Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 3, Issue. 11, November 2014, pg.660 – 667

RESEARCH ARTICLE

Adopting Number Sequences for Shielding Information

Mrs. Sandhya Maitra, Mr. Manish Bansal, Ms. Preety Gupta

Associate Professor - Department of Computer Applications and Institute of Information Technology and Management, India
Student - Department of Computer Applications and Institute of Information Technology and Management, India
Student - Department of Computer Applications and Institute of Information Technology and Management, India
msan324@gmail.com , manish05bansal@gmail.com , preety02gupta@gmail.com

Abstract:-The advancement of technology and global communication networks puts up the question of safety of conveyed data and saved data over these media. Cryptography is the most efficient and feasible mode to transfer security services and also Cryptography is becoming effective tool in numerous applications for information security. This paper studies the shielding of information with the help of cryptographic function and number sequences. The efficiency of the given method is examined, which assures upgraded cryptographic services in physical signal and it is also agile and clear for realization.

1. Introduction

Cryptography is the branch of information security. The basic goal of cryptography is to make communication secure in the presence of third party (intruder). Encryption is the mechanism of transforming information into unreadable (cipher) form. This is accomplished for data integrity, forward secrecy, authentication and mainly for data confidentiality.

The encryption is achieved by algorithm called cipher. It includes number of well defined steps that can be followed as a process. The actual information known as plain text is first converted to unreadable format(encryption) then reverse process takes place (known as decryption). The cipher text contains the original information but in unclear form. It needs a proper mechanism to decrypt it. It should be like random babble to those who are not expected to read.

2. Recurrence Sequence

Recurrence relation or recurrence equation gives description of a series which is based on previous term and recursively defines itself. In general, a recurrence relation links the j^{th} element of a sequence to its precedent. If we have a sequence, $x_1, x_2, x_3, \ldots\ldots x_j$, then it relates the x_j to its previous terms $x_1, x_2, x_3, \ldots\ldots x_{j-1}$, the initial conditions for the sequence $x_1, x_2, x_3, \ldots\ldots x_j$ are explicitly given.

2.1 Pell number

Pell number can be given by –

$$P_n = \begin{cases} 0 & if\ n = 0 \\ 1 & if\ n = 1 \\ 2P_{n-1} + P_{n-2} & \forall\ n > 1 \end{cases}$$

In general term, Pell number starts with 0 following 1, after that it is equal to sum of double the previous term and the term before the previous term.

The first few Pell numbers looks like –
0, 1, 2, 5, 12, 29, 70 …

In matrix form, it is represented with the formula –

$$P^n = \begin{bmatrix} P_{n+1} & P_n \\ P_n & P_{n-1} \end{bmatrix}$$

For n =1, 2, 3, 4 ....., P_{n-1} ,P_n ,P_{n+1}
For n=1, the matrix P_1^1 would be

$$P^1 = \begin{bmatrix} 2 & 1 \\ 1 & 0 \end{bmatrix}$$

For n=2, the matrix would be

$$P^2 = \begin{bmatrix} 5 & 2 \\ 2 & 1 \end{bmatrix}$$

And so on.

Suppose a multiplicative group M which consist the set of all 2X2 matrix over set of real numbers. Consider $P^* = \{P^1, P^2, P^3, \ldots.\}$

P^* is forming a subgroup under matrix multiplication. Moreover, Under M, for each plain text $[PT]_{2X2}$ their exist a cipher text CT(i) such that

$$CT(i) = PT \times P^n$$

The extended dimension matrix of P_1 can be defined as –

$$P_2 = \begin{bmatrix} 2 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

A representation of the matrices P_2^n where n= ±1, ±2…, based on the recurrence relation for a 3×3 matrix is mentioned below. This also represent the normal or direct and the inverse of the P_2^n matrix, where inverse of the

matrix P_2^{-n} is calculated as

$P_2^{-n} = \frac{1}{\det P}\begin{bmatrix} p & q \\ r & s \end{bmatrix}$ which is equal to $\frac{1}{ps-qr}\begin{bmatrix} s & -q \\ -r & p \end{bmatrix}$

for n=1,

$$P_2^{1} = \begin{bmatrix} 2 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

