Secret Information Sharing Using Probability and Bilinear Transformation

Kala Raja Mohan, Suresh Rasappan, Regan Murugesan, Sathish Kumar Kumaravel, and Ahmed A. Elngar

Abstract Information security is very much important in this Internet world, especially in electronic communications such as system security, smart card, mobile communications. Cryptography is based on transformation of multiple rounds of transformation of messages in the form of plain text as input into encrypted text message. Through suitable mathematical technique, secrecy of the information is maintained. This paper proposes a cryptographic technique using probability and bilinear transformation for encryption and decryption of a message. The algorithm for encryption and decryption is given. The probability concept is employed to secure the key between the communicator and recipient. The methodologies are used to get a safe communication between communicator and recipient. The bilinear transformation gives more secure for the process in key transformation. The bilinear transformation is used to encrypt the message. The inverse bilinear transformation is used to decrypt the message. The example is presented to validate the theory part.

Keywords Cryptography · Data encryption · Decryption · Bilinear transformation · Probability

K. R. Mohan (✉) · R. Murugesan · S. K. Kumaravel
Department of Mathematics, Vel Tech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology, Avadi, Chennai, Tamilnadu 600062, India
e-mail: kalamohan24@yahoo.co.in

S. Rasappan
Department of Mathematics, University of Technology and Applied Sciences-Ibri, Ibri, Sultanate of Oman 466, 516

A. A. Elngar
Faculty of Computers and Artificial Intelligence, Beni-Suef University, Beni-Suef City, Egypt

© The Author(s), under exclusive license to Springer Nature Singapore Pte Ltd. 2022

S.-L. Peng et al. (eds.), *Proceedings of 2nd International Conference on Mathematical Modeling and Computational Science*, Advances in Intelligent Systems and Computing 1422, https://doi.org/10.1007/978-981-19-0182-9_12

1 Introduction

In Universe, computer networks, Internet and mobile communications are more important and unavoidable part of our society, so that information security is obviously required to protect from hackers. One of the widely used approaches for information security is cryptography [1–4]. The mathematics of encryption, plays a major role in many fields. The main goal of cryptography is to ensure the secret communication between two individuals. Encryption is the process of obscuring information to make it unreadable without special knowledge.

A new cryptographic technique applying probability and bilinear transformation is carried out. Bilinear transformation find its application in many fields. In cryptography also, it plays a significant role [5–10]. The concept of probability is included in this method, which acts as a secured key between the sender and the receiver.

In this paper, Sect. 2 describes the standard definitions applied in this crypto analysis. Section 3 presents the algorithm for encryption. Section 4 demonstrates the algorithm for decryption [11–13]. The coding table applied for this cryptographic analysis is given in Sect. 5. Encryption process explained in Sect. 3 is demonstrated with an example in Sect. 6. Section 7 demonstrates the decryption process given in Sect. 4 with an example. Section 8 is about the conclusion followed by references.

2 Standard Definitions

The following standard definitions are applied in the cryptographic analysis in this paper.

2.1 Plain Text: Plain text is the data which can be directly read by any person. It is the information which has to be shared secretly to the receiver.

2.2 Cipher Text: The transformed form of plain text, which can be read only using the key specified by the sender is called the cipher text [14, 15].

2.3 Cipher: Cipher refers to the algorithm through which the plain text is transformed to cipher text.

2.4 Encryption: Encryption is the process in which the given information is converted into secret message. This hides the original information reaching unauthorized persons, using the secret key.

2.5 Decryption: Decryption is the reverse process of encryption. This is the process in which the encrypted text gets converted into original text with the usage of the secret key.

2.6 Bilinear Transformation: Bilinear transformation is given by $T = \frac{a_1 B + a_2}{a_3 B + a_4} T = \frac{a_1 B + a_2}{a_3 B + a_4}$. This is applied in the encryption process of this paper.

