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

APPLICATION OF MARVELOUS TERNARY CODES IN CLASSICAL CRYPTOSYSTEM

S. AGARWAL[1#], A.S. UNIYAL[2]

ABSTRACT. In our article [1] we have introduced "Ternary Coding System" in the field of symmetric encryption under classical cryptography and developed the encryption & decryption method, in which 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. Here we proposed secret key cryptosystem using ternary codes (α, β, γ) and a binary operation (Θ) seems to be very hard to break as compare to the previous one but have very simple encryption and decryption processes.

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. The proposed cryptosystem may be considered as 1/3-graph. 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." [2*]

Although the symmetric key cryptosystem is an oldest one, (in around 50 BC) used by Julius Caesar [3] and (in 499 AD) used by Aryabhata [4], it could not get due consideration of the cryptologists after development of public key cryptography (in 1976 AD) by Diffie [5] and Hellman [6].

We propose herein a symmetric cryptosystem using correlated prime triplets as ternary codes and a well-defined binary operation Θ which is closed under the set of ternary codes (α, β, γ). Secret key is taken as a group of characters. Every character of given alphabet may be broken into three elements and each element is represented by any of the ternary codes. Clearly three codes a, Bandy can be arranged as a triplet of elements in different order by 3^3(=27) ways if repetition of elements is allowed, hence we can provide different triplets of codes for all the 26

[#]***Corresponding Author***
Key words and phrases*: Secret key; Chain of elements; String of characters; Ternary codes; Encryption; Decryption; Diffusion; Restoration.*

characters of English alphabet. 27th triplet is provided for sign '?'. "Repetition of binary operation with the same element cancels the operation." This property of the binary operation gives us an idea to design this new type of symmetric encryption scheme. The reason behind proposing such a cryptosystem under classical cryptography with very easy method of encryption (as well as decryption) is that there are limited exhaustible options to be applied by 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.

In this proposed cryptosystem, during encryption process each character of plain-text is initially broken into three elements. Thus the string of characters in plain-text is converted into the chain of elements. Further these elements are rearranged under certain fixed rules and operated with corresponding secret key elements using a binary operation to yield a new chain of elements. Triplets of successive elements of this new chain taken from left generate a unique string of characters which may be collected as cipher-text.

Similarly during decryption each character of cipher-text is broken into three elements. Further these elements are operated with secret key elements and then rearranged under the predefined rules. Thus a different chain of elements is obtained, triplets of successive elements of which, taken from left, provides us required plain-text as a string of characters. If cipher-text "EDFZQT" is obtained for the plain-text "DANGER" using some secret key, anyone may like to find the possible cipher-text corresponding to plain-text "GENDER" with the same key. The right answer is "EAXZKZ". Is it not surprising? This is an example of simple encryption using a single key. Obviously multiple encryption schemes with three keys shall give us more typical results.

2. General Formulation

Let us consider three elements α, β and γ termed as ternary codes or elements which are used as digits to represent any character (as three digit number) of the given alphabet.

Let $$S = \{\alpha, \beta, \gamma\} \quad ...(2.1)$$

Also the prime triplet $\{\alpha, \beta, \gamma\}$ is any arbitrary element of the set R containing all the prime triplets $(P_\alpha, P_\beta, P_\gamma)$ such that

$$P_\beta = (P_\alpha+2) \text{ and } P_\gamma = (2P_\alpha+1) \quad ...(2.2)$$

i.e., $$R = [\{P_{\alpha_1}, P_{\beta_1}, P_{\gamma_1}\}, \{P_{\alpha_2}, P_{\beta_2}, P_{\gamma_2}\}, \ldots. \{P_{\alpha_i}, P_{\beta_i}, P_{\gamma_i}\}, \ldots..] \quad ...(2.3)$$

