ISSN No. 0976-5697

Volume 8, No. 6, July 2017 (Special Issue III)

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

NEW ENCRYPTION SCHEME USING FOURIER SINE AND COSINE TRANSFORMS AND FINITE STATE MACHINE

Sirivaram Srilakshmi
Lecturer, Department of Mathematics
J.N.T.U(A) College of Engineering
Ananthapuramu A.P.515001

Abstract Cryptography is the art and science of keeping message secure, has a long and fascinating history. Over the centuries, an elaborate set of protocols and mechanisms has been created to deal with information security issues, when the information is conveyed by physical documents. Often the objectives of information security cannot solely be achieved through mathematical algorithms and protocols alone, but require procedural techniques and abidance of laws to achieve the desired result.In mathematics the Fourier Sine and Cosine transforms are forms of the Fourier integral transform that do not use complex numbers. It is useful in many areas such as Signal processing statistics etc.Automata theory is the study of abstract computing devices or machines. In computer science we find many examples of finite state system and the theory of finite state systems, as a useful design tool for these systems. In the present paper an innovative technique for encrypting and hiding the data is proposed based on finite state machines and Fourier sine and cosine transformation. The efficacy of the proposed method is analysed, and the analysis shows an improved cryptographic protection in digital signals.

Key words Finite state machine, fourier transforms, Cryptography ,Moore machine, Modular Arithmetic

1. INTRODUCTION

All Today in the e-age, the need to protect communications from prying eyes is greater than ever before. Cryptography, the science of encryption plays a central role in mobile phone communication, e-commerce, pay-T.V., sending private e-mails, transmitting financial information and touches on many aspects of daily lives. Today's technology can be traced back to earliest ciphers, and have grown as a result of evolution. The initial ciphers were cracked, so new, stronger ciphers emerged. Code breakers set to work on these and eventually found flaws, forcing cryptographers to invent better ciphers. The significance of key is an enduring principle of cryptography. With the advent of the computer age, the mechanical encryption techniques were replaced with computer ciphers. Again each cipher depended on choosing a key known only by the sender and the receiver which defined how a particular message would be. This meant that there was a problem of getting the key to the receiver so that the message could be deciphered. This has to be done in advance, which was an expensive slow and risky process.

1.1 Cryptography

Cryptography refers to the art of protecting transmitted information from unauthorized interception or tampering. The other side of the coin, cryptanalysis, is the art of breaking such secret ciphers and reading the information, or perhaps replacing it with different information. It uses mathematical and logical principles to secure information. Encryption means the change of original information (plain text) into another form by some operations (algorithm) and decryption means the techniques of extracting the original information by some operation (algorithm) fromthe encrypted data (cipher text). In private key cryptography, the encryption and decryption on plaintext is done with the same key and key is known to the sender and receiver. Cryptography is well known and widely used in techniques that manipulate information in order to cipher or hide their existence. [1][2][3]

1.2 Finite State Machine

Automata theory is a key to software for verifying systems of all types that have a finite number of distinct states, such as communication protocols or protocol for secure exchange of information. In Moore Machine, every state of the finite state machine has a fixed output. [4][5] Mathematically Moore machine is a six- tuple machine and is defined as

M= ($Q, \sum, \Delta, \delta, \lambda', q_0$)

Q : A nonempty finite set of states in Moore machine

$\sum$: A nonempty finite set of inputs.

Δ : A nonempty finite set of outputs.

δ : It is a transition function which takes two arguments one is input state and another is input symbol. The output of this function is a single state.

λ' : Is a mapping function which maps Q x $\sum$ to Δ, giving the output associated with each transition.

CONFERENCE PAPER
National Conference dated 27-28 July 2017 on
Recent Advances in Graph Theory and its Applications (NCRAGTA2017)
Organized by Dept of Applied Mathematics
Sri Padmawati Mahila Vishvavidyalayam (Women's University) Tirupati, A.P.,

q_0 : is the initial state of Q

Moore machine can also be represented by transition table, as well as transition diagram.

Example

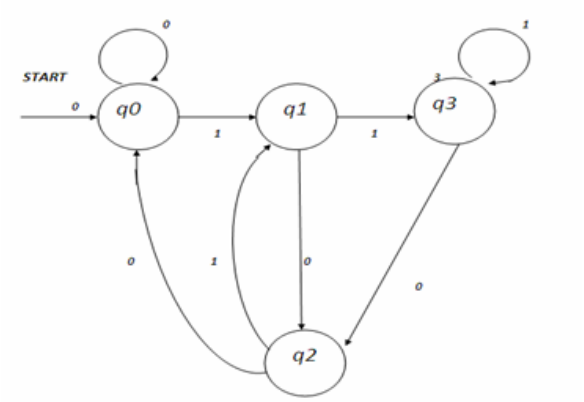

Figure 1 Moore machines which calculates residue of mod 4.

