Encryption Protocol using some Pieces of Message as Key

Somchai Prakancharoen
Department of Computer and Information Science Faculty of Applied Science
King Mongkut's University of Technology North Bangkok
1518 Pracharaj 1st road Bangsue Bangkok Thailand 10800.
spk@kmutnb.ac.th

Abstract---This paper presents a simple message encryption protocol. Mono alphabetic substitution was used in encryption while key was gotten from the original plain text by choosing particular characters which located in different assigned positions. The cipher text were composed of unchanged key part and encrypted part. In decryption, receiver has to pick up a key from received cipher text then performs message decryption by this key. This protocol was evaluated by three proficient in security field and point that this protocol could provide enough confidence in message sending and ease of use.

Keywords- encryption protocol; mono alphabetic; piece of key

I. INTRODUCTION

Message encryption is essential in security circumstance especially in critical consequence business such as finance, military, business strategy and even through individual personnel's information. Nowadays, message encryption is an importance activity to protect information security of each one from intruders. In typical basic encryption, sender has to send a defined conventional key to receiver then receiver should use it to decrypt received cipher text to gain plain text later. Key exchange between twos is weakness point. It might be attacked by anonymous intruders. This paper presents a simple security encryption protocol by mono alphabetic substitution algorithm which increase difficulty in key attack. This key, alphabets, were deliberately selected from original plain. Scrambling of plain text technique was used to increase confuse in encryption. The remain plain texts were encrypted with this key. The cipher text should be composed of cipher text and chosen key- alphabet, unchanged. Receiver has to calculate for key- alphabet position then pick them up. This key-alphabets was used to decrypt the other cipher texts then the order range of wholes decrypt message were reorder back to the prior range order to gain the original plain text. This designed protocol was assessed by three security task proficient for integrity, privacy- confidence and authentication of designed security protocol.

II. RELATED SECURITY ALGORITHM AND RESEARCH

A. Mono alphabetic substitution [1]

Mono alphabetic substitution is a technique to replace each plain text alphabet of entire plain text to new alphabet with a fixed substitution algorithm. There are many mono alphabetic substitution techniques such as Caesar, Atbash, Rot13 etc.

B. Position changing [2]

Permutation or transposition is a technique which is used to encrypt a character of any plain message to be cipher text which cipher text is still be the same character but be transposed to different position. There are many transposition techniques such as Affine cipher, Rail fence cipher, Route cipher, Columnar transposition, etc. Normally, input data of substitution technique is plain text. In other words, if the plain text character is a position, range order, of specific string then output of substitution should be new range order. The Affine – substitution technique could be used to perform string position changing. If "m" is the size of message then the position are 0, 1, 2…, m-1. Each character was transposed to new value with modular arithmetic equation (1)

$$E(x) = (ax + b) \bmod m \qquad (1)$$

While a, b are sender's defined number which were use as conventional key, in this designed protocol, "x" is a character of plain text but was denoted as a position, in this designed protocol. The value of m is assigned to be a size of string. "a" was sender's arbitrary defined constant which must be co-prime with "m". To decrypt the cipher text E(x), or position re order back, D(x) as (2) is used.

$$D(x) = a^{-1}(x - b) \bmod m \qquad (2)$$

While "a^{-1}" is multiplicative inverse modular of "*a mod m*".

C. Secret splitting [3]

If M is a secret message which was considered to be kept in secret. In message splitting algorithm, another defined message which has equal length to M, denoted as "R". M and R were exclusive .OR. (.XOR.) together to produce "S". In decryption, “M” could be called back by .XOR. R together with S.

D. Related research

Even though mono alphabetic substitution is a weak secrecy since it generated a little bit of possible events but it still benefit for some task which need not severe circumstance in case of being attacked as described in [4]. War department, USA, suggest choosing mono alphabetic substitution in some office operation tasks which were short lifetime of security awareness. [5] presented right security framework toward securing data and preserving reputation which coverage in information system risks management and keep information security in simple proactive, ease of use and likelihood of use.

E. Evaluation Security [6]

The key concepts to security theme are coverage in topics of confidentiality, integrity, accessibility, authenticity and non- repudiation. That is designed security protocol ought to be assessed in these items as much as possible.

III. PROTOCOL DESIGN

The designed protocol has described in detail step by step as follows.

A. Message preparation and Key choosing

- Step#1 Position reordering

Plain text amount of character was count to “m”. For example, “m” of plain text “ACTIS2012” was 9. This number was assigned to a modular size “m”.

TABLE I.. ORIGINAL PLAIN TEXT

Order of original plain text	0	1	2	3	4	5	6	7	8
Plain text	A	C	T	I	S	2	0	1	2

Affine cipher was used to re arrange the order of the prior order. Sender prepared “a”, “b” but not necessarily on “m”. Assume that a = +4, b= +2 and m = +9 then affine encryption was defined in (3). This plain message prior in range order 0th, 1st, 2nd,…8th was changed to new order range as 2nd, 6th, 1st, 5th, 0th, 4th, 8th, 3rd, 7th by Affine cipher algorithm.

$$E(x) = 4 * x + 2 \bmod 9 \tag{3}$$

After perform affine cipher, the new order of plain text was re arranged to new range.