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

$$x\Theta y = n^{1/2\,[3-\mu(n)]} \pmod N \text{ and } 0 < (x\Theta y) < N; \forall\, x, y \in S \quad ...(2.4)$$

where $$N = (\gamma+1) \text{ for } \gamma \in S, \quad ...(2.5)$$

$$n = x.y \quad ...(2.6)$$

and μ(n) is well known Mobius Function [7] for any positive integer n given by

$$\mu(n) = \begin{cases} 1 & \text{if } n = 1, \\ 0 & \text{if } p^2/n \text{ for some prime } p, \\ (-1)^n & \text{if } n = P_1.P_2.P_3.....P_r. \text{ Where } P_i\text{s are distinct primes.} \end{cases} \quad ...(2.7)$$

Relation between elements of the set S and N: From (2.2) & (2.5) we get

(i) $N = (\gamma+1) \Leftrightarrow \gamma = (N-1)$ ...(2.8)

(ii) $\gamma = (2\alpha+1) \Leftrightarrow \alpha = (\gamma-1)/2 \Leftrightarrow \alpha = (N/2-1)$ ...(2.9)

(iii) $\beta = (\alpha+2) = (N/2-1)+2 \Leftrightarrow \beta = (N/2+1)$ ...(2.10)

(iv) All of the ternary codes (α, β and γ) are odd primes therefore $(\alpha+1)$ is an even number $\Leftrightarrow 2/(\alpha+1) \Leftrightarrow 4/(2\alpha+2) \Leftrightarrow 4/([2\alpha+1]+1)$

$\Leftrightarrow 4/(\gamma+1) \Leftrightarrow 4/N \Leftrightarrow N/4$ is a whole number ...(2.11)

3. Properties of Algebraic Structure (S, Θ)

Case-I:

If $x \neq y$; $x,y \in S$; (2.4), (2.6) & (2.7) give

$x\Theta y = n^{1/2\,[3-\mu(n)]} \pmod N = xy \pmod N$ ...(3.1)

[as for n = x.y; x, y being different primes, $\mu(n) = 1$]

Now consider $A = [(xy-z)/N]$, $\forall$ x, y, z $\in$ S and $x \neq z \neq y$

For $z = \alpha$, we shall have $xy = \beta\gamma$ and

$A = [(\beta\gamma-\alpha)/N] = [\{(N/2+1)(N-1)-(N/2-1)\}/N] = (N/2)$, which is a whole number.

[using (2.8), (2.9), (2.10) and (2.11)]

Similarly for $z = \beta$ or $z = \gamma$ respectively we get

$A = [(\alpha\gamma-\beta)/N] = [\{(N/2-1)(N-1)-(N/2+1)\}/N] = (N/2-2)$, which is a whole number or $A = [(\alpha\beta-\gamma)/N] = [\{(N/2-1)(N/2+1)-(N-1)\}/N] = (N/4-1)$, which is also a whole number.

Thus $[(xy-z)/N]$ is always a whole number $\Leftrightarrow xy \pmod N \equiv z$ ...(3.2)

Case-II:

If x = y, $\forall$ x $\in$ S; (2.4), (2.6) & (2.7) give

$x\Theta x = n^{1/2\,[3-\mu(n)]} \pmod N = x^3 \pmod N$ ...(3.3)

[as for $n = x^2$; x being prime, $\mu(n) = 0$]

Again considering $B = [(x^2-1)/N]$, $\forall$ x $\in$ S, let us find B for $x = \alpha$, $x = \beta$ and $x = \gamma$ respectively.

Placing α, β and γ in terms of N from (2.9), (2.10) & (2.8) respectively and using (2.11) we get

$B = [(\alpha^2-1)/N] = [\{(N/2-1)^2-1\}/N] = (N/4-1)$, which is a whole number

$B = [(\beta^2-1)/N] = [\{(N/2+1)^2-1\}/N] = (N/4+1)$, which is a whole number and

$B = [(\gamma^2-1)/N] = [\{(N-1)^2-1\}/N] = (N-2)$, which is also a whole number.

