**Definition**:

Cryptography is a science of encryption/decryption. It is used to secure data in transmission internet or radio frequencies. It is also sometimes used for confidential data storage. Cryptanalysis is another important term in cryptology world. It is focused on how to decrypt and obtain original data from cyphered text. It is not necessary to find algorithm of encryption or key for decryption.

**History of cryptography:**

Cryptography is used to secure data from Egyptian ages. In ancient times Egyptians used nonstandard hieroglyphs while inscribing clay tablets (Mattord, p. 351).In 1518, Johannes Trithemius invented steganographic cipher. During world war 2, Alan Turing and the allied secretly broke the Enigma cipher , which helped to shortening war (Mattord, p. 353).

Cypher Methods:

It can be divided into two types: the bit stream method and block cipher method. In bit steam method, at one time only 1 bit is transformed into cipher bit from the plain text. But in block cipher method, first message is divided into blocks of different size, and then each block is converted into ciphered block using an algorithm and a key. Bit stream method uses different algorithm functions like XOR. Block method uses transposition, substitution, XOR or sometimes combination of these methods.

Cryptographic algorithm

Cryptographic algorithms are divided into two major groups. Symmetric and Asymmetric, based on the types of key they use for encryption and decryption. But sometimes hybrid mechanism is also use to utilize best feature of both methods.

Symmetric encryption:

In this method, same key is used for both encryption and decryption. This is also called as private key encryption method. Mathematical operations are used to encrypt data using private key. When sender wants to send any data to receiver, he/she encrypts data using common private key which shared by both sender and receiver. Receiver will decrypt this data using same private key. There is one loophole in this method that if someone else knows private key, then he can intercept that data and decrypt it without being tracked by sender or receiver. So, protection of key is more important in this method. Key transfer from sender to receiver should be secure so no one else can know that key.

Most commonly used symmetric key algorithms are DES, AES, 3DES, etc. Symmetric-key encryption can use either stream ciphers or block ciphers. Stream ciphers encrypt the digits (typically bytes) of a message one at a time. Block ciphers take a number of bits and encrypt

them as a single unit, padding the plaintext so that it is a multiple of the block size. Blocks of 64 bits have been commonly used (Rejani . R, 2015).

**Substitution**

The substitution cipher is a simple process to encode plaintext. It replaces each character with ciphertext. Ciphertext may be made of alphabets, numbers or symbols. At receiver side , by performing inverse substitution , original text can be recovered.

Plain alphabet : abcdefghijklmnopqrstuvwxyz

Cipher alphabet : badcfehgjilknmporqtsvuxwzy

Plain text : Cryptography is must

Cipher text: Dqosphqbogz jt nvts

**Transposition**

In transposition method , instead of replacing characters with other characters or symbols, location of character is changed. For example , “Hello” is plaintext and “elloH” is ciphered text where each character is shifted by 1 place. Replacing can also be done on blocks of characters. Here, key determines how different characters will be shifted to different location. So by doing reverse engineering at receiver side using key, original plain text can be obtained. There are many transposition cipher methods used for security.

Key In a transposition cipher, the key is a mapping between the position of the symbols

in the plaintext and cipher text.

Types of transposition cipher:

1. Rail Fence cipher
2. Route cipher
3. Columnar Transposition
4. Double Transposition
5. Myszkowski Transposition
6. Disrupted Transposition
7. Grilles
8. Scytale

**Rail Fence Cipher**

In rail-fence cipher, plaintext is written downwards across successive ‘rails’ of an imaginary ‘fence’. For example, the plaintext ‘UNCW CSIS PROGRAM’ can be written as a three-rail cipher:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| RAIL 1 | U | W | I | R | R |
| RAIL 2 | N | C | S | O | A |
| RAIL 3 | C | S | P | G | M |

Steps for ciphering plain text:

1. Write characters in vertical manner from top to bottom in each column
2. Read characters along the rail from left to right

For above example, ciphered text is “UWIRRNCSOACSPGM”.

To decipher, put characters into as many groups as rails. And read from top to bottom in each column.

**Route Cipher**

In Route Cipher, key decides how to follow route while reading ciphertext from block created with plaintext.

Steps for ciphering plain text:

1. Decide number of rows or number of columns of grid
2. Write plain text characters into grid
3. Read characters as per route defined as key

For example, plain text is “When nothing is going right go left”. Number of columns is 5.\

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| W | H | E | N | N |
| N | O | T | H | I |
| N | G | N | I | S |
| N | G | O | I | N |
| G | N | R | I | G |
| H | T | N | G | O |
| N | L | E | F | T |

We can also add nulls to replace space. With a route of reading columns top to bottom, ciphertext will be : “WNNNGHNHOGGNTLETNORNENHIIIGFNISNGOT”. If route is spiraling inward clockwise from the bottom left, ciphertext will be: “NHGNNNWHENNISNGOTFELTNGGOTHIIIGNRON”. An historical use of Route Cipher was the Union Route Cipher used by the Union forces during the American Civil War. Rather than transposing letters by the given route, it moved whole words around.(Rodriguez-Clark, n.d.)

**Column transposition**

It is also known as a row-column transpose. We can perform it by hand.

Steps:

1. Decide key length
2. Write data to be encrypted in column as shown in example
3. Rearrange column in ascending order
4. Note down encoded message from column in top to bottom

In Below example, key length is 6. And key is 362145. Input data is “THIS IS MOST SECRET MESSAGE DO NOT TRY TO DECODE IT”. And Encoded message is "STTGTDIISEAOOETMCSOYTISMETETSEEDRCDHORSNTD".

|  |  |  |
| --- | --- | --- |
| Columns | Unencoded | Encoded |
| 3 6 2 1 4 5  T H I S I S  M O S T S E  C R E T M E  S S A G E D  O N O T T R  Y T O D E C  O D E I T | 1 2 3 4 5 6  S I T I S H  T S M S E O  T E C M E R  G A S E D S  T O O T R N  D O Y E C T  I E O T D |

# Bibliography

Akins, T. (n.d.). */tools/cipher/coltrans.php*. Retrieved from Column Transposition: http://rumkin.com/tools/cipher/coltrans.php

Edition, B. A.-4. (n.d.). *Data Communications and Networking.* McGrawHill.

Gurpreet Singh, S. (April 2013). A Study of Encryption Algorithm (RDA, DES, 3DES and AES) for Information Security. *International Journal of Computera Application (0975 - 8887)*.

Mattord, M. E. (n.d.). *Principles of Information Security 4th ed.*

Rejani . R, D. V. (2015). Study of Symmetric key Cryptography Algorithms. *International Journal of Computer Techniques - Volume 2 Issue 2, Mar - Apr 2015.*

Bibliography

Akins, T. (n.d.). */tools/cipher/coltrans.php*. Retrieved from Column Transposition: http://rumkin.com/tools/cipher/coltrans.php

Edition, B. A.-4. (n.d.). *Data Communications and Networking.* McGrawHill.

Gurpreet Singh, S. (April 2013). A Study of Encryption Algorithm (RDA, DES, 3DES and AES) for Information Security. *International Journal of Computera Application (0975 - 8887)*.

Mattord, M. E. (n.d.). *Principles of Information Security 4th ed.*

Rejani . R, D. V. (2015). Study of Symmetric key Cryptography Algorithms. *International Journal of Computer Techniques - Volume 2 Issue 2, Mar - Apr 2015.*