Advances and Applications in Mathematical Sciences
Volume 20, Issue 9, July 2021, Pages 1645-1654
© 2021 Mili Publications

A SYMMETRIC KEY CRYPTOSYSTEM BASED ON GRAPHICAL REPRESENTATION OF LETTERS

R. ABRAHAM DINESH and D. JAYASEELAN SAMUEL

Department of Mathematics
Madras Christian College
Tambaram, Chennai-600059, India
E-mail: abraham.mathed@gmail.com
jayaseelansamuel@mcc.edu.in

Abstract

Every letter in English alphabet can be considered as graphs. Using an algorithm, each of these graphs are transformed into another graph. These transformed graphs exhibit certain properties. From each of these transformed graphs a pair of numbers is obtained. These pairs of numbers form the key for the proposed symmetric key cryptosystem. In this paper, the encryption and decryption algorithms are presented along with simple illustrative examples.

1. Introduction

Cryptography is the science of keeping the secrets secret. Message encryption and decryption are the main focus of cryptography. These encryption and decryption techniques are mostly based on different problems of Mathematics. There are many cryptosystems based on number theory [3, 9], formal languages and automata theory [1, 4, 5, 7], biological computing [10, 11] and elliptic curves [6, 8]. Graph theory is one of the well-established topics in Mathematics. But there are very few cryptosystems based on graph theory [2, 12] compared to other topics in Mathematics.

In this paper, we focus on developing cryptosystems using graphs. Here, we consider each English letter as a graph. Using a transformation algorithm, each of these graphs is transformed into another graph called transformed graph. Then we represent each of these transformed graphs as a

2010 Mathematics Subject Classification: 30C45.
Keywords: Symmetric key cryptosystem, Key generation, Encryption, Decryption, Graph.
Received February 21, 2020; Accepted May 8, 2020

unique tuple. That is, each letter in the English alphabet is mapped into a tuple by using a transformation algorithm. These tuples are used as the key for the proposed symmetric key cryptosystem.

2. Key Generation Algorithm

Here, we consider a specific style of English alphabets as graphs. Each of these graph is partitioned into two or three parts. If a graph is divided into three parts, then we call them as the left partition (L), the right partition (R) and the partition in the middle (M). If a graph is divided into two parts, then we consider the middle partition empty. For example, in Figure 1, for the letter E, the left partition L contains a set of vertices $\{1, 6, 7\}$ and the right partition R contains a set of vertices $\{2, 3, 4, 5\}$ that are joined by edges passing over between these partitions. The graph of the alphabet I has three partitions $L = \{1, 6\}$, $M = \{2, 5\}$ and $R = \{3, 4\}$. Similarly, in the graph of G, there are two partitions $L = \{3, 4\}$ and $R = \{1, 2\}$.

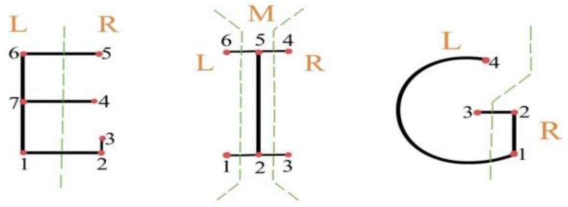


Figure 1

2.1. The Transformation Algorithm

The following algorithm will produce a transformed graph for each letter in the English alphabet.

Algorithm 1.

1. Start naming the vertices of the alphabet from the vertex at the south-west corner resulting in a sequence of vertices $1, 2, 3, \ldots, n$. (If there is no vertex at the south-west corner then the vertex on the right to it is taken.)

2. For each vertex of the alphabet, draw an edge one below the other. As edges are drawn, vertices are also formed.

3. Divide the graph that is being created into two equal halves, for convenience.

4. If there is an edge between the vertices i and j where both i and j lie in the partition L or R of the graph of the alphabet, then draw an edge from the edge that corresponds to i to the edge that corresponds to j, from the left or right end respectively.

5. If there is an edge between the vertices i and j where both are present in the partition M, then draw an edge that joins the corresponding edges of i and j. In this case the edge is drawn in the middle of the graph that is being created and is slightly curved towards the right.