Thus,
$[(x^2-1)/N]$ is always a whole number $\Leftrightarrow x^2 (\text{mod } N) \equiv 1 \Leftrightarrow x^3 (\text{mod } N) \equiv x$ ...(3.4)

Combining (3.1) & (3.2) together and (3.3) & (3.4) together we get respectively
for $x \neq y$, $x\Theta y = z$ such that $x \neq z \neq y$, $\forall$ x, y, z $\in$ S ...(3.5)
and for $x = y$, $x\Theta y = x\Theta x$ and $x\Theta x = x$, $\forall$ x $\in$ S ...(3.6)

Hence we can construct the following composition table shown below.

Table -1 (Composition table)

Θ	**α**	**β**	**γ**
α	α	γ	β
β	γ	β	α
γ	β	α	γ

Clearly for $x \neq y$

$(x\Theta y) = z$ and $(z\Theta y) = x$ ...(3.7)
also $(y\Theta y) = y$ and $(y\Theta y) = y$ ...(3.8)

This property of the binary operation has been used to design the proposed symmetric encryption scheme under classical cryptographic system. In (3.7) if we take x as an element of plain-text and y as element of the secret key then the resultant z will be corresponding cipher text element. Again operating z with the same key element y, we can get back the original plain text element x.

4. Encryption and Decryption

If p, c and k are corresponding elements of the plain-text, cipher-text and secret key respectively then using the properties of the algebraic structure (S, Θ) given at (3.7) and (3.8), simple encryption and decryption processes can be expressed as follow,

Encryption: $p\Theta k = c$
Decryption: $c\Theta k = p$ } ...(4.1)

5. Coding System for Characters

The coding system has been defined for different characters of English alphabets in Table -2.

Table -2

Character	Ternary Code	Character	Ternary Code
?	ααα	N	γγβ
A	ααγ	O	γβα
B	ααβ	P	γβγ
C	αγα	Q	γββ
D	αγγ	R	βαα
E	αγβ	S	βαγ
F	αβα	T	βαβ
G	αβγ	U	βγα
H	αββ	V	βγγ
I	γαα	W	βγβ
J	γαγ	X	ββα
K	γαβ	Y	ββγ
L	γγα	Z	βββ
M	γγγ		

6. Simple Example of Symmetric Encryption Scheme Using Ternary Codes

(i) Plain-text [p] = WORK ⇒ β γ β γ β α β α α γ α β

(ii) Binary Operation ⇒ Θ Θ Θ Θ Θ Θ Θ Θ Θ Θ Θ Θ

(iii) Secret Key [k] = TEMP ⇒ β α β α γ β γ γ γ γ β γ

(iv) [pΘk] ⇒ β β β β α γ α β β γ γ α ⇔ ZSHL = Cipher text [c]

(v) Θ Θ Θ Θ Θ Θ Θ Θ Θ Θ Θ Θ ⇐ Binary Operation

(vi) β α β α γ β γ γ γ γ β γ ⇐ TEMP = Secret Key [k]

(vii) Plain-text [p] = WORK ⇒ β γ β γ β α β α α γ α β ⇔ [cΘk]

Here steps (i) to (iv) show the encryption process while (iv) to (vii) show the decryption.

7. A Motivating Example of Symmetric Cryptosystem Using One Key Only

All the information is made available publicly except the secret key. Coding and decoding of the characters is done as per given Table -2. These characters are usually considered as integers consisting of a triplet of elements as digits.

7.1. Secret Key

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

7.2. How to use the Secret Key

Let us define two parameters μ_c & μ_e derived from the secret key and determines the action to be taken on the basis of their values.