TABLE II. PLAIN TEXT AND REORDERING POSITION

Order of original plain text	0	1	2	3	4	5	6	7	8
Plain text	A	C	T	I	S	2	0	1	2
New order	2	6	1	5	0	4	8	3	7

- Step#2 Prepare nonce-random number and key

After perform transposing each character to new order, sender has to prepare random number used once, R_{nonce}. R_{nonce} should be used to increase confusion and prevent intruder attack on keys surmise easily. Assume that R_{nonce} was denoted as “η”, given “11110000_2” as value of R_{nonce} in this paper. Next, sender chooses the piece of cipher text or some defined positions to be used as conventional key. Positions were mentioned with random number, ϕ_i, generating equation.

$$R_n = (c * R_{n-1} + d) \bmod m. \tag{4}$$

Assume that (4) arbitrary constants (c, d and R_{n-1}) was assigned by sender’s as equation.

$R_n = (4 * R_{n-1} – 3) \bmod 9$; c = 4, d = -3 and m = 9

While “4”, “-3” were assigned constants and “9” was modular m. If seed random number (Rn-1) equal to “2” then generated random numbers were 5, 8, 2, 5, 8 and so on. The amount of random number, “k”, must less than “m”. If “k” was assigned as quantity amount of 2 then transposed character number 5, 8 or character “2” (“00110010_2”) and “2” were chosen to be conventional key.

TABLE III. RE ORDERED POSITION PLAIN TEXT WHICH BE CHOSEN TO BE A CONVENTIONAL KEY

Order of original plain text	0	1	2	3	4	5	6	7	8
Plain text	A	C	T	I	S	2	0	1	2
New order	2	6	1	5	0	4	8	3	7
Re arranged plain text	T	0	C	2	A	S	2	I	1

B. Message encryption

Defined key from step#2 of A was used to encrypt the other remain characters, (“T”, “0”, “C”, “A”, “S”, “I” and “1”. Example of each character encryption, “T” was presented as equation follows.

$$E(“T”) = T \oplus \phi_1 \oplus \phi_2 \oplus \eta \tag{5}$$

It should be presented in detail equation as

$E(“T”) = 01010100_2 \oplus 00110010_2 \oplus 00110010_2 \oplus 11110000_2$ - - > 10100100_2 - - > “¤”

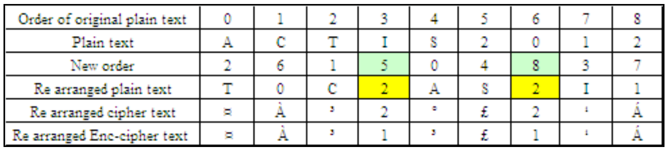
After complete perform encryption all the cipher texts were “¤À³2°£2¹Á” then sender sent it to receiver along with “a, “b”, “m”, R_{nonce} (- η), R_{n-1}, k, c and d which these part ought to be sent by difference channels and difference times as well in order to prevent attack on sending essential part, key involvement.

TABLE IV. RE ORDERED POSITION PLAIN TEXT WHICH BE CHOSEN TO BE A CONVENTIONAL KEY EXCEPT KEY TEXT

Order of original plain text	0	1	2	3	4	5	6	7	8
Plain text	A	C	T	I	S	2	0	1	2
New order	2	6	1	5	0	4	8	3	7
Re arranged plain text	T	0	C	2	A	S	2	I	1
Re arranged cipher text	¤	À	³	2	°	£	2	¹	Á

Unencrypted value ‘2’ and ‘2’ were also encrypted with Affine cipher equation (3). The cipher texts were changed to new value ‘1’ and ‘1’ as shown in table V..

TABLE V. RE ORDERED POSITION PLAIN TEXT WHICH BE CHOSEN TO BE A CONVENTIONAL KEY EXCEPT KEY TEXT WITH ENCRYPTED KEY



Order of original plain text	0	1	2	3	4	5	6	7	8
Plain text	A	C	T	I	S	2	0	1	2
New order	2	6	1	5	0	4	8	3	7
Re arranged plain text	T	0	C	2	A	S	2	I	1
Re arranged cipher text	¤	À	³	2	°	£	2	¹	Á
Re arranged Enc-cipher text	¤	À	³	1	³	£	1	¹	Á

C. *Message decryption*

Received cipher text should be performed decryption step by step as follows.

- Step#1 Seek for a key

Receiver gets cipher text which was composed of cipher characters and key characters (unchanged). Receiver could able to pick up key characters by perform random number generation and affine algorithm from equation as.