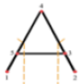
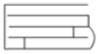
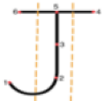
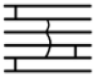
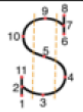
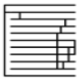
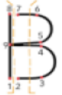
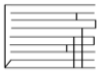
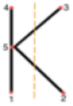
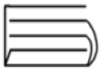
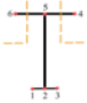
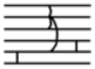
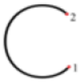
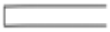
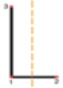
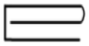
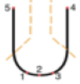
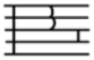
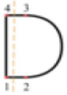
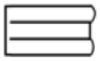
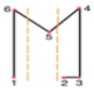
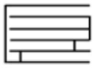
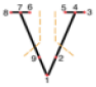
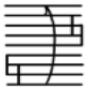
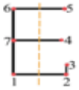
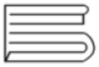
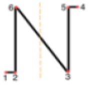
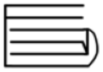
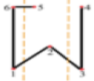
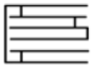
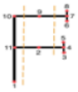
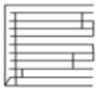
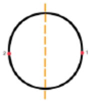
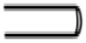
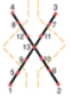
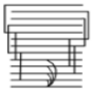
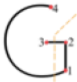
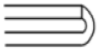
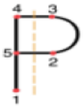
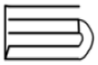
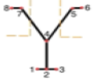
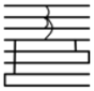
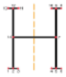
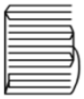
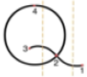
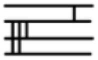
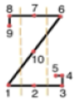
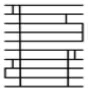
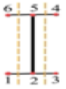
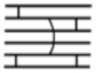
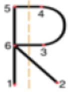
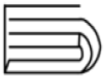
6. If there is an edge between the vertices i and j where one lies in the partition L of the graph of the alphabet and the other in the partition M, then draw an edge that joins the corresponding edges of i and j in the graph, lying within the left half but not on the end of this graph.

7. If there is an edge between the vertices i and j where one lies in the partition R of the graph of the alphabet and the other in the partition M, then draw an edge that joins the corresponding edges of i and j in the graph, lying within the right half of this graph.

8. If there is an edge between the vertices i and j where one lies in the partition R and the other in the partition L, then draw an edge from the right corner of the edge that corresponds to i to the right corner of the edge that corresponds to j where these edges are slightly curved towards the right.

9. If there is only one vertex in the graph of the alphabet, then draw a parallel from one of the vertices.

Table 1.

Alphabets	Transformed Graphs	Alphabets	Transform ed Graphs	Alphabets	Transformed Graphs
					
					
					
					
					
					
					
					
					

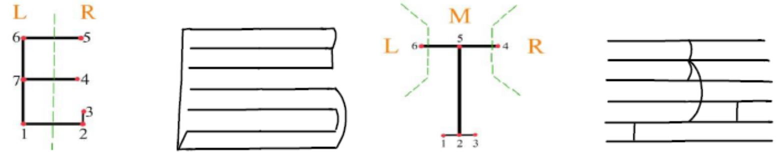


Figure 2.

Example 2.1. Consider the letter E as a graph given in Figure $2(a)$ This graph is partition into two parts $L = \{1, 6, 7\}$ and $R = \{2, 3, 4, 5\}$. There are seven vertices in this graph, so we draw seven edges one below the other. Since there are edges $(1, 7)$ and $(7, 6)$ from L to L and an edge (2, 3) from R to R of the graph in Figure $2(a)$, the corresponding edges are connected by new edges in the new graph. Now, since there are three edges (1, 2), (7, 4) and (6, 5) between the partitions L and R in the graph in Figure $2(a)$, the corresponding edges are also connected by new edges in the new graph as per the algorithm. The resulting transformed graph is given in Figure $2(b)$. Similarly, the letter T in Figure 2(c) is divided into three parts $L = \{6\}$, $R = \{4\}$ and $M = \{1, 2, 3, 5\}$ and the resulting transformed graph is given in Figure $2(d)$.

A complete list of transformed graphs for each English alphabet is given in Table 1.