The inverse is

$$P_2^{-1} = \begin{bmatrix} 0 & 1 & 0 \\ 1 & -2 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

For n=2,

$$P_2^{2} = \begin{bmatrix} 5 & 2 & 0 \\ 2 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

The inverse is

$$P_2^{-2} = \begin{bmatrix} 1 & -2 & 0 \\ -2 & 5 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

For n=3,

$$P_2^{3} = \begin{bmatrix} 12 & 5 & 0 \\ 5 & 2 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

The inverse is

$$P_2^{-3} = \begin{bmatrix} -2 & 5 & 0 \\ 5 & -12 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

Similarly it can be extended to further dimension as –

$$P_3 = \begin{bmatrix} 2 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

Also, for any variable value y

$$P_2^{y} \text{ X } P_2^{-y} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

2.2 Padovan sequence

Padovan number are given by recurrence relation as –

$$PS(n) = PS(n-2) + PS(n-3)$$

Basically, it is the sequence of integer with the initial conditions,
PS(0) = 1
PS(1) = 1
PS(2) = 1
Using this the first few values are –
1, 1, 1, 2, 2, 3, 4, 5…

In matrix form, the sequence can be given as –

$$PS^n = \begin{bmatrix} PS_{n-5} & PS_{n-3} & PS_{n-4} \\ PS_{n-4} & PS_{n-2} & PS_{n-3} \\ PS_{n-3} & PS_{n-1} & PS_{n-2} \end{bmatrix}$$

Where n = 1, 2, 3, 4…..
For negative values i.e. n<0 the padovan sequence is defined as –

$$PS(n) = P(n+3) – P(n+1)$$

For n = 1

$$PS^1 = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \end{bmatrix}$$

The inverse is

$$PS^{-1} = \begin{bmatrix} -1 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}$$

For n = 2

$$PS^2 = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix}$$

The inverse is

$$PS^{-2} = \begin{bmatrix} 1 & 1 & -1 \\ -1 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix}$$

The matrix PS^1 is equivalent to Fibonacci Q matrix. For any variable y

$$PS^y \text{ X } PS^{-y} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

2.3 Perrin Sequence

Perrin number are given by recurrence relation as –

$$PERS(n) = PERS(n-2) + PERS(n-3)$$

Basically, it is the sequence of integer with the initial conditions,
PERS(0) = 3

PERS(1) = 0
PERS(2) = 2
Using this first few values are –

3, 0, 2, 3, 2, 5, 5, 7, 10, 12…

In matrix form, the sequence can be given as –

$$\text{PERS}^n = \begin{bmatrix} PERS_{n-5} & PERS_{n-3} & PERS_{n-4} \\ PERS_{n-4} & PERS_{n-2} & PERS_{n-3} \\ PERS_{n-3} & PERS_{n-1} & PERS_{n-2} \end{bmatrix}$$

Where n = 1, 2, 3, 4…..
For n = 1

$$\text{PERS}^1 = \begin{bmatrix} -3 & 1 & 2 \\ 2 & -1 & 1 \\ 1 & 3 & -1 \end{bmatrix}$$

The inverse is

$$\text{PERS}^{-1} = \begin{bmatrix} -2/23 & 7/23 & 3/23 \\ 3/23 & 1/23 & 7/23 \\ 7/23 & 10/23 & 1/23 \end{bmatrix}$$

For n = 2

$$\text{PERS}^2 = \begin{bmatrix} 2 & -1 & 1 \\ 1 & 3 & -1 \\ -1 & 0 & 3 \end{bmatrix}$$

The inverse is

$$\text{PERS}^{-2} = \begin{bmatrix} 9/23 & 3/23 & -2/23 \\ -2/23 & 7/23 & 3/23 \\ 3/23 & 1/23 & 7/23 \end{bmatrix}$$

For any variable y

$$\text{PERS}^y \text{ X } \text{PERS}^{-y} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

3. Applications of recursive sequence

In this section the applications of recursive sequence with respect to cryptography and with respect to new dimension of matrix are given. Now as initial message be a digital signal and suppose this message be a sequence of real numbers as given below –

