CRYPTOGRAPHY – SURVEY OF TRANSPOSITION CIPHER METHODS

Dhaval Chauhan

MIS534 – Information Security Management

ABSTRACT

With the introduction of new smart objects and internet handy devices, security is considered as biggest concern for privacy and efficient use of technology. Cryptography is a wide term used from long time to secure data which is transmitted from one device or person to other. It uses different method to encrypt messages. At the same time overhead and computation complexity to do encryption is also considered. There are two types of cryptography used. Symmetric and Asymmetric. Various algorithms like AES, DES, 3DES provides excellent encryption compared to other methods. But at the same time AES algorithm takes more time to encrypt and decrypt data. So in this paper Transposition cypher method is discussed. Each algorithm has some advantages and disadvantages. This paper does not cover detailed study on encryption algorithms, but it is survey and understanding of basic transposition cipher methods.

1. INTRODUCTION

Cryptography is a science of encryption/decryption. It is used to secure data in which is transmitted over 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 know algorithm of encryption or key while decryption process. History of Cryptography is having roots in Egyptian ages when symbols were used to secure data. In ancient times Egyptians used nonstandard hieroglyphs while inscribing clay tablets (Mattord, p. 351). In 1518, Johannes Trithemius invented steganography cipher. During world war 2, Alan Turing and the allied secretly broke the Enigma cipher , which helped to shortening war (Mattord, p. 353). Components involved in cryptography is shown in Figure 1.1.

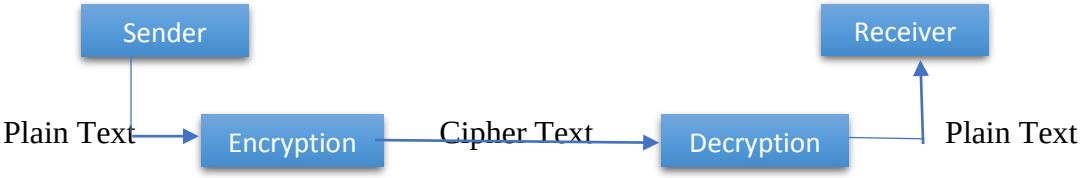

Figure 1.1

Plain Text and Cipher Text

It is the original message before encryption. After encryption, it becomes Cipher Text. Encryption algorithm encrypts original message into cipher text. In this paper various algorithms are discussed with example.

Cipher

Encryption and decryption algorithms are called as Cipher. This is not required to be unique. Same algorithm can be used by many entities involved in secure communication.

Key

Key is a unique number or combination of numbers and characters. Same key is required for encryption and decryption. But for some other methods like asymmetric, different key is required by sender and receiver. Key length may vary based on algorithm used.

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.

2. 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).

3. ASYMMETRIC ENCRYPTION

This is also called public key cryptography. In contrast to symmetric encryption, this algorithm requires two separate keys. One key is *secret* key and other is *public* key. But this two keys are linked mathematically. Here public key is used to encrypt data and secret key is used to decrypt data. For example, if person A wants to send some message to person B. A will use public key of person B for encryption. This public key can be obtained from some key management database. When person B receives data from person A, B will decrypt it with secret key to get original message. This secret key is not shared by person B. Only person B knows this key. So if any intruder or third person receives encrypted message sent by person A. He cannot decrypt it without secret key. This solution is more secure than symmetric encryption. But there is only one disadvantage of using this method is, if more than 2 person or 2 systems are involved in communication, it becomes hard to manage keys or different receivers. For example, for 2 persons, 4 different keys need to be used for successful communication.

4. TRADITIONAL CIPHERS

This ciphers are part of symmetric encryption method. This cipher is character-oriented. It can be divided into two major categories: Substitution ciphers and Transposition cipher. The substitution cipher is a simple process to encode plaintext. It replaces each character with cipher text. Cipher text 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

In above example, cipher alphabets depend on plain alphabet. Each pair of alphabet is switched. So “AB” becomes “BA”, “CD” becomes “DC”. At receiver side, by performing opposite process original text can be obtained.

5. 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

5.1 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.

5.2 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.)

5.3 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".

Step 1 & 2:

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	

Step 3 & 4:

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	

5.4 DOUBLE TRANSPOSITION

A columnar transposition is less secure. Because if attacker determines column length by observing multiple encrypted messages, He can try different anagrams. So to enhance security, columnar transposition can be applied twice. Different or same key can be used for both iterations. This approach makes double transposition algorithm much stronger than the previous transposition method. During World War 2, Allies and the Axis, both used this algorithm. And it was a success for both. But there is one loop hole in this method. If attacker intercepts two different messages having same length, by trying multiple anagrams this message can be decoded. But it is time consuming and tedious process. By this decoding method, keys also can be recovered.

As mentioned above, two different or same key can be used. Steps to follow for encryption are:

1. Pick a key or set of characters
2. Write message under its rows
3. Number the letters in alphabetical order
4. Read the cipher back by column
5. Pick a second key or set of characters
6. Follow the same steps from 2 to 4.

Example:

Plain Text: LETS GO FOR SKYDIVING AFTER MIS PRESENTATION

Key 1: DHAVAL

Key 2: CHAUHAN

Step 1 & 2: Use key “DHAVAL” and write down a message below its rows

D	H	A	V	A	L
L	E	T	S	G	O
F	O	R	S	K	Y
D	I	V	I	N	G
A	F	T	E	R	M
I	S	P	R	E	S
E	N	T	S	T	I
O	N				

Step 3: Number the letters in alphabetical order

3	4	1	6	2	5
D	H	A	V	A	L
L	E	T	S	G	O
F	O	R	S	K	Y
D	I	V	I	N	G
A	F	T	E	R	M
I	S	P	R	E	S
E	N	T	S	T	I
O	N				

Step 4: Read the cipher back by column. Reading will start from lowest number column.

Cipher Text: ATRVTPT AGKNRET DLFDAIEO HEOIFSNN LOYGMSI VSSIERS

Step 5: Pick a 2nd key and follow the same procedure mentioned in steps 2 and 3.

3	4	1	7	5	2	6
C	H	A	U	H	A	N
A	T	R	V	T	P	T
A	G	K	N	R	E	T
D	L	F	D	A	I	W
O	H	E	O	I	F	S
N	N	L	O	G	M	S
I	V	S	S	I	E	R
S						

After reading it again from column, cipher text will be:

ARKFELS APEIFME CAADONIS HTGLHNV HTRAIGI NTTWSSR UVNDOOS

6. CONCLUSION

This paper explains various transposition method for symmetric encryption. The paper addresses how substitution and transposition methods are different from conventional AES, DES and 3DES algorithms. After studying and exploring all methods with example, I found that these transposition algorithms lacks some stronger encryption. Because transposition keeps the occurrences of individual characters of plain text unchanged. By testing with proper anagrams encrypted message can be broken into original message after number of iteration. Jumbled characters in encrypted text can be searched in dictionary to find closer words. So technically, it is not fully secure. At the time of world war, this method was useful. But now with the help of faster computers anagrams search and test is faster. For future work combination of multiple methods can be tested against time to decrypt message with the help of faster computers.

References

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

Edition, Behrouz A. Forouzan. 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)*.

Inc., T. A. (2012). Rail-fence cipher.

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

Prashant Kumar Arya, D. M. (n.d.). Comparative Study of Asymmetric Key Cryptographic Algorithms. *International Journal of Computer Science & Communication Networks*.

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

Rodriguez-Clark, D. (n.d.). *Route Cipher*. Retrieved from Crypto Corner: http://crypto.interactive-maths.com/route-cipher.html