TWMS J. App. and Eng. Math. V.13, N.1, 2023, pp. 285-290

ENCRYPTION THROUGH SQUARE GRID AUTOMATA

F. R. P. MARY[1*], L. SHOBANA[1], R. SUJATHA[3], §

Abstract. In this paper, a new approach to encrypt and decrypt messages by implementing the concept of cordial words and cordial numbers to square grid automaton is being analyzed.

Keywords: Encryption, decryption, cordial words, cordial numbers.

AMS Subject Classification: 05C78, 68Q45.

1. Introduction

A method is explored to encrypt and decrypt messages by applying the idea of [2] cordial words and cordial numbers to a square grid automaton. Cryptography [7] is a technique of protecting information and communications through use of codes so that only the correct person for whom the information is intended can understand and process it. The process of encoding a plaintext into ciphertext in such a way that only authorized parties can access it is known as encryption. The procedure of converting ciphertext into its original form plaintext is decryption. There are many forms of ciphers namely affine, Hill, RSA, knapsack etc., amongst these, the cipher type used in our proposed method is affine cipher. Affine cipher[7] is defined as a monoalphabetic substitution cipher which is defined by a formula $C \equiv [aP + k] \pmod{26}$ where a is a positive integer less than $25(mod\ 26)$, C is the ciphertext represented by ordinal numbers, P is the plain text represented by ordinal numbers, k is an assigned constant and gcd (a, 26) = 1. The condition that gcd (a, 26) = 1 is taken to ensure that $C \equiv [aP + k] \pmod{26}$ has an unique solution for $P,\ P = \left[a^{-1}(C - k)\right] \pmod{26}$.
Different encryption techniques are used for promoting the information security. Relating to automata theory, any special graphical structures are given specific orientation and various automata are being studied in the literature.[3] Web automaton, grid automaton,

[1] Department of Mathematics, SRM Institute of Science and Technology. SRM Nagar, Kattankulathur-603 203 Kanchipuram, Chennai, Tamilnadu, India.
e-mail: maryf@srmist.edu.in; ORCID: https://orcid.org/0000-0002-1924-1926.
[*] Corresponding author.
e-mail: shobanal@srmist.edu.in; ORCID: https://orcid.org/0000-0002-6401-6533.
[2] Department of Mathematics, Sri Sivasubramaniya Nadar College of Engineering, Chennai 603110, India.
sujathar@ssn.edu.in; ORCID: https://orcid.org/0000-0002-3379-6776.
§ Manuscript received: December 14, 2020; accepted: March 7, 2021.

square grid automaton etc., are some of the kinds to name a few. Consider the path graph P_m on m vertices $u_1, u_2, ..., u_m$ and P_n the path graph on n vertices $v_1, v_2, ..., v_n$ which can be labeled in a particular way as $(u_1, v_1), (u_2, v_2), ...\ (u_m, v_n)$. A new automaton called Grid automaton is described by introducing orientations and labels for edges as in the Figure below. In our technique, we make use of the square grid automata. Among the