$a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8, a_9, a_{10}, a_{11}, a_{12}, a_{13}, a_{14}, a_{15}, a_{16}, a_{17}, a_{18}, a_{19}, a_{20}, a_{21}, \ldots\ldots$

Now, suppose nine readings are chosen from this sequence of real numbers. It forms a matrix of plain text PT of dimension 3X3.To form a matrix there can be 9! Permutations.

$$\text{PT} = \begin{bmatrix} a_9 & a_8 & a_7 \\ a_6 & a_5 & a_4 \\ a_3 & a_2 & a_1 \end{bmatrix}$$

If Per_i be the choice of matrix. The direct matrix is the matrix for encryption and inverse of this matrix is matrix for decryption. For cryptographic key, the variable y is chosen. Generally the key involves three parameters. First is permutation chosen Per_i, the second is variable y and last is recursion type R. The representation of the key is as follow –

K = $\{Per, y, R\}$

The encryption and decryption algorithm with CT(y) as the cipher text matrix is –

IF R = Pell
THEN
[CT] ⟵ [PT][P_2^y];
[PT] ⟵ [CT][P_2^{-y}];
ENDIF

IF R = PS
THEN
[CT] ⟵ [PT][PS^y];
[PT] ⟵ [CT][PS^{-y}];
ENDIF

IF R = PERS
THEN
[CT] ⟵ [PT][$PERS^y$];
[PT] ⟵ [CT][$PERS^{-y}$];
ENDIF

4. Example

Suppose the plain text to be communicated be –

$$PT = \begin{bmatrix} 9 & 8 & 7 \\ 6 & 5 & 4 \\ 3 & 2 & 1 \end{bmatrix}$$

Let the variable y is 1 and recursion type is pedovan, so,

$$PS^1 = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \end{bmatrix}$$

To encrypt our message, first step is to make cipher text by using following statement –

$$CT(y) = \begin{bmatrix} 9 & 8 & 7 \\ 6 & 5 & 4 \\ 3 & 2 & 1 \end{bmatrix} X \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \end{bmatrix}$$

$$\Rightarrow \begin{bmatrix} 7 & 16 & 8 \\ 4 & 10 & 5 \\ 1 & 4 & 2 \end{bmatrix}$$

Now, to decrypt our message, the next step is to make again the plain text from the cipher text by using the following statement –

$$PT = \begin{bmatrix} -1 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix} X \begin{bmatrix} 7 & 16 & 8 \\ 4 & 10 & 5 \\ 1 & 4 & 2 \end{bmatrix}$$

$$\Rightarrow \begin{bmatrix} 9 & 8 & 7 \\ 6 & 5 & 4 \\ 3 & 2 & 1 \end{bmatrix}$$

5. Time Computation for Cryptography Procedure

The total time for cryptography process in which, time is calculated for encryption and then for decryption. This is given as, E_t and D_t, respectively.
For e.g.
Consider a plain text matrix $PT = \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix}$
Choosing recursive type as pell number for n= 1.so
$P = \begin{bmatrix} 2 & 1 \\ 1 & 0 \end{bmatrix}$

Applying algorithm, we do encryption as -
$CT = \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix} X \begin{bmatrix} 2 & 1 \\ 1 & 0 \end{bmatrix}$

$$\Rightarrow \begin{bmatrix} 4 & 1 \\ 10 & 3 \end{bmatrix}$$

Now, for decryption –

$$PT = \begin{bmatrix} 4 & 1 \\ 10 & 3 \end{bmatrix} X \begin{bmatrix} 0 & 1 \\ 1 & -2 \end{bmatrix}$$

$$\Rightarrow \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix}$$

This calculation involves total four reading and hence the encryption process includes 1 addition and 2 multiplications to make message as cipher text. Similarly, it is done for decryption process i.e. to convert cipher text to plain text again. It is given as –
$E_t = 8m_T$ X 4 a_T
$D_t = 8m_T$ X 4a_T
The total time taken for encryption and decryption is not much as it includes simple mathematical operation. So this method is an agile method for upgraded cryptography.

