Polynumeric cipher for encryption and decryption

Santhosh Kumar B.J [#1]

[1]Department of Computer Science
[1]Amrita Vishwa Vidyapeetham University
Mysuru Campus, Karnataka, India
[1]santhoshbj50@gmail.com

Abstract— Polynumeric cipher uses numbers for encryption. S-DES is used for initial permutation for key generation mechanism. Its weakness is the key repetition. To overcome this weakness there are many research going on to modify the key generation. In this paper a key generator function is implemented which address the same. It generates a key with length depends on the message security level Length of the plain text is equal to length of the key. Sender and receiver generate key exchange mechanism for resulting common secret key. This common secret key is further processed for encrypting numbers using poly numeric table.

Keyword- S_DES- Simplified Data encryption standard,IP- initial permutation, Plain text, Cipher text, key generation.

I. Introduction

The poly numeric cipher is a method of encrypting numbers by using a series of different Caesar ciphers based on the numbers of a keyword. There is a symmetric key generation mechanism for keyword. Caesar ciphers are text based. It is a simple form of polynumeric substitution cipher. The poly numeric cipher uses a 10×10 table with 0 to 9 as the row heading and column heading. This table is usually referred to as the Vigenere Table. The first row of this table has the 10 numbers. Starting with the second row, each row has the numbers shifted to the left one position in a cyclic way.

II. *Proposed System*

The two schemes that are associated with the application are:

(i) Symmetric key generation mechanism.
(ii) Encryption and decryption.

This paper proposes an encryption and decryption of numbers and key generation. The application makes use of permutations and substitution for key generation. Generated key used for encrypting numbers of any length. Encryption process makes use of numeric vigenere table. The numeric vigenère cipher uses a 10×10 table with 0 to 9 numbers.

III.Methodology

A. symmetric key generation mechanism

Both users share a global public element P10 table(permutation table).In this case plain text input is 10 numbers. If plain text is six digits the P6 table has to be shared. Since key is symmetric same procedure is applied by the receiver.

The application makes use of S-DES(Simplified Data encryption standard permutation step for key generation mechanism.

P10(permutation of ten numbers)

3	5	2	7	4	0	1	9	8	6

Input sequence is:

0	1	2	3	4	5	6	7	8	9

Apply P10(permutation of ten numbers)

Input	0	1	2	3	4	5	6	7	8	9
P10	7	0	2	9	4	3	5	6	8	1

Input is a sequence of numbers from 0-9.P10 sequence is applied to input. Input is XOR with P10 to get a key. Bitwise XOR operation is performed on numbers. If the XOR result is more than 9 then:-

Result= Result mod 9

51 ⊕ 57 =10 i.e 10 mod 9=1

0 ⊕ 7=> ASCII(0) ⊕ ASCII(7) = 48 ⊕ 55=7

1 ⊕ 0=> ASCII(1) ⊕ ASCII(0) = 49 ⊕ 48=1

2 ⊕ 2=> ASCII(2) ⊕ ASCII(2) = 50 ⊕ 50=0

3 ⊕ 9=> ASCII(3) ⊕ ASCII(9) = 51 ⊕ 57=1

4 ⊕ 9=> ASCII(4) ⊕ ASCII(4) = 52 ⊕ 52=0

5 ⊕ 9=> ASCII(5) ⊕ ASCII(3) = 53 ⊕ 51=6

6 ⊕ 9=> ASCII(6) ⊕ ASCII(5) = 54 ⊕ 53=3

7 ⊕ 9=> ASCII(7) ⊕ ASCII(6) = 55 ⊕ 54=1

8 ⊕ 9=> ASCII(8) ⊕ ASCII(8) = 56 ⊕ 56=0

9 ⊕ 9=> ASCII(9) ⊕ ASCII(1) = 57 ⊕ 49=8

Final key generation

Input	0	1	2	3	4	5	6	7	8	9
P10	7	0	2	9	4	3	5	6	8	1
Key=(Input)⊕P10	7	1	0	1	0	6	3	1	0	8

Key generated is:-

Key=7101063108 (key size: 10 numeric digits)

The application requires a keyword which is repeated so that the total length is equal to that of the numbers or plaintext input.

For example, suppose the input number is a cell number "9945439885" and the keyword generated is "7101063108" Then, the key is equal length of plaintext.

