International Journal For Technological Research In Engineering
Volume 4, Issue 1, September-2016 *ISSN (Online): 2347 - 4718*

ENHANCING RANDOM NUMBER GENERATION TECHNIQUE IN CRYPTOGRAPHY USING AUTOMATA

Pradeep Peter[1], Mr Manubhai Jha[2]
[1]M.Tech, [2]Asst Prof, UCER, Allahabad

ABSTRACT: In this paper we will discuss about the use of automaton over cryptography for the key management as randomness tool for key generation. In automaton we have a input string as input and it pass through different internal stages and provides a deterministic or nondeterministic output. Here we will use the automaton mechanism for generating secure random number for input for key generation in any cryptography methodology. In our ancient way of cryptography method we used random number generation technique as Lehmer's scheme and Blum Blum Shub Scheme. All this random number are generated for the unpredictability of key string in cryptography so by using automaton techniques we will use the random no in binary form and these random number in binary will then transformed by automaton mechanism. That output is then again converted in decimal form and new value of that number will be used for key generations. These new random numbers play an important role in the field of cryptography. The security and cryptography algorithm is based on the use of random numbers in

- ***Key generation protocol of RSA,***
- ***Key management/distribution of session keys,***
- ***Authentication schemes/digital signature schemes.***

Here we will be using transition diagram for our desired output of the given input.

I. INTRODUCTION

Automata used as the basic design of our computer, in computer science Automata refer to the study of abstract computing devices. An automaton has a mechanism to read input, which is a string over a given alphabet. This input is written on an "input file", which is a string over a given alphabet. Input files is divided into cells, each of which holds a symbol It defines how all inputs are transformed inside a machine into desired output.

Automaton has a control unit, which is said to be in one of a finite number of "internal stages". The automaton can change state in a defined way.

A deterministic automaton is one in which each moves is uniquely determined by the current configuration. If the internal state, input and contents of the storage are known, it is possible to predict the future behaviour of the automaton. This is said to be deterministic automaton otherwise it is nondeterministic automaton.

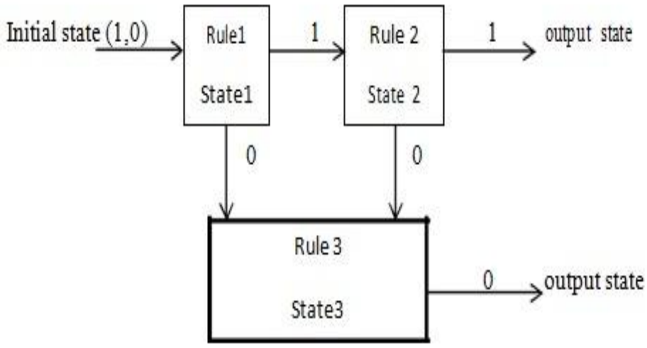
Cryptography is a science which is used in encryption and decryption of data. Cryptography enables you to store sensitive information or transmit it across insecure network (like internet) so that it cannot be read by anyone except the intended recipient. The term cryptography comes from Greek i.e. hidden- to- write.

Cryptography is a practice and study of hidden information. In modern times, cryptography is considered to be a branch of both mathematics and computer science. Cryptography is used in applications present in technologically advanced societies; example including the security of ATM cards, computer password, and electronic commerce, which all depend on cryptography.

Cipher designing using Automata

In automata we use a set of input string, number of states, initial stat, and transition function for moving from one state to another state such that the input string goes to a final state and provides us a desired output .Here automaton will increase the quality of keys used for designing cipher which is done by encryption using keys and those keys are generated by random numbers.

Fig:1



In cryptography we use random number generation for key generation. Random number generation is computational or physical device designed to generate sequence of numbers and different patterns. Similarly here we will use automaton methods for generating number patterns in defined manner but not exactly known. This will help us in increasing the efficiency of randomness and unpredictability of generated patterns. According to cryptography we need this kind of randomness for making our plane text encryption and decryption so confidential such that the generated cipher would be free from correlation attack and algebraic attack. In total through this paper the strength of generated cipher using key generation by automaton method enhanced. Automaton provides optimization in random number generation.