6. Performance of Recommended Method

It is very much possible to raise the security of information by using numerous encryption and decryption process. To encrypt the message, the first step for specific recursion is to pick the variable y and permutation Per.
Also, the cryptographic key is formed with choosing permutation and variable y. Let variable be y_i and permutation be Per_i

The cryptographic key is introduced as –
$K_1 = \{Per_{i,} y_1 ,R\}$
With the help of this value the encryption matrix would be formed as –
$CT_1 = CT(Per_{i,} y_1 ,R)$
Now considering CT_1 as initial matrix, the next key is formed as –
$K_2 = \{Per_{i+1}, y_2 ,R\}$
Again with the help of this value the next encryption matrix would be formed as –
$CT_2=CT_1(Per_{i,} y_1,R ;Per_{i+1,} y_2,R)$
Now considering CT_2 as initial matrix, the next key is formed as –
$K_3 = \{Per_{i+2}, y_3 ,R\}$
Again with the help of this value the next encryption matrix would be formed as –
$CT_3=CT_2(Per_{i,} y_1,R ;Per_{i+1,} y_2,R,Per_{i+2}, y_3,R)$
And so this process is continuously used for different variable values and random permutations upto n terms.
As the outcome of this repeated procedure, the matrix CT is obtained as CT(K) ,
Where $K = \{Per_i, y_1, R; Per_{i+1}, y_2, R; Per_{i+2}, y_3, R;\ldots\ldots Per_k, y_n, R.\}$
The inverse of cryptographic key K^{-1} is employed to decrypt the information. The key because of the closure property is given as –
$K^{-1} = \{Per_k, y_n ,R;Per_{k-1},y_{n-1} ,R; Per_{k-2}, y_{n-2}, R;\ldots\ldots\ldots\ldots Per_i,y_1 ,R\}$

7. Conclusions

This paper uses symmetrical cryptography where same key is used. In this paper three recursion types are explained but any number of recurrence sequences can be used. This also involves higher level of security as it includes three parameters i.e., first is the power of the matrix, second is the permutation and third is the recurrence type used. Also, it enhances the security of information as it involves numerous encryption and decryption process. Therefore a more dependable cryptosystem can be accomplished. Additionally, as size of the matrix increases, more data can be sent strongly at a time.

References

1) R. L. Rivest, A. Shamir, and L. Adleman . A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. Communicationsof the ACM, 21(2):120-126, February 1978.
2) N. Koblitz, Elliptic Curve Cryptosystems, Mathematics of Computation, Vol. 48, pp. 203-209, 1987.
3)"Fibonacci and Lucas numbers". Palo Alto,CA:Houghton-Mifflin;1969.
4) T. Blum and C. Paar, Montgomery modular multiplication on reconfigurable hardware. In Proceedings of the 14th IEEE Symposium on Computer Arithmetic (ARITH-14), pages 70-77, 1999.
5) Martin E. Hellman & W. Diffie "Privacy and Authentication: An Introduction to Cryptography" PROCEEDINGS OF THE IEEE, VOL. 67, NO. 3,MARCH,1979,pp397-427
6) A. Odlyzko, Discrete logarithms and smooth polynomials. Finite Fields: theory, applications, and algorithms, Contemp. Math 168, American Mathematical Society, pp. 269–278, 1994.
7) A.Sekhar D.Kumar.Ch.Suneetha ,Encryption of Data streams using Paul‟s spin ½ matrices, International Journal of Engineering science and Technology. Vol2(6), 2010, 2024 -2028
8) S.Vanstone.A.Menezed, P.Van Oorschot,Hand book of Applied Cryptography
9) N. Gura, S. Chang, H. Eberle, G. Sumit, V. Gupta, D. Finchelstein, E.Goupy, and D. Stebila. An End-to-End Systems Approach to EllipticCurve Cryptography. In C. K. Koc and C. Paar, editors, Cryptographic Hardware and Embedded Systems - CHES 2001, volume LNCS 1965,pages 351-366. Springer-Verlag, 2001.
10) F. J. (1993). *Signal Processing of Speech*.