2.2. Key Generation from the Transformed Graph

Now let us consider the number of vertices and number of edges of each of the transformed graph. Let V and E be the vertex set and the edge set of any transformed graph and $|V|$ and $|E|$ denote the cardinality of V and E respectively. Consider the tuple $(|V|, |E|)$ of each transformed graph. For example, The number of vertices in the transformed graph of W is 18 and the number of edges is 17. Thus $(|V|, |E|) = (18, 17)$ for the letter W. Note that, there is a one-to-one correspondence between each tuple and each transformed graph. The complete set of letters and the corresponding tuples are given in Table 2.

This table of tuples is used as the key in the proposed symmetric key cryptosystem. Since this is a symmetric key cryptosystem, this key must be available for both the sender and receiver and must be kept away from the third party. In all the 26 tuples in Table 2, note that $|V| \geq |E|$. This property helps us to decrypt the encrypted messages.

3. Encryption and Decryption

Table 2.

SI. No	Alphabet	Tuple
1	A	(14, 14)
2	B	(26, 25)
3	C	(4, 3)
4	D	(8, 8)
5	E	(14, 13)
6	F	(30, 29)
7	G	(8, 7)
8	H	(28, 27)
9	I	(22, 21)
10	J	(21, 20)
11	K	(10, 9)
12	L	(6, 5)
13	M	(16, 15)
14	N	(12, 11)
15	O	(4, 4)
16	P	(10, 10)
17	Q	(16, 16)
18	R	(12, 12)
19	S	(34, 33)
20	T	(20, 19)
21	U	(17, 16)
22	V	(25, 24)
23	W	(18, 17)
24	X	(39, 38)
25	Y	(24, 23)
26	Z	(32, 31)

Encryption Algorithm

1. Replace each letter in the plaintext with the tuple from the key table.

2. Remove brackets and commas and concatenate all of them to form a number sequence.

3. Form a table with fixed k columns and arbitrary (required) number of rows by filling one digit of the number sequence in each cell, row wise. This number k must be known to both sender and receiver and so it a part of the secret key.

4. Form a new number sequence by reading the table column wise.

This new number sequence is the corresponding ciphertext.

The sender of the message will send this ciphertext to the receiver. To decrypt the message, the receiver will follow the following steps.

Decryption Algorithm

1. Form a table with fixed k rows and arbitrary (required) number of columns by filling one digit of the number sequence in each cell, column wise.

2. Form a new number sequence by reading the table by row wise.

3. Construct the tuples from the number sequence.

4. Replace tuples with the corresponding letters from Table 2.

This is the required plaintext.

Table 3.

1	4	1	4	6	5	2	2	2	1
4	3	1	4	1	3	0	0	0	0
3	4	3	3	1	4	1	3	1	2
1	1	8	8	3	4	3	3	0	0
1	4	1	4	0	0	0	0	0	0
1	6	1	5	1	4	1	3	3	4
3	3	3	4	3	3	1	4	1	4
8	7	1	4	1	3	0	0	0	0

We construct the tuples from the new number sequence by using the following simple procedure. Consider the first letters, say ab, of the new number sequence. Suppose that a is numerically equal or greater than b, then check the key table. These two letters make the tuple (a, b). If not, then the letter b is concatenated to a and they are taken as one number say $u = ab$. This number u is compared to the third letter c of the number sequence. If u is equal or numerically greater than c and the tuple (u, c) is present in the key table, then (u, c) is the corresponding tuple. Otherwise the fourth letter d is concatenated to c to form the number $v = cd$ and the pair (u, v) is the corresponding tuple. This procedure is repeated by considering the remaining letters of the number sequence till the end.

4. Example Consider the plaintext: ALICE SENDS A MESSAGE.

Encryption. The corresponding tuples from Table 2 are: (14, 14), (6, 5), (22, 21), (4, 3), (14, 13), (34, 33), (14, 13), (12, 11), (8, 8), (34, 33), (14, 14), (16, 15), (14, 13), (34, 33), (34, 33), (14, 14), (8, 7), (14, 13). Removing all the brackets and commas and concatenating them we obtain: 1414652221431413343314131211883433141416151413343334331414871413 Filling them row-wise in a table with $k = 10$ columns, we obtain Table 3.

