Stochastic Modeling and Applications
Vol.13, No. 2 , (2009)
ISSN: 0972-3641

SCOPE OF MULTIPLE ENCRYPTION SCHEMES IN CLASSICAL CRYPTOSYSTEM USING TERNARY CODES

D.K. LOHANI[1], S. AGARWAL[2#], A.S. UNIYAL[3]

ABSTRACT. After development of Public key cryptography the classical methods used for encryption and decryption have become obsolete. It is so because cryptologists did not search for any possible new area in the field of symmetric cryptosystem. Herein an idea of introducing ternary codes in secret key cryptosystem has been developed. In this symmetric encryption scheme there are limited exhaustible options for any intruder to search for the secret key even then it is quite difficult for him to get the success. An observation on possible difficulty for breaking one of such system has also been taken. In multiple encryption scheme using three different keys, a set of all combinations of characters including the plain text is obtained. It is not possible to identify the plain text whatever that may be, because all possible meaningful texts will also be included in the complete set of possible plaintexts. Hence the cryptosystem seems to be unbreakable.

An idea of introducing ternary codes in secret key cryptosystem has been developed in this paper. Suitable logical circuit can be designed easily to convert the ternary codes into binary codes so as to be useful for present computer system. In proposed symmetric encryption scheme there are limited exhaustible options for any intruder to search for the secret key but even then it is quite difficult to get the success. An observation on possible difficulties for breaking the system has also been taken for a particular such system.

1. Introduction

Basically the encryption is the method for converting the original message (plain text) into the disguised message (cipher text) to make it able to understand only by intended recipient. The method applied for removing the disguise to change cipher text into original plain text is termed as decryption.

Initially in symmetric cryptosystem, encryption and decryption was done using affine map, digraph (taking two characters together) and tri graph transformations besides application of matrices. Later various public key cryptosystems e.g. RSA (after the names of its inventers), system based on knapsack problems and elliptic curve cryptosystem respectively were developed. “While there are not many crypto-systems which empirically seem to earn the right to be called ‘Public Key’, there is no cryptosystem in existence which is provably public key”*[1].

[#] *Corresponding Author*

***Key words and phrases**: Public Key Cryptography; Cryptosystem; Secret Key; Encryption; Decryption*

Although the symmetric key cryptosystem is an oldest one, (in around 50 BC) used by Julius Caesar *[2] and (in 499 AD) used by Aryabhata *[3], it could not get due consideration of the cryptologists after development of public key cryptography (in 1976 AD) by Diffie *[4] and Hellman *[5].

The idea behind this newly proposed cryptosystem with very easy methods for encryption (as well as for decryption) is that there are limited options for any intruder to break the system. Even after applying all the available options if he does not succeed in his mission, the only option left is to sit aside. On the other hand in public key cryptosystem the intruder may continue to search for the private key with inexhaustible available options.

The new symmetric cryptosystem has been proposed here wherein every character (member of given alphabet, numerals, punctuations etc.) is broken into three parts (ternary codes) termed as elements; elements are processed through the well-defined encryption/decryption methods with elements of secret code and finally converted back into characters.

2. General Formulation

A binary operation Θ in a set S along with all the elements of the set is suitably defined to obey the following composition table as shown below.

Table -1 (Composition table)

Θ	α	β	γ
α	α	γ	β
β	γ	β	α
γ	β	α	γ

$$S = \{\alpha, \beta, \gamma\} \qquad \text{... (2.1)}$$

Where α, β and γ are the elements of the arbitrary set S chosen from the set of sets R as defined below,

Set R contains all the prime triplets $(P_\alpha, P_\beta, P_\gamma)$ where $P_\beta = (P_\alpha+2)$ and $P_\gamma = (2P_\alpha+1)$. [Example: Prime Triplet $(3,5,7) \in R$ as $5 = 3+2$, $7 = 2.3+1$. There exist infinitely many such prime triplets.]

Thus $R = [S_1,S_2,...S_i, ...] = [\{P_{\alpha_1}, P_{\beta_1}, P_{\gamma_1}\}, \{P_{\alpha_2}, P_{\beta_2}, P_{\gamma_2}\}, …. \{P_{\alpha_i}, P_{\beta_i}, P_{\gamma_i}\}, …..]$

[If we choose $S = S_i$ i.e. $\{\alpha, \beta, \gamma\} = \{P_{\alpha_i}, P_{\beta_i}, P_{\gamma_i}\}$, the face values of α, β and γ may be taken as P_{α_i}, P_{β_i} and P_{γ_i} respectively.]