II. METHODOLOGY

Random number generation by Universal Turing Machine

The Universal Turing Machine can stimulate the behaviour of an arbitrary Turing Machine over any

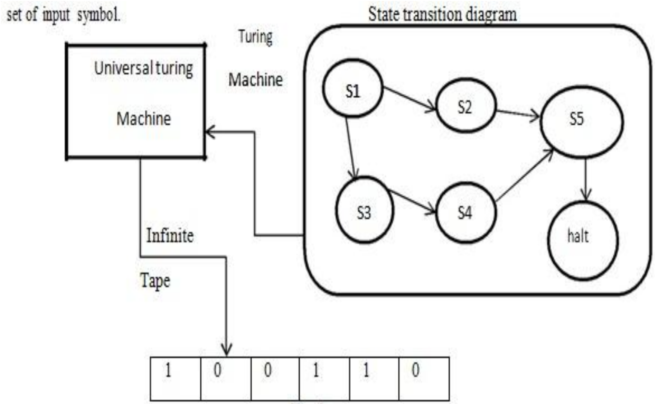


Fig:2

Any Universal Turing Machine can be programmed to carry out any calculation that can be performed by a human mathematician working with paper and pencil in accordance with some algebraic method. This is what is meant by calling this machine Universal Turing Machine.

Working of Universal Turing Machine

So here we will use the binary forms of all random sequence and those patterns are defined by the algorithm by which it has to be converted in a new random form in Universal Turing Machine and then plain text is XOR with the key stored in an array of automaton and using number of times to encapsulate the plaintext up to a secured level of layers den the reverse state transition will be the key to DE capsulate the cipher text into plain text. This process is as shown in figure:

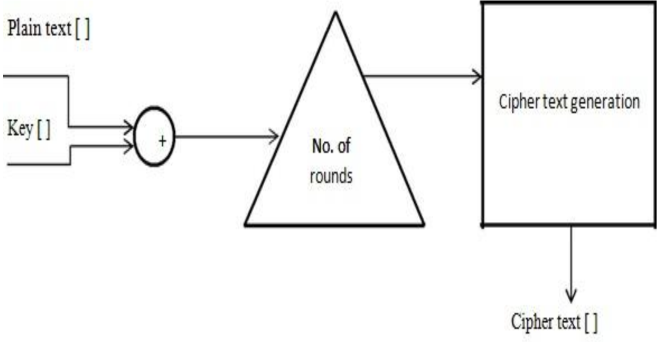


Fig:3

Implementation

- Plaintext [] : data to be converted into cipher text
- Key [] : key used for encryption process
- No of rounds for layered encryption
- Cipher text generation by any of algorithms of DES,RSA,AES
- The reverse algorithm in Turing machine with state transition table will help to decryption process of cipher text.

Future scope

Cryptography using automata will change the key management technique and enhance the quality or random number in key generation. This key generation can be implemented on all encryption and decryption of all protocols. Just providing the algorithm for designing the number of our chosen pattern.

III. CONCLUSION

As we have seen a Turing machine can change the technique for the random number generation such that the complexity can be increased much number of times and its reverse process with reverse algorithm will produce the input numbers as well.

REFERENCES

[1] On the complexity of pseudo-random sequences - or: If you can describe a sequence it can't be random.

[2] Undecidability of the Halting Problem for Recursively Enumerable Sets, World Journal of Applied Science and Technology, Vol. 2, No. 1, ISSN: 2141 – 3290, pp. 41-48. 3. Boolos, G. S. and Jeffrey, R. C. (1974).

[3] Minsky, M. (1967). Computation: Finite and Infinite Machines, Prentice-Hall, Inc., N. J., 1967. 16. Petrzold, G. (2008).

[4] In R. L. Rivest, A. Sherman, and D. Chaum, editors, Proc. CRYPTO 82, pages 61--78, New York, 1983. Plenum Press.

[5] The Annotated Turing: A Guided Tour through Alan Turing's Historic Paper on Computability and Turing Machines, Indianapolis, Indiana, Wiley Publisher 17. Radó, T. (1962).

[6] On Non-Computable Numbers, with an Application to the Etscheidungsproblem. In Proceedings of London Mathematical Society, Ser. 2 , Vol. 42, pp. 230-265. 18.

[7] Implementation of Recursive Enumerable Languages in Universal Turing Machine. Int'l journal of Computer Theory and Engineering, Vol. 3, No. 1, 1793-8201, pp. 153-157. 19. Turing, A. M. (1936).

[8] Unbiased bits from sources of weak randomness and probabilistic communication complexity. [9]In Proc. (26)th IEEE Symp. on Foundations of Comp. Science, pages 429-- 442, Portland, 1985. IEEE.

[9] Unbiased bits from sources of weak randomness and probabilistic communication complexity. SIAM J. Computing, 17(2):230--261, April 1988.

[10] Cryptographic randomness from air turbulence in disk drives. In Yvo G. Desmedt, editor, Proc. CRYPTO 94, pages 114--120. Springer, 1994. Lecture Notes in Computer Science No. 839.

[11] In J. Feigenbaum, editor, Proc. CRYPTO 91, page 300. Springer, 1992. Lecture Notes in Computer Science No. 576.