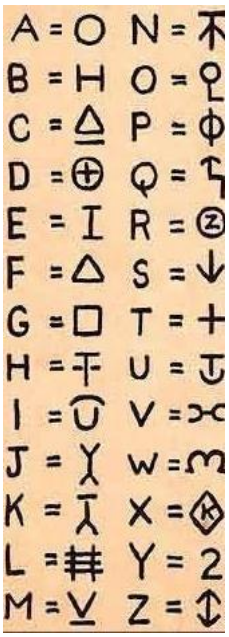
c r y p t o

Codebook Cipher

Encryption:To encrypt a given word a cipher clerk would simply look up the word in the codebook and replace it with the corresponding codeword.

Key:Comprosises of codeword in the Codebook.

Decryption:Using the inverse Codebook.



Example:

Plaintext	Ciphertext
Febraury	13605
Fest	13732
Forbidden	13850
Flower	13918

The above examples are based on symmetric key encryption [5] scheme, that is the algorithm uses only one key for encryption as well as decryption. There is another scheme of encryption which uses two keys and it is known as asymmetric key encryption scheme, this uses a public key and private key for encryption and decryption respectively.

Advantages of Cryptography

- Secure data transmission
- Simple to implement encryption process

Disadvantages of Cryptography

- Decryption process of certain multiple algorithms takes more time.
- Sharing single key between nodes in symmetric key scheme is not secure (Brute Force Attack).

3. Conclusion

Cryptography is a widely used process in daily life w.r.t multiple fields for maintaining the data secrecy, which includes the integrity of the data along with the confidentiality. At the same time this process might use more time in decrypting process and the efficiency of the system will be decreased. Finally, it can be said that this process has the same amount of disadvantage as advantage.

4. References

[1] DENNING, D., and DENNING, P.J.: 'Data security', *ACM Comput. Surveys*, 1979, 11, pp. 227-250

[2] A Role-Based Trusted Network Provides Pervasive Security and Compliance - interview with Jayshree Ullal, senior VP of Cisco.

[3] Coron, J. S. , " What is cryptography?", *IEEE Security & Privacy Journal, 12(8), 2006, p. 70-73.*

[4]DIFFIE, W., and HELLMAN, M.: 'New directions in cryptography', *IEEE Trans.*, 1976, **IT-22,** pp. 644-654

[5] SIMMONS, G.J.: 'Symmetric and asymmetric encryption', *ACM Comput. Surveys*, 1979, **11,** pp. 305-330

[6] Algorithms: http://www.cryptographyworld.com/algo.htm