Binary operation Θ on the set S may be defined as,

$$x\Theta y = n^{1/2\,[3-\mu(n)]} \pmod N \text{ and } 0 < (x\Theta y) < N;\ \forall\, x, y \in S \quad \text{...(2.2)}$$

where $N = (\gamma+1)$ for $\gamma \in S$, $n = x.y$ and $\mu(n)$ is well known Mobius Function *[6] for any positive integer n given by

$$\mu(n) = \begin{cases} 1 & \text{if } n = 1, \\ 0 & \text{if } p^2/n \text{ for some prime } p, \\ (-1)^n & \text{if } n = P_1.P_2.P_3.....P_r. \text{ Where } P_is \text{ are distinct primes.} \end{cases} \qquad ...(2.3)$$

3. Labeling of the Elements

α, β and γ are labeled as to obey the rule,

(Label of x) = (Face Value of x) mod α, where x = α, β or γ. ...(3.1)

Hence α, β and γ have been labeled as 0, 2 and 1 respectively. Label is numerical equivalent for elements and is used for labeling n digit integers on this base. Here α, β and γ are digits to represent any character or multiple (fractional with denominator 3 or whole) of any character called integer.

4. Properties of Algebraic Structure

Algebraic structure (S,Θ) satisfies the following axioms. These axioms may be used for Encryption, Decryption and Cryptanalysis. (set S and binary operation Θ have already been defined at (2.1) and (2.2) above respectively.)

(1) Closure Property: Set S is closed under the operation Θ i.e.

$$x\Theta y \in S \ \forall \ x,y \in S.$$

(2) Θ over the set S is commutative i.e.

$$x\Theta y = y\Theta x \text{ for every pair of elements } x, y \in S.$$

(3) Θ is not associative i.e.

$$(x\Theta y)\Theta z \neq x\Theta(y\Theta z) \ \forall \ x, y, z \in S.$$

(4) If x and y are unknown elements (variables) of set S then solutions of certain following equations are given by α, β, γ

(i) $x\Theta y = \alpha \Rightarrow (x,y) = (\alpha, \alpha), (\beta, \gamma)$ or (γ, β)

(ii) $x\Theta y = \beta \Rightarrow (x, y) = (\beta, \beta), (\alpha, \gamma)$ or (γ, α)

(iii) $x\Theta y = \gamma \Rightarrow (x, y) = (\gamma, \gamma), (\alpha, \beta)$ or (β, α)

(5) Left and Right cancellation laws hold good in S i.e.

$$z\Theta x = z\Theta y \Rightarrow x = y \text{ and } x\Theta z = y\Theta z \Rightarrow x = y, \ \forall \ x, y, z \in S.$$

(6) Repetition of operator with same element cancels the operation i.e.

$$(x\Theta y)\Theta y = x, \ \forall \ x, y \in S$$

Also, $(y\Theta x)\Theta y = x$ because $(y\Theta x) = (x\Theta y)$.

5. Encryption and Decryption

If p, c and k are corresponding elements of the plain-text, cipher-text and secret key respectively then using above properties of the algebraic structure (S, Θ) simple encryption and decryption can be processed as follow,

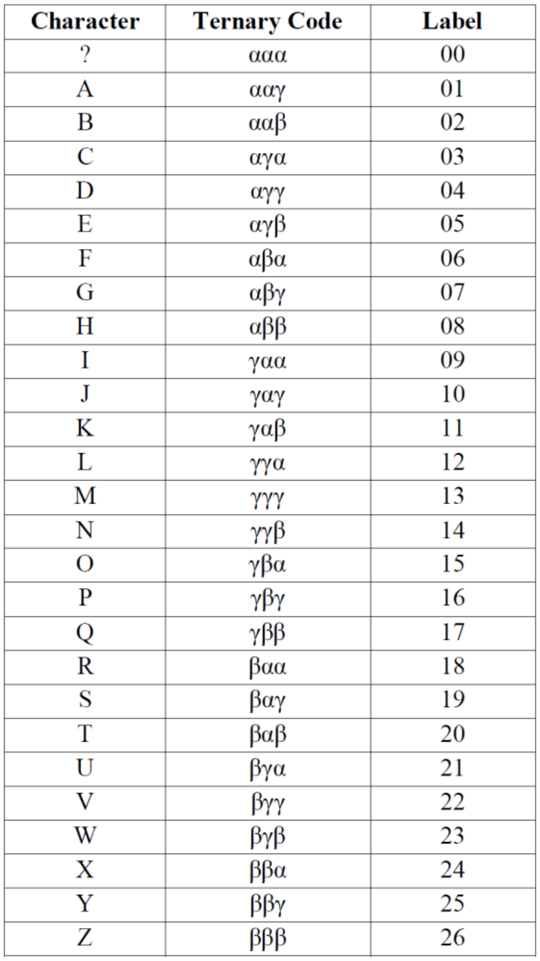
$$\left.\begin{array}{ll} \textbf{Encryption:} & p\Theta k = c \\ \textbf{Decryption:} & c\Theta k = p \end{array}\right\} \qquad ...(5.1)$$