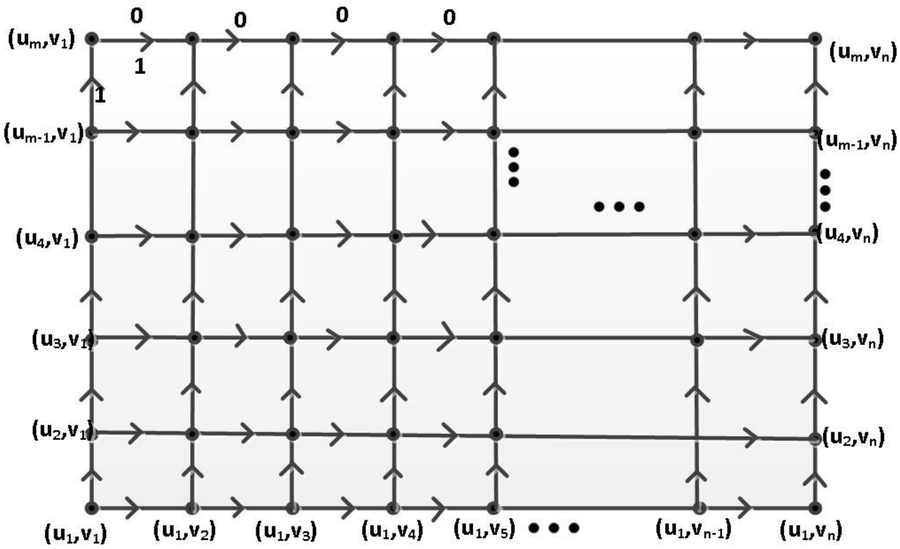

FIGURE 1. $P_n X P_m$ **- Grid Automaton**

words generated over the square grid automaton a characterized form is given to a set of words derived from the concept of cordial labeling. The set of all strings over $\sum = \{0, 1\}$ beginning with one, in which the number of zeros and the number of ones differ at most by one is said to be cordial word. In other words, a word w over the alphabet $\sum$ is said to be cordial word, if $|\eta_0 - \eta_1| \leq 1$ where η_0 is the number of zeros in w and η_1 is the number of ones in w. Cordial language is the language that consists only cordial words. The decimal form of any cordial word over $\{0, 1\}$ is said to be cordial number.
In this paper, an approach to encrypt and decrypt confidential messages by applying the principle to square grid automaton by generating cordial words and cordial numbers is studied.

2. MAIN RESULTS

In this section, a new concept is introduced to encrypt the message using a square grid graph $P_n \times P_n, n \geq 2$. In this grid, movements are characterized by a series of rightward and upward moves from one vertex to the other vertex. A step is recognized as an edge and is labeled with an upward movement label one and a horizontal right movement zero. This approach could be done in several methods, and from each such path its path labels are regarded as a string over zeros and ones. A language L constitutes a set of all such path labels or strings. The count of words [3] in the language L identified by P_m X P_n grid automaton is represented by $|L| = \left[\dfrac{(m+n-2)!}{[(m-1)(n-1)!]}\right]$. In a square grid automaton the possible words generated will be $\left[\dfrac{(2n-2)!}{[(n-1)!]^2}\right]$. According to the notion of cordial words the count of words will become $\dfrac{1}{2}\left[\dfrac{(2n-2)!}{[(n-1)!]^2}\right]$. The total number of possible cordial words are converted to cordial numbers and choose the least cordial number denoted by a which suffices the greatest common divisor condition that a and 26 is one. Finding out the appropriate cordial word and corresponding cordial number by using the congruence relation $C \equiv [aP + k] \pmod{26}$ where a is the cordial number of the respective cordial word and k equals n, the sequence of encrypted numbers are obtained. Among these cordial words a private key a is chosen by the sender which has to be provided to the receiver to decode the message. Translate the encrypted numbers to encrypted message using the normal chart ie., assign numbers from 00 to 25 for alphabets from A to Z. The encrypted message is separated using five in a block and rearranged to arrive at a meaningful message. The encrypted message can be solved using the congruence relation $P \equiv \left[a^{-1}(C-k)\right] \pmod{26}$ to get the decrypted message.

2.1. **Working Algorithm for Encrypting Message. Input:** The original message M and a square grid graph $P_n \times P_n, n \geq 2$
Output: The encrypted message E

- **Step 1:** Convert the original message M to its ordinal numbers by the use of normal chart. Denote it by P.
- **Step 2:** Construct the square grid automaton with the provided dimension n and generate $\dfrac{1}{2}\left[\dfrac{(2n-2)!}{[(n-1)!]^2}\right]$ cordial words.
- **Step 3:** Choose the least cordial number modulo 26 denoted by a which suffices the relation gcd(a,26)=1 and also k equals n.
- **Step 4:**
Enumerate

$$C \equiv [aP + k] \pmod{26} \tag{1}$$

- **Step 5:** From the above congruence relation estimates the encrypted numbers as C and convert it to their corresponding alphabets from the normal chart.