$R_n = (4 * R_{n-1} – 3) \bmod 9$; $R_{n-1}= 2$, $c = 4$, $d = -3$ and $m = 9$

Then $R_n = 5$ and $R_{n-1} = 8$

$E(x) = 4 * x + 2 \bmod 9$; $x =0, 1, 2,…8$

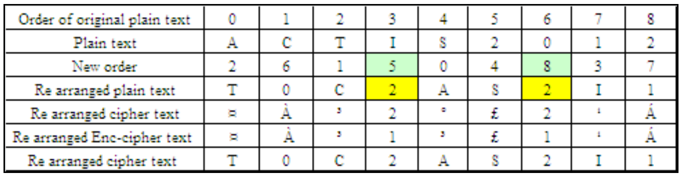
Then x = 2, 6, 1, <u>5</u>, 0, 4, <u>8</u>, 3, 7. When this sequence were compare to 0, 1, 2, <u>3</u>, 4, 5, <u>6</u>, 7, 8 then sender known that the positions of key in cipher text were 5th and 8th. In these positions, character “1” and “1” were gathered. These encrypted ciphers were decrypt with inverse of Affine equation (3); 4^{-1} (x-2) mod 9. The output plaint texts were then return to original value ‘2’, ‘2’.

- Step#2 Decrypt re arranged cipher text

To perform decryption, receiver has to pick up another cipher characters that were not located at position 3rd and 6th then decrypt them with equation (5). The remaining ciphers (except keys) were performed in the same solution.

$D(x)$ = “¤” $\oplus$ $00110010_2 \oplus 00110010_2 \oplus 11110000_2$ - - > 01010100_2 - - > “T”

TABLE VI. RE ORDERED POSITION PLAIN TEXT

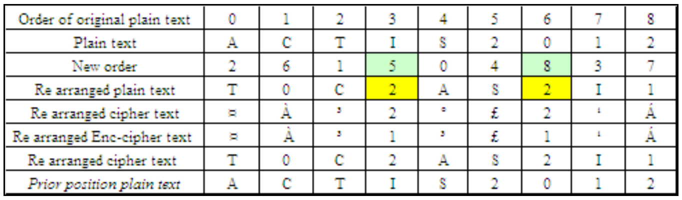


Order of original plain text	0	1	2	3	4	5	6	7	8
Plain text	A	C	T	I	S	2	0	1	2
New order	2	6	1	5	0	4	8	3	7
Re arranged plain text	T	0	C	2	A	S	2	I	1
Re arranged cipher text	¤	À	³	2	°	£	2	¹	Á
Re arranged Enc-cipher text	¤	À	³	1	³	£	1	¹	Á
Re arranged cipher text	T	0	C	2	A	S	2	I	1

- Step#3 Reorder back to the original plain text

When every reordered cipher text and key (not be changed) were finished step #2 performing then perform re ordering them back to their prior position by 2, 6, 1, <u>5</u>, 0, 4, <u>8</u>, 3, 7. Final, cipher texts were already called back to the original plain texts, as present in table VII.

TABLE VII. PLAIN EXT IN PRIOR POSITION



Order of original plain text	0	1	2	3	4	5	6	7	8
Plain text	A	C	T	I	S	2	0	1	2
New order	2	6	1	5	0	4	8	3	7
Re arranged plain text	T	0	C	2	A	S	2	I	1
Re arranged cipher text	¤	À	³	2	°	£	2	¹	Á
Re arranged Enc-cipher text	¤	À	³	1	³	£	1	¹	Á
Re arranged cipher text	T	0	C	2	A	S	2	I	1
Prior position plain text	A	C	T	I	S	2	0	1	2

D. *Protocol assessment*

The designed protocol was sent to three Information technology persons who responsible duty in security fields. Evaluation items were mentioned on secrecy which a five level Likert scale score. The average score were 3.9 and 0.35 standard deviation.

IV. CONCLUSION

Secrecy of designed protocol assessments was a little bit larger than average score (2.5). The objective of this protocol was to provide a simple encryption protocol therefore complexity of calculation should be avoided. Nevertheless, this protocol ignores about integrity and authentication awareness thus, in practical system implementation, hashing function and some authentication protocol might be included in order to guarantee message integrity and individuals authentications.

REFERENCES

[1] Avi Kak,“Classic encryption techniques”, Purdue university, USA, 2012.

[2] Christof Paar, “Applied cryptography and data security”, University of Bochuam, Germany, 2005.

[4] NSA, “Mono alphabetic substitution system”, USA, 1938.

[3] Bruce Schneier, “Applied Cryptography”, John Wiley & Sons, 1994.

[5] Gary Sheehan,“IMS risk management-Keep Information security simple”, Integrated management system, 2012.

[6] Easttom, C., "Computer Security Fundamentals (2nd Edition)" Pearson Press, 2011.