6. “TYPE-I” Cryptosystem

All the information is made available publicly except the secret key. In this cryptosystem S is chosen as (5,7,11) i.e. face values of α, β and γ has been taken as 5, 7 and 11 respectively.

6.1. Coding System and Labeling of the Characters

Table -2



Character	Ternary Code	Label
?	ααα	00
A	ααγ	01
B	ααβ	02
C	αγα	03
D	αγγ	04
E	αγβ	05
F	αβα	06
G	αβγ	07
H	αββ	08
I	γαα	09
J	γαγ	10
K	γαβ	11
L	γγα	12
M	γγγ	13
N	γγβ	14
O	γβα	15
P	γβγ	16
Q	γββ	17
R	βαα	18
S	βαγ	19
T	βαβ	20
U	βγα	21
V	βγγ	22
W	βγβ	23
X	ββα	24
Y	ββγ	25
Z	βββ	26

Here in Table -2, characters are usually considered as integers consisting of a triplet of elements (as digits) e.g. S = βαγ implies that Label of S = $2.3^2 + 0.3^1 + 1.3^0 = 19$ (0, 1 and 2 being labels of α, β and γ respectively).

6.2. Secret Key

Secret key "K" is taken as a string of four characters say "ABCD". Obviously it is a chain of twelve elements (consisting α, β and γ) say "$\lambda_1\lambda_2\lambda_3\lambda_4\lambda_5\lambda_6\lambda_7\lambda_8\lambda_9\lambda_{10}\lambda_{11}\lambda_{12}$". How it is used in encryption and decryption process, is explained as below.

"λ_1": The first element of the chain indicates how the grouping of the characters is done in plain text (as well as in cipher text) from left. Complete text is divided into groups, each group consisting of number of characters equal to face value of λ_1. The last group may have remaining fewer elements.

"λ_2": The second element of the chain indicates how the elements of characters in a group are diffused with each other. If λ_2 is equal to α, then the end elements of successive characters are interchanged and first element of the first character of the chain in a group is also interchanged with last element of last character during encryption and decryption processes evenly. If λ_2 is equal to γ or β respectively then during encryption process one or two elements from the beginning of the chain is/are shifted to the end of the group; during decryption corresponding end elements (one or two) are shifted to the beginning of the chain in the group. These processes during encryption and decryption respectively may be termed as diffusion and restoration.

"$\lambda_3\lambda_4\lambda_5\lambda_6\lambda_7\lambda_8\lambda_9\lambda_{10}\lambda_{11}\lambda_{12}$": Group of remaining ten elements (termed as secret code) is used for direct operation with plain-text (or cipher-text) elements using Θ operator.

6.3. Encryption

Now let us encrypt the statement

"INDIAISMYCOUNTRY" ...(A)

Statement is also called plain-text.

Available well-defined 'Secret Key' is "PGRT" say. ...(B)

Encoding the characters of the secret key with the help of Table-2, we get chain of elements in 'Secret Key' as

PGRT ≈ "γβγ αβγ βαα βαβ" ...(C)

Comparing it with "$\lambda_1\lambda_2\lambda_3\lambda_4\lambda_5\lambda_6\lambda_7\lambda_8\lambda_9\lambda_{10}\lambda_{11}\lambda_{12}$" we get,

(i) "λ_1" = γ, which implies that, in given plaintext, grouping is to be done from left taking 11 characters.

