Cryptography Protection of Digital Signals using Some Recurrence Relations

K.R. Sudha[1], A.Chandra Sekhar[2], Prasad Reddy P V G D [3]

[1] Department of Electrical Engg , Andhra University , Visakhapatnam(INDIA)
[2] Department of Engineering Mathematics, GITAM , Visakhapatnam (INDIA)
[3]Department of Computer Science and Systems Engg , Andhra University , Visakhapatnam(INDIA)

Summary
Communications security is gaining importance as a result of the use of electronic communications in more and more business activities. Cryptography is the only practical means to provide security services and it is becoming a powerful tool in many applications for information security. Literature demonstrates a new kind of cryptography called golden cryptography [1]. This paper examines the application of recurrence relations in the continuous domain, and a cryptographic method based on recurrence relations is proposed and implemented. The performance of the proposed method is analyzed, which ensures improved cryptographic protection in digital signals and it is also fast and simple for realization.

Keywords:
Recurrence relations, Cryptography, Fibonacci numbers, Bernoulli's numbers, Lucas numbers.

1. Introduction:

The fundamental objective of cryptography is to enable two people, to communicate over an insecure channel in such a way that an opponent cannot understand what is being said. Encryption is the process of obscuring information to make it unreadable without special knowledge. This is usually done for secrecy, and typically for confidential communications.

A cipher is an algorithm for performing encryption (and the reverse, decryption) — a series of well-defined steps that can be followed as a procedure. An alternative term is encipherment [4-7]. The original information is known as plaintext, and the encrypted form as cipher text. The cipher text message contains all the information of the plaintext message, but is not in a format readable by a human or computer without the proper mechanism to decrypt it; it should resemble random gibberish to those not intended to read it.

Ciphers are usually parameterized by a piece of auxiliary information, called a key. The encrypting procedure is varied depending on the key which changes the detailed operation of the algorithm. Without the key, the cipher cannot be used to encrypt, or more importantly, to decrypt.

2. Recurrence relations:

Recurrence relation is useful in certain counting problems like Fibonacci numbers. A recurrence relation relates the nth element of a sequence to its predecessors. Recurrence relations are related to recursive algorithms. A " recursive relation" for the sequence $a_0,a_1,a_2,....$ is an equation that relates a_n to certain of its preceding terms $a_0,a_1,a_2,.... ,a_{n-1}$.Initial conditions for the sequence $a_0,a_1,a_2,....$ are explicitly given values for a finite number of the terms of the sequence.

As an example the Ackermann's function can be defined by the recurrence relations:

$A(m, n) = A(m-1,1), \quad m = 1,2.....$
$A(m-1, A(m,n-1)), \quad m = 1,2.....$
$\qquad\qquad\qquad\qquad n = 1,2.....$

and initial conditions

$A(0,n) = n+1, \qquad n = 0,1.....$

In this section three recurrence relations Fibonacci, Bernoulli's, Lucas numbers were presented and their application to cryptography is examined.

2.1 Fibonacci numbers:

Fibonacci numbers are given by the following recurrence relation

$$F_{n+1} = F_n + F_{n-1} \qquad (1)$$

With the initial conditions $F_1=F_2=1$ (2)

A square matrix (2X2) as shown below was introduced in [1]

$$Q = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} \qquad (3)$$

and the following property of nth power of Q was proved in [1-3]

$$Q^n = \begin{bmatrix} F_{n+1} & F_n \\ F_n & F_{n-1} \end{bmatrix} \qquad (4)$$

Where n=0, ±1, ±2…….. F_{n-1}, F_n, F_{n+1} are the Fibonacci numbers

The following identity holds good for the matrix Q^n

$$Q^n = Q^{n-1}+Q^{n-2} \quad (5)$$

Which is similar to the recurrence relation in Fibonacci numbers.

Consider the multiplicative group M_2 the set of all 2 X2 matrices over the set of real numbers. Let

$$Q^* = \{Q^1, Q^2, Q^3, ...\}$$

Clearly Q^* forms a subgroup under matrix multiplication with

$$Q^n = \begin{bmatrix} F_{n-1} & F_n \\ F_n & F_{n+1} \end{bmatrix}$$

with

$$Q^1 = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix} \quad (6)$$

Moreover for each plain text $[A]_{2X2}$ which belongs to M_2 there exists a cipher text C(i) such that $C(i) = A \times Q^n$.