In this paper we use FSM in a different way [6].

1.3 Fourier Transforms

The Fourier transform is a tool that breaks a wave form (a Function or a signal) into alternate representation, characterized by sine and cosines. The Fourier transforms shows that any wave form can be rewritten
as sum of sinusoidal functions.
The Fourier Sine transform of f(t) ,some times denoted by

$$F_s(f(t)) = \int_0^\infty f(t)sinpxdx$$

Similarly we use cosine transform of f(t) as

$$F_c(f(t)) = \int_0^\infty f(t)cospxdx$$

In this paper we use Maclurin's series expansion of f(x) to convert given function of f(x).
We can also find inverse fourier transform also (sine or cosine)

2 Proposed method.

Whole class of cryptographic security systems which rely on transfer functions, are generally easy to compute, but it is very hard to find the inverse. That is if you have an extra piece of information, finding the inverse is easy as well.

3.ALGORITHM

Forward process

Step 1
Let M={m_1,m_2,…….m_n} be the plain text.
Step 2
Define Moor machine through public channel. Send secret key and private key to the receiver in binary form.
We allocate 0to A , 1 to B .....25 to Z
Consider a function f(t) and itsFourier sin or cosine transform . we know that Fourier sine or cosine transform of f(t) exists iff f(t) is continuous. Messages in integers are converted into coefficient of infinite series expansion of f(t) of variable order. Apply Fourier sin or cosine according to the power of x transformation on each block of messages and forward it to the Moore machine .
Step 3
Consider a block of secret key in binary form
cipher text at each block of message is message * out put of each state mod (26)
Step 4
Send the cipher text to the receiver.

Back ward process

Step 1
Let C be the cipher text in blocks .
Step 2
Use Moore machine, secret key and private key to decrypt the message using the definition of the cipher text at q(i-1)th stage.

4.PERFORMANCE OF THE PROPOSED ALGORITHM

Mathematical work

Algorithm proposed is based on ordinary multiplication using secret key and chosen finite state machine. The secrecy is maintained in secret key, private key and finite state machine. It is very difficult to break the cipher text without proper key and the chosen finite state machine. The number of element in the sequence S must be maximum to avoid the cipher attacks.

Security

It is very difficult to extract the original information, due secret key, private key .

Brute force attack on key is also difficult due to the increase in key size.

S.No	Name of the attack	Possibility of the attack	Remarks
1	Cipher text attack	Very difficult	Due to the secret key, private key and finite state machine.
2	Known plain text attack	Difficult	Due to the chosen finite state machine and secret key.
3	Chosen plain text attack	Difficult	Due to the chosen finite state machine and secret key.
4	Adaptive chosen plain text attack	Difficult	Due to the chosen finite state machine and secret key.
5	Chosen cipher text attack	Very difficult	Due to the secret key, private key and finite state machine.

CONFERENCE PAPER
National Conference dated 27-28 July 2017 on
Recent Advances in Graph Theory and its Applications (NCRAGTA2017)
Organized by Dept of Applied Mathematics
Sri Padmawati Mahila Vishvavidyalayam (Women's University) Tirupati, A.P.,

6	Adaptive chosen cipher text attack	Very difficult	Due to the secret key, private key and finite state machine.

Table 1 Security analysis

5.Conclusions

Algorithm proposed, is based on finite state machine and Fourier sine and cosine Transformation. Secrecy is maintained at three levels, the secret key, the chosen finite state machine, and the Fourier sine or cosine Transformations. The obtained cipher text becomes quite difficult to break or to extract the original information even if the algorithm is known.

REFERENCES

[1] A.Menezed, P.Van Oorschot and S.Vanstone Hand book of Applied Cryptography e-Book.

[2] Ciphers: http://en.wikipedia.org/wiki/Cipher

[3] W.Stallings; "Cryptography and Network Security" 2nd Edition, Prentice Hall, 1999 [22]. Bruce Schneier: Applied Piper, F "Encryption". Security and Detection, Ecos 97. European Conference;

[4] Adesh K.Pandey. Reprint 2009, "An introduction to automata theory and formal languages 'S.K.Kararia & sons. New Delhi.

[5] John E.Hopcroft, Rajeev Motwain, Jeffrey D.Ulman. "Introduction to automata theory, language, and computation" Vanstone3rd imp.

[6] B.Krishna Gandhi ,.A.Chandra Sekhar, S.Srilakshmi "Cryptographic scheme for digital signals using finite state machine" international journal of computer applications (September 2011)

CONFERENCE PAPER
National Conference dated 27-28 July 2017 on
Recent Advances in Graph Theory and its Applications (NCRAGTA2017)
Organized by Dept of Applied Mathematics
Sri Padmawati Mahila Vishvavidyalayam (Women's University) Tirupati, A.P.,