$\mu_c = \lambda_1\Theta\lambda_2\Theta\lambda_3\Theta\lambda_4\Theta\lambda_5\Theta\lambda_6\Theta\lambda_7\Theta\lambda_8\Theta\lambda_9\Theta\lambda_{10}\Theta\lambda_{11}\Theta\lambda_{12}$ ...(7.2)-A

$\mu_e = \lambda_{12}\Theta\lambda_{11}\Theta\lambda_{10}\Theta\lambda_9\Theta\lambda_8\Theta\lambda_7\Theta\lambda_6\Theta\lambda_5\Theta\lambda_4\Theta\lambda_3\Theta\lambda_2\Theta\lambda_1$ ...(7.2)-B

Encryption process can be completed passing through the following steps:

7.2.1. If $\mu_c = \alpha$

7.2.1.(a). First divide the plain text into equal groups of four characters from left; last group may contain remaining characters that may be less than four.

7.2.1.(b). Then the end characters of successive groups in the plaintext are interchanged and first character of the first group is also interchanged with the last character of the last group.

7.2.2. If $\mu_c = \gamma$ or $\mu_c = \beta$ respectively

7.2.2.(a). First one or two characters from the beginning of the plain-text is/are placed after last character of the plain-text.

7.2.2. (b). Then the resultant text is divided into equal groups of four characters from left, last group may have one, two, three or four characters.

7.2.3. The characters are coded into elements using the Table -2 to get the coded plain-text groups.

7.2.4.(a). If $\mu_e = \alpha$, 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.

7.2.4.(b). $\mu_e = \gamma$ or $\mu_e = \beta$ respectively then within a group one or two elements from the beginning of the chain is/are placed after the last element of the chain.

[Process carried out at step (7.2.4) may be termed as diffusion. Its reverse process traversed during decryption may be termed as restoration.]

7.2.5. Now diffused plain text elements in each group are operated one by one with the corresponding secret key elements "$\lambda_1\lambda_2\lambda_3\lambda_4\lambda_5\lambda_6\lambda_7\lambda_8\lambda_9\lambda_{10}\lambda_{11}\lambda_{12}$" using Θ operator.

7.2.6. Chain of elements thus obtained is decoded into a string of characters which is required cipher text message.

7.3. Encryption

Now let us encrypt the given statement (also called plain-text).

"DANGER" ...(7.3.1)

Available well-defined 'Secret Key' is "PGRT" say. ...(7.3.2)

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

PGRT ≈ "γβγ αβγ βαα βαβ" ...(7.3.3)

This chain may be compared with "$\lambda_1\lambda_2\lambda_3\lambda_4\lambda_5\lambda_6\lambda_7\lambda_8\lambda_9\lambda_{10}\lambda_{11}\lambda_{12}$".

Now let us find the parameters μ_c & μ_e for the given secret key as defined under (7.2)-A and (7.2)-B respectively.

$\mu_c = \gamma\Theta\beta\Theta\gamma\Theta\alpha\Theta\beta\Theta\gamma\Theta\beta\Theta\alpha\Theta\alpha\Theta\beta\Theta\alpha\Theta\beta = \alpha$ and

$\mu_e = \beta\Theta\alpha\Theta\beta\Theta\alpha\Theta\alpha\Theta\beta\Theta\gamma\Theta\beta\Theta\alpha\Theta\gamma\Theta\beta\Theta\gamma = \alpha$ ...(7.3.4)

As here is μ_c equal to α, step [7.2.1] is applied.

(a) Dividing the plain text into equal groups of four characters from left we get,

DANG ER ...(7.3.5)

(b) Interchanging the end characters of successive groups and also interchanging the first character of the first group with the last character of the last group we get,

RANE GD …(7.3.6)

Encoding the characters into elements using Table -2 we get the coded plain-text groups as

βαα ααγ γγβ αγβ and αβγ αγγ ...(7.3.7)

Also here μ_e is equal to α, step [7.2.4.(a)] is applied. Interchanging the end elements of successive characters and also interchanging the first element of the first character with last element of last character in all groups we get the diffused plain-text chains as

βαα ααγ γγα βγβ γβα γγα …(7.3.8)

Repeating secret key elements given at (7.3.3) so as to match its length with the diffused plain text chain we get

