ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 6, Special Issue 13, July 2017

New Encryption Scheme Using Laplace Transforms and Finite State Machine

Sirivaram Srilakshmi

Lecturer, Department of Mathematics, J.N.T.U(A) College of Engineering, Ananthapuramu, India

ABSTRACT: The need to attain information security is critical and vital. Cryptography has been and stays behind the most proficient approach employed to achieve security. In general, it is based on repeated rounds of transformation that alter input plain text to encrypted text or cipher text output. Each round consists of several functions and always includes a depending on the round, secret key. Multiple rounds establish inverse transformation cipher text in to the original using the same secret key. The majority of the algorithms calculations are accomplished in finite fields.

In mathematics the Laplace transform is an integral transform which transforms real variable t to a complex variable s. It is useful in many areas such as circuit theory 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 Laplace transformation. The efficacy of the proposed method is analysed, and the analysis shows an improved cryptographic protection in digital signals.

KEYWORDS: Moore Machines, key, encryption, cipher text, Laplace transformation

I. INTRODUCTION

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 receivers so that the message could be deciphered. This had to be done in advance, which was an expensive slow and risky process.

A cryptanalyst can normally find the key but the approach of a combination of two prime numbers is used for encryption along with finite state machine in this paper.

II. LITERATURE REVIEW

2.1 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 getting the original information by some operation (algorithm) from the encrypted data (cipher text). In private key cryptography, the encryption and decryption on plaintext is one with the same key and key is

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 6, Special Issue 13, July 2017

known to the sender and receiver. Cryptography is well known and widely used techniques that manipulate information in order to cipher or hide their existence. [1][3]

2.2 Automata

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 of finite state machine has a fixed output. [2][4] 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 state 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.

q_0 : is the initial state of Q

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

Example

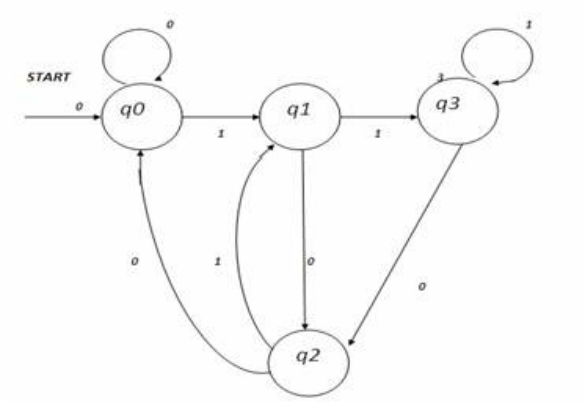

Figure 1 Moore machines which calculates residue mod 4.

2.3 Laplace Transormations

The Laplace transformation of f(t) is a function defined for all positive values of t, then the laplace transform of f(t) is defined as $L(f(t)) = \int_0^\infty f(t)e^{-st}dt = F(s)$

Provided the integral exists , where the parameter s is a real or complex number. We can also define inverse of laplace transform as f(t) =F^{-1}(F(s))

We know that Laplace transformation satisfies linearity property [5]

III.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.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 6, Special Issue 13, July 2017

We allocate 0to A , 1 to B .....25 to Z
Consider a function f(t) and its Laplace transform . we know that Laplace transform of f(t) exists iff f(t) is piece wise continuous and function of exponential order . Messages in integers are converted into coefficient of infinite series expansion of f(t) of variable order. Apply Laplace 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.

IV.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.

Time calculation

let 't_m 'be the time required for each multiplication of corresponding element in the sequence S or P. then total time required to convert the total n messages is $n^2 t_m$.

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

Table 1 Security analysis

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 6, Special Issue 13, July 2017

V. CONCLUSIONS

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

We can also increase the number of rounds if necessary.

REFERENCES

[1] B.Krishna Gandhi ,.A.Chandra Sekhar, S.Srilakshmi "Cryptographic scheme for digital signals using finite state machine" international journal of computer applications (September 2011)
[2] Adesh K.Pandey. Reprint 2009, "An introduction to automata theory and formal languages 'S.K.Kararia & sons. New Delhi.
[3] A.Menezed, P.Van Oorschot and S.Vanstone Hand book of Applied Cryptography e-Book.
[4] John E.Hopcroft, Rajeev Motwain, Jeffrey D.Ulman. "Introduction to automata theory, language, and computation" Vanstone3rd imp.
[5] G.Nagalakshmi,Ravi kumar B.and A.Chandra Sekhar "A cryptographic scheme of Laplace transformations " IJMA 2(12) ,2011,2515-2319.