Thus Grouped Plain-text is "INDIAISMYCOUNTRY" ...(D)

Coded plain-text groups are:

"γαα γγβ αγγ γαα ααγ γαα βαγ γγγ ββγ αγα γβα"

and "βγα γγβ βαβ βαα ββγ" ...(E)

(ii) "λ_2" = β, which implies that in each group two elements from the beginning are to be shifted to the end of the group. Thus diffused plain-text chains are:

“αγγ βαγ γγα ααα γγα αβα γγγ γββ γαγ αγβ αγα”
and “αγγ ββα ββα αββ γβγ” ...(F)

(iii) “$\lambda_3\lambda_4\lambda_5\lambda_6\lambda_7\lambda_8\lambda_9\lambda_{10}\lambda_{11}\lambda_{12}$” = “γαβγβααβαβ” (secret code)

Equivalent chains of secret code:

Repeating the secret code, a long chain of secret code is made and it is cut from left into pieces of same length as that of corresponding plain-text chains.

Thus obtained equivalent chains of secret codes are:

“γαβ γβα αβα βγα βγβ ααβ αβγ αβγ βαα βαβ γαβ”
and “γβα αβα βγα βγβ ααβ” ...(G)

Applying binary operation between corresponding elements, we get coded cipher-text groups as shown below.

(F)Θ(G):

“ββα αγβ βαα γβα αγγ αγγ βαγ ββα ααβ γββ ββγ”
and “βαβ γβα βαα γαβ βγα” ...(H)

Using Table -2, we get decoded grouped cipher-text as

“XERODDSXBQY TORKU” ...(J)

Standard cipher text thus obtained is

“XERODDSXBQYTORKU” ...(K)

This cipher text is ready for transmission to distant end intended recipient.

6.4. Decryption

Received cipher-text is “XERODDSXBOYTORKU”

Available well-defined ‘Secret Key’ is “PGRT” (known to intended recipient)

In reverse order of encryption, decryption process may be carried out Grouped cipher text can be obtained as (J) by grouping the cipher text as defined by “λ_1” = γ in secret key.

Hence we get coded cipher groups as,

“ββα αγβ βαα γβα αγγ αγγ βαγ ββα ααβ γββ ββγ”
and “βαβ γβα βαα γαβ βγα” ....(L)

Equivalent chains of secret code formed by last ten elements of secret key:

“γαβ γβα αβα βγα βγβ ααβ αβγ αβγ βαα βαβ γαβ”
and “γβα αβα βγα βγβ ααβ” ....(M)

Applying binary operation between corresponding elements, we get diffused plain text chains as available at (F) above i.e.

(L)Θ(M):

“αγγ βαγ γγα ααα γγα αβα γγγ γββ γαγ αγβ αγα”
and “αγγ ββα ββα αββ γβγ” ...(N)

Coded plaintext groups is obtained after restoring the diffusion by carrying last two elements in each group to the beginning of the group as defined by "λ_2" = β in secret key as,

"γαα γγβ αγγ γαα ααγ γαα βαγ γγγ ββγ αγα γβα"

and "βγα γγβ βαβ βαα ββγ" ...(P)

By decoding with the help of available Table -2, we get required plaintext as

"INDIAISMYCOUNTRY" ...(Q)

7. Multiple Encryption Scheme under TYPE-I Cryptosystem

7.1. Multiple Encryption Scheme with Three Keys

One of the simple forms of multiple encryptions *[1] has three encryption stages and three keys. Given a plaintext P, three secret keys K1, K2 and K3, cipher-text C is generated as,

$$C = E_{K3}\,[E_{K2}\,[E_{K1}\,[P]\,]\,] \qquad \text{…(R)}$$

Decryption requires that the keys be applied in reverse order. Thus plaintext is generated from the cipher-text as,

$$P = D_{K1}\,[D_{K2}\,[D_{K3}\,[P]\,]\,] \qquad \text{…(S)}$$

Initially string of characters is converted into the chain of elements with the help of Table -2 for plaintext as well as for secret keys. In all of the three stages these elements undergo through the process of successive encryption with the available keys K1, K2 and K3 respectively. Then finally obtained complete chain of elements is converted into a string of characters. Grouping these characters in same fashion as they were in plain text, we get the required cipher-text.