2.2. **Working Algorithm for Decrypting Message. Input:** The received encrypted message E
Output: The original message M

- **Step 1:** Convert the received encrypted message to ordinal numbers using a normal chart.
- **Step 2:** From equation (1) obtain $P \equiv \left[a^{-1}(C-k)\right] \pmod{26}$.
- **Step 3:** Solving for P for the varying values of C, equivalence classes can be obtained for a particular value of C. Maintaining the order a finite number of solutions are acquired. Amongst them assign the initial solution to P.
- **Step 4:** The obtained numerical values as solutions are converted to the ordinal numbers by using a normal chart where the original message is decrypted.

3. Representation for Encryption and Decryption

3.1. **Encryption. Input:** The original message MAKER EADYF ORATT ACK and a square grid $P_6 \times P_6$
Output: The encrypted message MGYIV IGBSP AVGJJ GUY

- Convert the given message to its ordinal numbers 12, 00, 10, 04, 17, 04, 00, 03, 24, 05, 14, 17, 00, 19, 19, 00, 02, 10. Let the sequence of numbers be represented by P.
- The grid automata $P_6 \times P_6$ for the path graph and choosing the cordial word as $(u_1, v_1), (u_2, v_1), (u_2, v_2), (u_2, v_3), ... (u_2, v_6), (u_3, v_6), (u_4, v_6), ..., (u_6, v_6)$. The chosen cordial number satisfying the relation gcd (a,26) = 1 is 7.

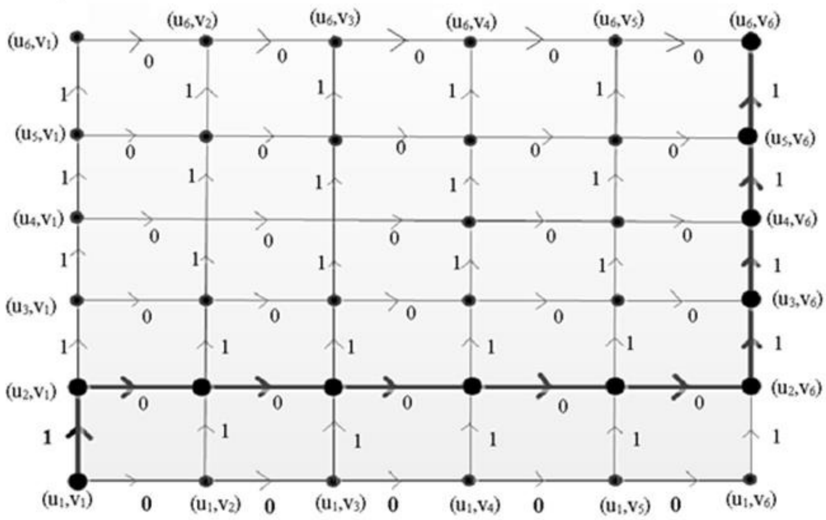

FIGURE 2. P_6XP_6 **- Square Grid Automaton**

- Compute $C \equiv (7P + 6) mod 26$.
- Obtain the sequence 12, 06, 24, 08, 21, 08, 06, 01, 18, 15, 00, 21, 06, 09, 09, 06, 20, 24.
- The encrypted numbers converted using the normal chart is MGYIV IGBSP AVGJJ GUY.

3.2. **Decryption. Input:** The received encrypted MGYIV IGBSP AVGJJ GUY
Output: The decrypted message MAKER EADYF ORATT ACK

- Convert the received encrypted MGYIV IGBSP AVGJJ GUY by using normal chart as 12, 06, 24, 08, 21, 08, 06, 01, 18, 15, 00, 21, 06, 09, 09, 06, 20, 24 denoted by C
- Solve the equation

$$7P \equiv (C - k)\text{mod } 26 \tag{2}$$

by varying the values of C, retaining the order.

