Encryption and Decryption Scheme by Using Finite State Machine

G. Karudaiyar[1], S.Karthikeyan[2] and B. Sainath[3]

[1,3] Master of Engineering, Embedded System, Sathyabama University, India.
[2] Assistant Professor,Electronics And Communication,Sathyabama University, India.

doi: http://dx.doi.org/10.13005/bbra/1595

(Received: 15 August 2014; accepted: 10 October 2014)

Cryptography is the science of using mathematics to encrypt and decrypt information. Encryption is the process of masking information to make it unreadable without a key approach. Secrecy is to be maintained for confidential communications. Decryption is the process of extracting the original information from the encrypted data. In This Approach secrecy is maintained by using finite state machine. Fibonacci series are the series of numbers in which each number is the sum of the foregoing numbers.Moore Machine is one of the finite state machine that is being used. Recurrence relations are recursive definitions of mathematical functions or sequences. In this paper cryptographic scheme using Moore machine is applied to verify is result on Fibonacci numbers.

Key words: Fibonacci,MooreMachine,Recurrence Relation

Cryptography is an art of storing and transmitting data in a particular form. so that only those for whom it is signified can read and process it. Cryptography includes techniques such as microdots, integrate words with images, and other ways to hide information in storage or transmit. The cryptography having two important factors. The one is encryption and another one is decryption. Both the techniques are mainly used for secure the information. Encryption is a method and conversion of plain text into cipher text. Decryption is the reverse process of encryption. Conversion of cipher text into plain text. Individual who practice their encryption and decryption is known as cryptographers. The information is determined by whether the user has a certain piece of secret knowledge. The secret knowledge can transform the opaque information back into its useful form. The secret knowledge can be called as a key. This paper approach is purely depends on finite state machine. The finite state machine is a set of possible inputs.A set of possible actions or output events that result from a new state. The recurrence relation has introduced based on Fibonacci series.

A finite state machine is one that has a limited or finite number of possible states. A finite state machine can be used both as a development tool for approaching and solving problems and as a formal way of describing the solution for later developers and system maintainers

* To whom all correspondence should be addressed.

Encryption and decryption:

In cryptography encryption is the process of changing the one type of information into another type of information in a secure manner. Unauthorized people could not read that data. The value of encryption is a cipher text. The cipher text is not in an original format. The purpose of encryption is a confidentiality of a data stored in a computer system or transmitted via internet. The encryption key is a major part in an encryption. The key classified as a two types. The one is public key and another one is a private key. Both two keys are mainly used in encryption and decryption. The public key shared with everyone. But the private must be kept secret. The encryption strength is related to key size directly. But as the key size increases so too do the resources required to perform the computation**.**

Decryption is the process of taking encoded or encrypted text or other data and converting it back into text that you or the computer are able to read and understand. This term is used to describe a method of un-encrypting the data manually or with un-encrypting the data using the proper codes or keys. Very difficult to decrypt the data without knowing the secret key. After decryption we will get the original text.

Mealy machine:

The mealy machine is also one of the state machine. The state machine is nothing but change the states depends on the input.it generates an output based on its current state and input. Basically the output of a mealy machine is depends on the input and next state. The use of a Mealy FSM leads often to a reduction of the number of states.

A Mealy machine is a six-tuple, (S, S0, Ó, Ë, T, G), consisting of the following:

A finite set of states’ S

A start state (also called initial state) S0 which is an element of S

A finite set called an input alphabet Ó

A finite set called an output alphabet Ë

A transition function T: S × Ó ’! S mapping pairs of a state and an input symbol to the corresponding next state.

An output function G: S × Ó ’! Ë mapping pairs of a state and an input symbol to the corresponding output symbol.

The transition and output functions are merged into a single function T: S × Ó ’! S × Ë.

Recurrence relations:

A recurrence relation is an equation which is defined in terms of itself.The recurrence relation, which are the form of $C_0 X_N+ C_1 X_{N-1} + C_2 X_{N-2}+ …. + C_K X_{N-K}=B_{N.}$Where C_0=! 0. If b_n=0 the recurrence relation is called as homogeneous. Otherwise it is called as non-homogenous. TheFibonacci sequence relation is based on recurrence relation. TheFibonacci relation is 1, 1,2,3,5,8,13, Thefibbnoccidefinition is F_n=Fn-1+Fn-2.....

The initial condition is F1=1; F2=1.the iteration is the only one method to solve the recurrence relation problem.

Recurrence matrix

The recurrence matrix is based on recurrence relation whose value taken from recurrence relation.

For example

F_{N+1} F_N

R=F_N

$F_{N-1}$where n=0, 1,2,3,……F_N is the fibbnocci numbers.

Theorem 1:

The recurrence matrix is a secret key if it is invertible matrix.

Proof:

Suppose R is a recurrence matrix which is a confidential key and let P be the plain text. Then PR = C, where c is the encrypted text. To receive the original message P= CR^{-1}. Therefore R-1 must exit. Therefore R must be non-singular and vice versa.

Applications to Cryptography:

The initial message could be a digital signal which is a sequence of separate real numbers $a_{0,}$ a1, a2$_{,.....}$ Let us choose nine readings and form a 2x2 matrix P which is considered as plain text matrix P = $\begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix}$

There can be 4! Permutations to form the matrix, if Pi be the choice of ith permutation. Selecting 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 Moore Machine M, the variable x the permutation Pi and the type of recurrence relation used is R[1][2][3][4].

Algorithm using recurrence matrix:

Algorithm:

Step 1:

Let as consider the plain text as p.

Step 2:

Define the public channel input

Step 3:

Implement Moore and mealy machine through public channel.

Step 4:

Send the Secret key to the receiver.