For deciphering the disguised text, the characters are converted into elements first then the process of successive decryption in three stages is done using the keys in reverse order i.e. K3 first then K2 and at last K1. Finally obtained elements are decoded into characters and desired grouping of characters, as it was in cipher-text, is done to get the required plaintext.

7.2. Observations

Let us consider that three secret keys are selected for multiple encryption. Although the keys may be defined in a numerous different ways but let us select the same type of keys as defined in above type-I simple secret cryptosystem. Thus there are 12 elements in each key.

No. of different ways available for selecting 1st secret key = 3^{12}

No. of different ways available for selecting 2nd secret key = 3^{12}

No. of different ways available for selecting 3rd secret key = 3^{12}

Total ways for selecting all the three secret keys simultaneous

$$\begin{aligned}&= 3^{12} \times 3^{12} \times 3^{12}\\ &= 3^{6} \times 3^{30}\\ &> 3^{6} \times 2 \times 10^{14} \qquad (\text{As } 3^{30} > 2 \times 10^{14})\end{aligned}$$

If 100 MB clock is used for selection of different ways, it selects @ 10^8 ways per second for deciphering the data.

Total time taken for selecting all the possible keys

$$> (3^6 x\ 2\ x\ 10^{14})/10^8 \text{ seconds}$$
$$> (1458\ x\ 10^6)/(3.156\ x\ 10^7) \text{ years}$$
$$> 46 \text{ years} \qquad (\text{As 1 year} < 3.156\ x\ 10^7 \text{ seconds})$$

Time for processing the elements at three stages and decoding into possible plaintext during decryption is extra, which is expected to be more than double of the time taken by the clock to select all set of keys. Thus total time required for deciphering the disguised message in all possible ways will be more than 3 x 46 = 138 years.

Moreover the use of all the keys shall provide a set of all combinations of characters including the plain text. Therefore it is not possible to identify the plain text whatever and wherever that may be, because all possible meaningful texts will also be included in the complete set of possible plaintexts. Hence the cryptosystem seems to be unbreakable.

8. Conclusion

We have discussed here very simple cryptosystems (One ordinary and other with multiple encryption schemes) even then it is quite strong. If we define different coding systems and use different type of secret keys and use suitable combination of these at appropriate stages, the system becomes stronger. Randomly selected prime i.e. face value of a may be used as a generator of secret key, which has not been explained here to avoid further expansion of topic.

Moreover if provision for compression of text, introducing various techniques to confuse the intruder and transmission of master key to the authorized recipient in the cipher text on the cost of compression, is made in the process of encryption, the system becomes strongest one. These elements of the set S may also be mapped easily as $\alpha \equiv 01$, $\beta \equiv 11$ and $\gamma \equiv 10$ with binary coding system where 01, 11 and 10 are merely different ordered pairs of binary digits 0 and 1 and do not possess any numerical values. Suitable logical circuit can be designed easily to enable these binary codes to follow the given composition Table -1. Possibility of introducing quinary codes in this field may also be explored.

References

1. N. Koblitz, A Course in Number Theory and Cryptography, 2nd ed., Springer Verlag (1994), pp.87, pp.54-65.
2. William Stallings, Cryptography and Network Security, 3rd ed., Pearson Education Singapore, reprint (2003), pp.24-102.

3. V. K. Sharma and Mustafizur Rahman, Applied Science Periodical, Vol.-II, No.-3, August (2000), pp.155-160.
4. W. Diffie and M. Hellman, Multi-user Cryptographic Techniques, IEEE Transaction on Information Theory, November (1976).
5. M. E. Hellman, The Mathematics of Public-key Cryptography, Scientific American 241 (1979), pp.146-157.
6. David M. Burton, Elementary Number Theory, 6th ed., The McGraw Hill Companies Inc. New York, Reprint (2006), pp. 112-116.

[1]**D.K. LOHANI**: RESEARCH SCHOLAR, DEPARTMENT OF MATHEMATICS, M.B. (GOVT.) P.G. COLLEGE, HALDWANI, INDIA

[2]**S. AGARWAL**: ASSISTANT PROFESSOR, DEPARTMENT OF MATHEMATICS, KCMT, BAREILLY, INDIA

[3]**A.S. UNIYAL**: ASSOCIATE PROFESSOR, DEPARTMENT OF MATHEMATICS, M.B. (GOVT.) P.G. COLLEGE, HALDWANI, INDIA