- For every value of C, obtain the finite number of solutions for P.
  Among them, assign the initial solution to P.
  For example let for
  (i) $C = 12$ substituting in (2),
  $$7P \equiv (12 - 6)\text{mod } 26 \tag{3}$$
  By solving for P, $P = 12$ is obtained.
  (ii) $C = 06$ substituting in (2),
  $$7P \equiv (6 - 6)\text{mod } 26 \tag{4}$$
  By solving for P, $P = 00$ is obtained.
  Proceeding in the same manner for the sequence with respect to C, obtain the sequence P.
- Convert the sequence of numbers 12, 00, 10, 04, 17, 04, 00, 03, 24, 05, 14, 17, 00, 19, 19, 00, 02, 10 obtained in to its corresponding letters by using normal chart.
- MAKER EADYF ORATT ACK which is the required original message.

4. Observations

Among the possibilities of $\frac{1}{2}\left[\frac{(2n-2)!}{[(n-1)!]^2}\right]$ cordial words generated by the grid automaton and the number of vertices n there are numerous ways to develop the affine ciphers for the congruence relation $C \equiv [aP + k]$ (mod 26). Alternating the values one can find various ways to encrypt and decrypt messages satisfying the greatest common divisor relation, gcd (a, 26) = 1.

5. Conclusions

There are numerous techniques to encrypt and decrypt confidential messages. In this paper, a new approach to encrypt and decrypt messages through cordial words is investigated which is efficient in transferring confidential messages in various fields.
Our future scope of work is to assign different equivalents in affine ciphers and develop strong congruence relations for encryption and decryption which can be used in real time scenario like military and network communications.

References

[1] Cahit, I., (1987). Cordial graphs: a weaker version of graceful and harmonious graphs, Ars Combin, 23, pp. 201-207.

[2] Baskar Babujee J., Shobana L., (2012). Cordial languages and Cordial Numbers, Journal of Applied Computer Science and Mathematics, 13(6), pp 9-12.

[3] Baskar Babujee J. and Julie J., (2011). Special Automata from Graph Structures, Proceedings of the International Conference on Mathematics and Computer Science, Loyola College Science, pp. 135-137.

[4] Hopcroft, J. E., Motwani R. and Ullman, J. D., (2007). Intoduction to Automata Theory, Languages and Computation, $3_r d$ Edition, Pearson Education, Inc.

[5] Remigius Perpetua Mary F. and Shobana L., (2019). On Cordial Labeling of Double Duplication of Rhombic Grid Graph, Journal of Advanced Research in Dynamical and Control Systems, 11(5), pp 1-6.

[6] Shobana L., Baskar Babujee J. and Cangul, I. N., (2019). A New Cryptographic Method by means of Molecular Graphs, Proceedings of the Jangjeon Mathematical Soceity, 23(4), pp 503-507.

[7] Kohsy,T, (2007). Elementary Number Theory with Applications, Second Edition, Academic Press, Elsevier.

Francis Remigius Perpetua Mary received her M.Sc degree (2010) from Bharathidasan University, Tiruchirapalli, India and M.Phil degree (2011) in Mathematics from Madras University, Chennai, India. She is working as an assistant professor, Department of Mathematics, SRM Institute of Science and Technology, India. Her research of interest are in the area of applied mathematics which includes graph theory and its application.

Loganathan Shobana received her Ph.D degree in 2013 in Mathematics (Graph Theory) at Anna University, India. Presently she is working as an assistant professor (Sr.G), Department of Mathematics, SRM Institute of Science and Technology, India. Her current research areas includes number theory and cryptography.

Ramalingam Sujatha is an associate professor in the Department of Mathematics, SSN College of Engineering, Chennai. She has received her MSc and Ph.D. from IITM. She is a recognized guide for Ph.D. in Anna University, Chennai. Her research interests are Hidden Markov models, software reliability and fuzzy theory.