Key	7	1	0	1	0	6	3	1	0	8
Plain text	9	9	4	5	4	3	9	8	8	5

Numeric Vigenere table (Polynumeric tableau)

	Plain text input										
		0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**
Key	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**0**
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**0**	**1**
	2	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**0**	**1**	**2**
	3	**4**	**5**	**6**	**7**	**8**	**9**	**0**	**1**	**2**	**3**
	4	**5**	**6**	**7**	**8**	**9**	**0**	**1**	**2**	**3**	**4**
	5	**6**	**7**	**8**	**9**	**0**	**1**	**2**	**3**	**4**	**5**
	6	**7**	**8**	**9**	**0**	**1**	**2**	**3**	**4**	**5**	**6**
	7	**8**	**9**	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**
	8	**9**	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**
	9	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**

The poly numeric cipher uses a 10×10 table with 0 to 9 as the row heading and column heading. This table is usually referred to as the Vigenere Table. The first row of this table has the 10 numbers. Starting with the second row, each row has the numbers shifted to the left one position in a cyclic way. The intersection of the Vigenère tableau column of plain-text number and the row of the key number is the cipher-text number [4].

B. Encryption process

Rule:

The intersection of plaintext number in x-axis with key in y axis will be the cipher text number. The encryption algorithm is implemented based on key generated.

Encrypt each number using C7, C1, C0, C1, C0, C6, C3, C1, C0, C8 in turn.

Key	7	1	0	1	0	6	3	1	0	8
Plain text	9	9	4	5	4	3	9	8	8	5
Cipher text	7	1	5	7	5	0	3	0	9	4

There is no statistical relationship between the plain text and cipher text. Each plaintext number has multiple corresponding cipher text numbers. This makes cryptanalysis harder since the number frequency distribution will be flatter.

C. Decryption:

Rule: Decryption simply works in reverse.

Key	7	1	0	1	0	6	3	1	0	8
Cipher text	7	1	5	7	5	0	3	0	9	4
PT	9	9	4	5	4	3	9	8	8	5

D. Numeric vigenere analysis:

(i) Key space?

$10^{\text{Length(Key)}}$

(ii) Frequency analysis?

Doesn’t work because of different keys.

E. Security of Vigenère Ciphers

There are multiple cipher text numbers corresponding to each plaintext number.So,number frequencies are obscured but not totally lost.

F. To break poly numeric cipher

(i) Try to guess the key length.

(ii) If key length is N, the cipher consists of N Caesar ciphers.

IV. CONCLUSION

I have considered a new requirement of key exchange with poly numeric cipher. It is used to exchange secret key between two users by symmetric scheme. This makes an efficient use of key exchange mechanism for sharing a common secret key.

V. FUTURE WORK

To provide Usage of High security cryptographic key exchange using parametric equations or any similar mathematical equations. To ensure integrity of a message, sender can use any MAC/HMAC message authentication schemes. It helps to ensure the sender’s data being transmitted in a secure manner. It is still in its infancy now, and many research are yet to be identified in future.

ACKNOWLEDGMENT

We would like to express our gratitude towards our parents and members of the Department for their kind co-operation and encouragement.Our special gratitude and thanks to all people for giving us such attention and time for completion of this project.

REFERENCES

[1] Ragheb Toemeh and Subbanagounder Arumugam, J., “Applying Genetic Algorithms for Searching Key-Space of Polyalphabetic Substitution Ciphers ”, Vol. 5, No. 1, January 2008. The International Arab Journal of Information Technology.

[2] Omolara, A.I. Oludare and S.E. Abdulahi , “Developing a Modified Hybrid Caesar Cipher and Vigenere Cipher for Secure Data Communication” O.E.. Computer Engineering and Intelligent Systems, Vol.5, No.5, 2014

[3] Ayman Al-ahwal, Sameh Farid. “ The Effect Of Varying Key Length On A Vigenère Cipher” IOSR-JCE, Volume 17, Issue 2, Ver. VI (Mar – Apr. 2015),

AUTHOR PROFILE

Santhosh Kumar B J has completed his M.Tech(I.T) from Karnataka State Open University (KSOU), Mysuru, Karnataka, M.Sc (S.I.S) from Bharathiar University, Coimbathore, Tamil Nadu, B.Sc (PMC) from Mysore University, Karnataka. Now he is working as Assistant Professor, Department of Computer Science, Amrita Vishwa Vidyapeetham University, Mysuru Campus.