γβγ αβγ βαα βαβ γβγ αβγ …(7.3.9)

Applying binary operation Θ between corresponding elements of (7.3.8) and (7.3.9) we get coded cipher-text groups as

αγβ αγγ αβα βββ γββ βαβ ...(7.3.10)

In other words (7.3.8) Θ (7.3.9) = (7.3.10)

Decoding these groups with the help of Table -2, we get the cipher-text groups as

EDFZ QT ...(7.3.11)

Combining these cipher text groups together, required cipher text is obtained as

"EDEZOT" ...(7.3.12)

Which is ready for transmission to distant end intended recipient.

7.4. Decryption

Traversing the reverse path of encryption, decryption process may be carried out.

8. Multiple Encryption Scheme with Three Keys-General Discussion

One of the simple forms of multiple encryptions [2**] has three encryption stages and three keys. Given a plaintext P, three secret keys K1, K2 and K3, cipher-text C is generated as

$$C = E_{K3} [E_{K2} [E_{K1} [P]]] \quad ...(8.1)$$

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

$$P = D_{K1} [D_{K2} [D_{K3} [C]]] \quad ...(8.2)$$

Initially strings of chance of plaintext as well as that of secret keys are converted into the separate chains of elements with the help of Table -2. 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 the finally obtained complete chain of elements is converted into a string of characters, which is 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 thus the required plaintext message is obtained.

If three secret keys, each consisting of four characters, are chosen for multiple encryption scheme then there will be 12 elements corresponding to each key. In this case let us calculate the minimum time required by any intruder to exhaust all possible ways to find the secret keys.

Thus the total ways for selecting all the three secret keys simultaneously

$$= 3^{12} \times 3^{12} \times 3^{12}$$
$$> 3^6 \times 2 \times 10^{14}$$

If 100 MBPS clock is used for selection of different possible keys, it can select @ 10^8 keys per second. Hence total time taken for selecting all the possible keys will be greater than $(3^6 \times 2 \times 10^{14})/10^8$ seconds which is more than 46 years [as 1 year < 3.156×10^7 seconds & $(1458 \times 10^6)/(3.156 \times 10^7) > 46$].

Time for determining the parameters μ_c & μ_e, rearranging the elements, processing the elements with binary operation at three stages and decoding into possible plaintext during decryption, is extra, which is expected to be more than four times 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 with 100 MBPS clock will be more than 5 x 46 years = 230 years. Hence the proposed cryptosystem seems to be unbreakable.

9. 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 triplet from set R may be used to generate three different secret keys.

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 circuits can be designed easily to convert the ternary codes into binary codes (and vice versa) and also to operate the elements under the well-defined binary operation so as to be useful for present computer system.

References

1. D.K. Lohani, S. Agarwal and A.S. Uniyal, Scope of Multiple Encryption Schemes in Classical Cryptosystem using Ternary Codes, Stochastic Modeling & Application, Vol. 13, No. 2, (2009), pp. 1-9.
2. N. Koblitz, A Course in Number Theory and Cryptography, 2nd ed., Springer Verlag (1994), pp.87*, pp.54-65**.
3. William Stallings, Cryptography and Network Security, 3rd ed., Pearson Education Singapore, reprint (2003), pp.24-102.
4. V. K. Sharma and Mustafizur Rahman, Applied Science Periodical, Vol.-II, No.-3, August (2000), pp.155-160.
5. W. Diffie and M. Hellman, Multi-user Cryptographic Techniques, IEEE Transaction on Information Theory, November (1976).
6. M. E. Hellman, The Mathematics of Public-key Cryptography, Scientific American 241 (1979), pp.146-157.
7. David M. Burton, Elementary Number Theory, 6th ed., The McGraw Hill Companies Inc. New York, Reprint (2006), pp. 112-116.

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

EMAIL: meshubhamagarwal@gmail.com

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

EMAIL: asuniyal0111@gmail.com