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).

Symmetric algorithm
DES
AES
3DES

1.DES

DES is one of the most widely accepted, publicly available cryptographic systems. It was developed by IBM in the 1970s but was later adopted by the National Institute of Standards and Technology (NIST), as Federal Information Processing Standard 46 (FIPS PUB 46). The Data Encryption Standard (DES) is a block Cipher which is designed to encrypt and decrypt blocks of data consisting of 64 bits by using a 64-bit key [10, 15]. Although the input key for DES is 64 bits long, the actual key used by DES is only 56 bits in length. The least significant (right-most) bit in each byte is a parity bit, and should be set so that there are always an odd number of 1s in every byte. These parity bits are ignored, so only the seven most significant bits of each byte are used, resulting in a key length of 56 bits. The algorithm goes through 16 iterations that interlace blocks of plaintext with values obtained from the key. The algorithm transforms 64-bit input in a series of steps into a 64-bit output. The same steps, with the same key are used for decryption. There are many attacks and methods recorded till now those exploit the weaknesses of DES, which made it an insecure block cipher. Despite the growing concerns about its vulnerability, DES is still widely used by financial services and other industries worldwide to protect sensitive on-line applications [3, 16]. The flow of DES Encryption algorithm is shown in Figure 3. The algorithm processes with an initial permutation, sixteen rounds block cipher and a final permutation (i.e. reverse initial permutation).

3DES

3DES or the Triple Data Encryption Algorithm (TDEA) was developed to address the obvious flaws in DES without designing a whole new cryptosystem. Data Encryption Standard (DES) uses a 56-bit key and is not deemed sufficient to encrypt sensitive data. 3-DES simply extends the key size of DES by applying the algorithm three times in succession with three different keys. The combined key size is thus 168 bits (3 times 56). TDEA involves using three 64-bit DEA keys (K1, K2, K3) in Encrypt-Decrypt- Encrypt (EDE) mode, that is, the plain text is encrypted with K1, then decrypted with K2, and then encrypted again with K3 [17]. The standards define three keying options:
Option 1, the preferred option, employs three mutually independent keys (K1 ≠ K2 ≠ K3 ≠ K1). It gives keyspace of 3 × 56 = 168 bits. Option 2 employs two mutually independent keys and a third key that is the same as the first key (K1 ≠ K2 and K3 = K1). This gives keyspace of 2 × 56= 112 bits. Option 3 is a key bundle of three identical keys (K1 = K2 = K3). This option is equivalent to DES Algorithm. In 3-DES the 3-times iteration is applied to increase the encryption level and average time. It is a known fact that 3DES is slower than other block cipher methods [11, 18].

AES

AES is the new encryption standard recommended by NIST to replace DES in 2001. AES algorithm can support any combination of data (128 bits) and key length of 128, 192, and 256 bits. The algorithm is referred to as AES-128, AES-192, or AES-256, depending on the key length. During encryptiondecryption process, AES system goes through 10 rounds for I28-bit keys, 12 rounds for I92-bit keys, and 14 rounds for 256-bit keys in order to deliver final cipher-text or to retrieve the original plain-text [19]. AES allows a 128 bit data length that can be divided into four basic operational blocks. These blocks are treated as array of bytes and organized as a matrix of the order of 4×4 that is called the state. For both encryption and decryption, the cipher begins with an AddRoundKey stage. However, before reaching the final round, this output goes though nine main rounds, during each of those rounds four transformations are performed; 1) Sub-bytes, 2) Shiftrows, 3) Mix-columns, 4) Add round Key. In the final (10th) round, there is no Mix-column transformation [3, 20]. Figure 4 shows the overall process. Decryption is the reverse process of encryption and using inverse functions: Inverse Substitute Bytes, Inverse Shift Rows and Inverse Mix Columns. Each round of AES is governed by the following transformations [10]: 3.4.1 Substitute Byte transformation AES contains 128 bit data block, which means each of the data blocks has 16 bytes. In sub-byte transformation, each byte (8-bit) of a data block is transformed into another block using an 8-bit substitution box which is known as Rijndael Sbox. 3.4.2 Shift Rows transformation It is a simple byte transposition, the bytes in the last three rows of the state, depending upon the row location, are cyclically shifted. For 2nd row, 1 byte circular left shift is performed. For the 3rd and 4th row 2-byte and 3-byte left circular left shifts are performed respectively. 3.4.3 Mixcolumns transformation This round is equivalent to a matrix multiplication of each Column of the states. A fix matrix is multiplied to each column vector. In this operation the bytes are taken as polynomials rather than numbers. 3.4.4 Addroundkey transformation It is a bitwise XOR between the 128 bits of present state and 128 bits of the round key. This transformation is its own inverse.

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 FO NOT TRY TO DECODE IT”. And Encoded message is "STTGTDIISEAOOETMCSOYTISMETETSEEDRCDHORSNTD". (Akins, n.d.)

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