Step5:

Calculate the cipher text using the theorem.

Step6:

Send the cipher text to the receiver.

Step 7:

Decryption

Decrypt the cipher text using the inverse operation and key to get the plain text.

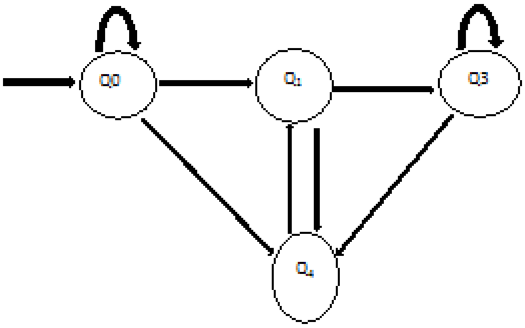

Fig. 1. Moore Machine to calculate residue mod 31

Examples

Example 1:

Let the plain text to be

$P = \begin{matrix} 1 & 2 \\ 3 & 4 \end{matrix}$

and $R(n) = \begin{matrix} f_{n+1} & f_n \\ f_n & f_{n-1} \end{matrix}$ of Fibonacci sequence.

Let the input key be 10110 and recurrence matrix key is $\begin{matrix} 2 & 1 \\ 1 & 1 \end{matrix}$

, and finite state machine is defined as a machine which calculates the residue mod 31 of the given value.

Example 1:

Let the cipher text at q(i+1) state is equal to the cipher text at q(i)th the state multiplied by R(n)output of the moore machine at q(i+1) state

Table1. Cipher text for the given secret key

S No	Input	Previous State	Present State	Output	Cipher Text
1	1	Q_0	Q_1	1	4 3 10 7
2	0	Q_1	Q_2	2	29 18 71 44
3	1	Q_2	Q_1	1	76 47 186 115
4	1	Q_1	Q_3	3	1364 843 3338 2063
5	0	Q_3	Q_2	0	9349 5778 22879 14140

For the easy of computations take mod 31 then the cipher text will be $= \begin{matrix} 18 & 12 \\ 1 & 4 \end{matrix}$

Example 2:

Let the plain text to be

$P= \begin{matrix} 1 & 2 \\ 3 & 4 \end{matrix}$

and $R(n)= \begin{matrix} f_{n+1} & f_n \\ f_n & f_{n-1} \end{matrix}$ of Fibonacci sequence.

Let the input key be 10110 and let the cipher text at q(i+1) state is equal to the cipher text at $q(i)^{th}$ the state multiplied by $R(n)^{\text{output of the Moore machine at q(i+1) state}}$

Performance analysis:

Key strenth:

It is very difficult to guess the secret key even finite state machine is known

Table 2. Cipher text for the given secret key

S.No	Input	Previous State	Present state	Output	Key Matrix	Cipher Text
1	1	Q_0	Q_1	1		
2	0	Q_1	Q_2	2		
3	1	Q_2	Q_1	1		
4	1	Q_1	Q_3	3		
5	0	Q_3	Q_2	2		

Time calculation:

Let t1 be the time required for each multiplication. Let t2 be the time required for each addition. Then the total time required for n key bit matrix multiplication isr(n^3t1+n(n-1)t2)

Example	Mathematical computations	Total Encryption Time
1	Less	r (n^3t1+n(n-1)t2)
2	Less	r (n^3t1+n(n-1)t2)

Security analysis:

The original information extraction is highly impossible because of the difficult mathematical calculations. Even the finite state machine is known the two stage attacks are at a time impossible.Brute force attack is not at all possible because the key size increased.

S. NO	Name Of The Attack	Possibility Of The Attack	Remarks
1	Cipher Text Attack	Very Difficult	Very difficult due to the different cipher texts at different states
2	A knownplain textattack	Verydifficult	Very difficult due to thedifferent states in chosenfinite state machine andrecurrence matrix
3	A chosenplain textattack	Verydifficult	Very difficult due to thematrix multiplicationpropagationErrors.
4	An adaptivechosen plaintext attack	Verydifficult	Very difficult due to thechosen finite statemachine and therecurrence matrix
5	A chosencipher textattack	Verydifficult	Very difficult due to theinverse recurrence matrixmultiplication withoutknowing apt key
6	An adaptivechosencipher textattack	Verydifficult	Very difficult due to themathematical calculations

CONCLUSION:

Algorithm proposed, is based on finite state machine (Moore machine) and matrix multiplication. In this algorithm linear recurrence relation of order 2 is used. Secrecy is maintained at two levels, one is key and other is key matrix obtained using recurrence relation. The obtained encrypted text becomes quite difficult to break or to find the original information even if the algorithm is known.

REFERENCES:

1. A.P. Stakhov, "The „„golden matrices and a new kind of cryptography", *Chaos, Soltions and Fractals*, 2007; **32**; 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;* 1989; **17**: pp613–638.
4. S.Karthikeyan."Cloned Agent based data computed in Homogeneous sensor networks"(IJCSIS) *International JournalComputer Science and Information Security*, **10**(9), pp. 136-140/2012
5. K.R.Sudha ,A.chandraSekhar ,Prasad Reddy P.V.G.D. Cryptography protection of Digital Signals using some recurrence relations" *International Journal of Computer Science and Network security*, 2007; **7**(5),203-207.
6. D.SravanKumar.Ch.SuneethaA.ChandraSekhar "Encryption of Data streams using Paul s spin ½ matrices", *International Journal of Engineering science and Technology.*, 2010; **2**(6), 2024 -2028.
7. E Logashanmugam, R Ramachandran "An Improved Algorithm for Image Compression Using Wavelets and Contrast Based Quantization Technique". *Information Technology Journal*, 2008.