The extensions to the above matrix is as follows

$$Q_2 = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \quad (7)$$

This matrix is formed from (6) as

$$Q_2 = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \quad (8)$$

The Q_2 matrix is so formed such that its determinant is invariant without loss of generality to the ''Cassini formula'' [8] which is one of the most important theorems of the Fibonacci numbers theory.

$$\left|Q^n\right| = F_{n-1} \times F_{n+1} - F_n^2 = (-1)^n$$

The same logic can be extended to a 4×4 matrix

$$Q_3 = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

Similarly it can be extended to any order square matrix.

A representation of the matrices Q^n for n=0,±1, ±2…, based on the recurrence relation in (5) for a 3×3 matrix is given in table 1. The Table 1 gives the direct as well as the inverse of the Q^n matrix. For any variable value x

$$Q_2^x \times Q_2^{-x} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \quad (9)$$

n	1	2	3	4	5
Q_2^n	$\begin{bmatrix} 0 & 1 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$	$\begin{bmatrix} 1 & 1 & 0 \\ 1 & 2 & 1 \\ 0 & 0 & 1 \end{bmatrix}$	$\begin{bmatrix} 1 & 2 & 0 \\ 2 & 3 & 0 \\ 0 & 0 & 1 \end{bmatrix}$	$\begin{bmatrix} 2 & 3 & 0 \\ 3 & 5 & 0 \\ 0 & 0 & 1 \end{bmatrix}$	$\begin{bmatrix} 3 & 5 & 0 \\ 5 & 8 & 0 \\ 0 & 0 & 1 \end{bmatrix}$
Q_2^{-n}	$\begin{bmatrix} -1 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix}$	$\begin{bmatrix} -2 & -1 & 0 \\ -1 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$	$\begin{bmatrix} -3 & 2 & 0 \\ 2 & -1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$	$\begin{bmatrix} 5 & -3 & 0 \\ -3 & 2 & 0 \\ 0 & 0 & 1 \end{bmatrix}$	$\begin{bmatrix} -8 & 5 & 0 \\ 5 & -3 & 0 \\ 0 & 0 & 1 \end{bmatrix}$

Table 1 : Explicit forms of Matrices Qn

2.2 Bernoulli Numbers:

The famous Bernoulli numbers are defined by [8][9]

$$\frac{x}{e^{x-1}} = \sum_{n=0}^{\infty} B_n \frac{x^n}{n!}, \ |x| < 2\pi \quad (10)$$

The recursion formula involving Bernoulli is

$$B_n = \sum_{k=0}^{n} \binom{n}{k} B_k \quad for \ n \geq 2 \quad (11)$$

Taking $B_0 = 1$, $B_1 = \frac{-1}{2}$, which successively yields the values

$$B_2 = \frac{1}{6}, B_4 = -\frac{1}{30}, B_6 = \frac{1}{42}, B_8 = -\frac{1}{30}, B_{10} = \frac{5}{66}, B_{12}$$

$= -\frac{691}{2730}$ .....

$B_{2k+1} = 0,(k=1,2,....)$

Moreover, the Bernoulli numbers B_{2k} alternate in sign, and are related to Riemann zeta function $\zeta(2k)$ as follows:

$$\zeta(2k)=(-1)^{k+1}\frac{(2\pi)^{2k}B_{2k}}{2(2k)!} \qquad (12)$$

The proposed matrix using Bernoulli's recursion is

$$B^n=\begin{bmatrix} B_{n-1} & B_n \\ B_n & B_{n+1} \end{bmatrix} \qquad (13)$$

$$\Rightarrow B_1=\begin{bmatrix} 1 & \frac{-1}{2} \\ \frac{-1}{2} & \frac{1}{6} \end{bmatrix}$$

The extensions of the above matrix is as follows

$$\Rightarrow B_2=\begin{bmatrix} 1 & \frac{-1}{2} & 0 \\ \frac{-1}{2} & \frac{1}{6} & 0 \\ 0 & 0 & 1 \end{bmatrix} \qquad (14)$$

$$B_2^{-1} = \begin{bmatrix} -2 & -6 & 0 \\ -6 & -12 & 0 \\ 0 & 0 & 1 \end{bmatrix} \qquad (15)$$

For any variable x

$$B_2^x \times B_2^{-x}=\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \qquad (16)$$

The other explicit forms of B^n can be obtained recursively same as Q^n

2.3 Lucas numbers:

The sequence of Lucas numbers L_k is defined by the second-order linear recurrence formula and initial terms [10] [11] [12]

$L_{k+1} = L_k + L_{k-1}$, $L_0=2, L_1=1$ (17)