Here, note that the remaining cells in the table are filled with a filler character 0. Now, reading them in column-wise we obtain the ciphertext.

$c =$ 1414311138434146371138113144384544611301315344433201301102 03303402010 031010200440.

Decryption

To decrypt the ciphertext c, first form a table with $k = 10$ columns and a required number of rows by filling each letter of the ciphertext in each cell column-wise. We obtain the same table given in Table 3. By reading this table row-wise, we obtain a new sequence

1414652221431413343314131211883433141416151413343334331414871 413.

Now consider the first two letters 1 and 4 of the sequence. 1 is not greater than 4. Therefore, we concatenate a and 4 and obtain 14 and compare it with the next letter. The next letter is 1. Here $14 > 1$, but there is no tuple (14, 1) in Table 2. Hence, the next number 4 is concatenated with 1 to form the number 14. This results the tuple $(14, 14)$ and this corresponds to the alphabet ‘A’. Therefore the first letter of the plaintext is A.

The first four elements in the sequence are processed so we move to the next elements of the number sequence. The next two elements are 6 and 5. Since $6 > 5$ and $(6, 5)$ is present in Table 2 and corresponds to the alphabet ‘L’, the next letter of the plaintext is L. Similarly, the other letters are also formed and the message “ALICE SENDS A MESSAGE” was found.

5. Conclusion

In this paper, a new symmetric key cryptosystem which uses the graphical representation of English alphabet was proposed. This cryptosystem is easy to implement but before implementing a complete study of security analysis is needed. This can be considered for further research.

References

[1] A. Clarridge and K. Salomaa, A Cryptosystem Based on Composition of Reversible Cellular Automata, In: A. H. Dediu, A. M. Ionescu and C. Martín-Vide (eds) Language and Automata Theory and Applications (LATA 2009), Lecture Notes in Computer Science 5457 (2009), 314-325.

[2] A. Costache, B. Feigon, K. Lauter, M. Massierer and A. Puskás, Ramanujan Graphs in Cryptography, In: J. Balakrishnan, A. Folsom, M. Lalín and M. Manes (eds.), Research Directions in Number Theory, Association for Women in Mathematics Series Springer, Cham 19 (2019), 1-40.

[3] T. ElGamal, A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms, IEEE Transactions on Information Theory, IT-31(4) (1985), 469-472.

[4] D. Jayaseelan Samuel and P. J. Abisha, A Block Cipher based on Shuffle and θ-Deletion on Trajectories, International Journal of Pure and Applied Mathematics 113(10) (2017), 226-234.

[5] D. Jayaseelan Samuel and P. J. Abisha, A Novel Cryptosystem based on Cooperating Distributed Grammar Systems, International Journal of Artificial Intelligence and Soft Computing (IJAISC) 6(3) (2017), 174-186.

[6] V. Miller, Uses of Elliptic curves in Cryptography, In Crypto ’85, LNCS218 (1986), 417-426.

[7] G. Khaleel, S. Turaev and T. Zhukabayeva, A Novel Stream Cipher Based on Nondeterministic Fiinite Automata, Proceedings of Information Technologies in Science, Management, Social Sphere and Medicine (2016), 110-115.

[8] N. Koblitz, Elliptic Curve Cryptosystems, Mathematics of Computation 48(177) (1987), 203-209.

[9] R. Rivest, A. Shamir and L. Adleman, A Method for obtaining digital Signature and Public Key Cryptosystems, Communications of ACM 21(2) (1998), 120-126.

[10] J. Urias, E. Ugalde and G. Salazar, A cryptosystem based on cellular automata, Chaos 8(4) (1998), 819-822.

[11] A. A. Ubdo, S. Lian, I. A. Ismail, M. Amin and H. Diab, A Cryptosystem Based on Elementary Cellular Automata, Communications in Nonlinear Science and Numerical Simulations 18(1) (2103), 136-147.

[12] M. Yamuna, M. Gogia, A. Sikka and Md. J. H. Khan, Encryption Using Graph Theory and Linear Algebra, International Journal of Computer Application 5(2) (2012), 102-107.