The proposed matrix using Lucas's recursion

$$L^n=\begin{bmatrix} L_{n-1} & L_n \\ L_n & L_{n+1} \end{bmatrix} \qquad (18)$$

$$\Rightarrow L_1=\begin{bmatrix} 2 & 1 \\ 1 & 3 \end{bmatrix} \qquad (19)$$

The extensions of the above matrix is as follows

$$\Rightarrow L_2=\begin{bmatrix} 2 & 1 & 0 \\ 1 & 3 & 0 \\ 0 & 0 & 1 \end{bmatrix} \qquad (20)$$

$$\Rightarrow L_2^{-1}=\begin{bmatrix} 0.6 & -0.2 & 0 \\ -0.2 & 0.4 & 0 \\ 0 & 0 & 1 \end{bmatrix} \qquad (21)$$

For any variable x

$$L_2^x \times L_2^{-x}=\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \qquad (22)$$

The other explicit forms of L^n can be obtained recursively same as Q^n

3 Application to Cryptography :

This section examines the application of recurrence relations to golden cryptography [1] with a new dimensionality in the matrix.

Let the initial message be a digital signal which is a sequence of separate real numbers

$a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8, a_9,.....$

Let us choose nine readings and form a 3 X 3 matrix A which is considered as a plain text matrix.

$$A=\begin{bmatrix} a_1 & a_2 & a_3 \\ a_4 & a_5 & a_6 \\ a_7 & a_8 & a_9 \end{bmatrix} \qquad (23)$$

There can be 9! permutations to form the matrix. If P_i be the choice of i^{th} permutation. Choosing the direct matrix enciphering matrix and inverse as deciphering matrix. The variable x is chosen as cryptographic key. In general the key K consists of the permutation P_i , the variable x and the type of recursion used is R

K= {P, x, R} (24)

Let C(x) be the cipher text matrix then the encryption algorithm is

If R=Fib then

$[C] \leftarrow [A][Q_2^X]$;

[A] ←[C][Q_2^{-X}];
Endif

If R=Luc then
[C] ←[A][L_2^{X}];
[A] ←[C][L_2^{-X}];
Endif

If R=Bern then
[C] ←[A][B_2^{X}];
[A] ←[C][B_2^{-X}];
Endif

4 Example:

Let the plain text to be transmitted be

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

Choosing x=1 and the type of recursion as Fibonacci

Q_2^n for n=2 is

$$\begin{bmatrix}1 & 1 & 1\\ 0 & 1 & 0\\ 0 & 0 & 1\end{bmatrix}$$

The first step is to form C(x) from (25)

$$C(x)=\begin{bmatrix}1 & 2 & 3\\ 4 & 5 & 6\\ 7 & 8 & 9\end{bmatrix}\times\begin{bmatrix}1 & 1 & 1\\ 0 & 1 & 0\\ 0 & 0 & 1\end{bmatrix}=\begin{bmatrix}1 & 3 & 4\\ 4 & 9 & 10\\ 7 & 15 & 16\end{bmatrix}$$

The second step is calculation of A from C(x) using (26)

$$A=\begin{bmatrix}-1 & 1 & 0\\ 1 & 0 & 0\\ 0 & 0 & 1\end{bmatrix}\times\begin{bmatrix}1 & 3 & 4\\ 4 & 9 & 10\\ 7 & 15 & 16\end{bmatrix}=\begin{bmatrix}1 & 2 & 3\\ 4 & 5 & 6\\ 7 & 8 & 9\end{bmatrix}$$

5 Calculation of Encryption and Decryption time:

The encryption consists in calculation of the nine elements of the C(x) which include three multiplications and two additions.
If Δt_m is the time required for each multiplication
Δt_a is the time required for each addition

Total encryption time is given as

$$T_e = 27\Delta t_m + 18\,\Delta t_a \qquad (25)$$

Similarly the total decryption time is given as

$$T_d = 27\Delta t_m + 18\,\Delta t_a \qquad (26)$$

From (31) and (32) the time taken for encryption and decryption is less and hence this method as an enhanced Golden Cryptography can prove to be a fast method for digital signals.

6 Performance of the proposed method:

It is possible to increase the cryptographic protection using multiple encryption and decryption [1]. The first step of encryption is for a particular recurrence choose randomly the permutation P and variable x.
Let the initial value of permutation be P_i and variable be x_1 .
Hence the first cryptographic key would be
$K_1 = \{P_i, x_1, R\}$
The encryption matrix due to this value is
$C_1=C(P_i, x_1, R)$
The second step of encryption is to use this matrix as the initial matrix. The second cryptic key would be
$K_2 = \{P_j, x_2, R\}$
The new matrix formed with this cryptic key is
$C_2=C_1(P_i, x_1, R ; P_j, x_2, R)$
The procedure can however be repeated for n random permutations and n values of the variable
we get the matrix C=C(K)
That is $K = \{P_i, x_1, R; P_j, x_2, R \ldots\ldots P_k, x_n, R.\}$ (27)
As a result of this multiple encryption
For the decryption algorithm we shall apply the inverse cryptographic key K^{-1} which due to the closure property is equal to

$K^{-1} = \{ P_k, x_n, R; P_r x_{n-1}, R; \ldots\ldots\ldots\ldots P_i, x_1, R\}$ (28)

7 Conclusions

The above method refers to symmetrical cryptography. In the present paper three types of recurrences are discussed but in general can be extended to any recurrence relation. The transmission of the key can be done using any algorithm used in asymmetric cryptosystem. The level of security is more since it involves three parameters i.e., the permutation, the power of the matrix and type of recurrence used. Also the cryptographic protection of digital signals can be improved by using multiple encryption and decryption. Therefore a more reliable cryptosystem can be realized. Moreover by increasing the size of the matrix, more information can be sent securely at a time.

References:

[1]. A.P. Stakhov, ”The ‘‘golden’’ matrices and a new kind of cryptography”, Chaos, Soltions and Fractals 32 ((2007) pp1138–1146

[2]. A.P. Stakhov. “The golden section and modern harmony mathematics. Applications of Fibonacci numbers,” 7,Kluwer Academic Publishers; (1998). pp393–99.

[3]. A.P. Stakhov. “The golden section in the measurement theory”. Compute Math Appl; 17(1989):pp613–638.

[4]. Whitfield Diffie And Martin E. Hellman, New Directions in Cryptography” IEEE Transactions on Information Theory, Vol. -22, No. 6, November 1976 ,pp 644-654

[5]. Whitfield Diffie and Martin E. Hellman “Privacy and Authentication: An Introduction to Cryptography” PROCEEDINGS OF THE IEEE, VOL. 67, NO. 3, MARCH 1979,pp397-427

[6]. A. M. Odlyzko. Discrete logarithms in finite fields and their cryptographic significance. In Advances in Cryptology (EUROCRYPT 1984), Springer LNCS 209, pp224–314, 1985

[7]. A. M. Odlyzko.” Discrete logarithms and smooth polynomials. Finite Fields: theory, applications, and algorithms”, Contemp. Math 168, American Mathematical Society, pp. 269–278, 1994.

[8]. Tianping Zhang, Yuankui Ma “ On Generalized Fibonacci Polynomials and Bernoulli Numbers” Journal of Integer Sequences, Vol. 8 (2005), pp1-6

[9]. M. Apostol, Introduction to Analytic Number Theory, Springer-Verlag, New York, 1976.

[10]. Hoggat VE. “Fibonacci and Lucas numbers”. Palo Alto, CA: Houghton-Mifflin; 1969.

[11]. Tony D. Noe, Jonathan Vos Post “ Primes in Fibonacci n-step and Lucas n-step Sequences” Journal of Integer Sequences, Vol. 8 (2005), Article 05.4.4, pp1-12

[12]. T. Koshy, Fibonacci and Lucas Numbers with Applications, John Wile y and Sons, NY, 2001

K.R.Sudha received her B.E. degree in Electrical Engineering from GITAM, Andhra University 1991.She did her M.E in Power Systems 1994. She was awarded her Doctorate in Electrical Engineering in 2006 by Andhra University. During 1994-2006, she worked with GITAM Engineering College and presently she is working as an Associate Professor in the department of Electrical engineering, Andhra University, Visakhapatnam, India.

A .Chandra Sekhar received his MSc., degree with specialization in algebraic number theory from Andhra University in 199 He Secured the prestigious K.NAGABHUSHANAM Memorial Award in M.Sc., for obtaining University First rank. He did his MPhil from Andhra University in 2000.He was with Gayatri degree college during 1991to 1995 and later joined GITAM Engineering college in 1995. Presently he is working as Associate Professor in the department of Engineering Mathematics at GITAM Engineering college, Visakhapatnam, INDIA.

Dr Prasad Reddy P V G D, is a Professor of Computer Engineering with Andhra University, Visakhapatnam, INDIA. He works in the areas of enterprise/distributed technologies, XML based object models. He is specialized in scalable web applications as an enterprise architect. With over 20 Years of experience in filed of IT and teaching, Dr Prasad Reddy has developed a number of products, and completed several industry projects. He is a regular speaker in many conferences and contributes technical articles to international Journals and Magazines with research areas of interest in Software Engineering, Image Processing, Data Engineering , Communications & Bio informatics