2.7 Inverse Bilinear Transformation: Inverse bilinear transformation is given by $B = \frac{a_2 - a_4 T}{a_3 T - a_1} . B = \frac{a_2 - a_4 T}{a_3 T - a_1}$. Decryption process of this process uses this inverse transformation.

2.8 Modulo Operator: The modulo operator gives the remainder value when one number is divided by another number.

2.9 Probability: Probability of the event is the chance of the event to happen.

$$\text{Probability} = \frac{\text{number of favourable outcomes}}{\text{total number of outcomes}}$$

The concept of probability is applied in framing the bilinear transformation in this paper.

3 Collection of Raw Data

The step by step procedure to be followed in encryption are as follows.

Step 1: Assign numerical values to alphabets, space and full stop.
Step 2: Apply Bilinear Transformation $T = \frac{a_1B+a_2}{a_3B+a_4}.T = \frac{a_1B+a_2}{a_3B+a_4}$. Here, $a_1, a_2, a_3a_1, a_2, a_3$ and a_4a_4 are chosen using probability method. It can be chosen based on the willingness of both the sender and the receiver which can help to maintain secrecy.
Step 3: To each numerical value in step 1, find its equivalent T value.
Step 4:Multiply the values of T by 100,000.
Step 5: To the values in obtained in step 4, find modulo 54 and its equivalent key values $K_n.K_n$.
Step 6: Cipher text is obtained from the equivalent encrypted codes of values in step 5.

4 Algorithm for Decryption

Decryption is the reverse process of encryption. In this stage the cipher text gets converted to plain text. The process of decryption has the following steps to be performed.

The step by step procedure to be followed in encryption are as follows.

Step 1: Using each values of key K_nK_n and the corresponding values of K_n, K_n, are obtained.
Step 2: $q_n = K_n * 54 + E_nq_n = K_n * 54 + E_n$
Step 3: Divide each q_nq_n by 100,000.
Step 4: Inverse Bilinear Transformation $B = \frac{a_2-a_4T}{a_3T-a_1}.B = \frac{a_2-a_4T}{a_3T-a_1}$.
Step 5: With the help of the coding table, the plain text is obtained from the values of $B.B$.

5 Coding Table Used for Cyptographic Analysis

A	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**	**N**	**O**	**P**	**Q**	**R**
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
S	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**	**a**	**b**	**c**	**d**	**e**	**f**	**g**	**h**	**i**	**j**
19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36
k	**l**	**m**	**n**	**o**	**p**	**q**	**r**	**s**	**T**	**u**	**v**	**w**	**x**	**y**	**Z**	**Space**	**Full Stop**
37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	0

6 Encryption—Worked Example

The encryption process applied here is explained using the word 'Mathematics'.

Step 1: To each letter of the word 'Mathematics' the corresponding code is obtained using the code table mentioned in Sect. 5.

M	a	t	h	e	m	a	t	i	c	s	
13	27	46	34	31	39	27	46	35	29	45	0

Step 2: For choosing the values of $a_1, a_2, a_3a_1, a_2, a_3$ and a_4a_4, the method of probability is applied.

In this example, the experiment of tossing two coins is considered. The possible outcomes are as follows:

$$S = \{HH, TT, HT, TH\} S = \{HH, TT, HT, TH\}$$

The values of $a_1, a_2, \ a_3a_1, a_2, \ a_3$ and a_4a_4 are chosen as follows:

$$a_1 = \text{the probability of getting 1 head} = \frac{2}{4} = 0.5$$

$$a_2 = \text{the probability of getting 2 head} = \frac{1}{4} = 0.25$$

$$a_3 = \text{the probability of getting no head} = \frac{1}{4} = 0.25$$

$$a_4 = \text{the probability of getting atleast 1 head} = \frac{3}{4} = 0.75$$

Thus, TT is obtained as,

$$T = \frac{0.5B + 0.25}{0.25B + 0.75} T = \frac{0.5B + 0.25}{0.25B + 0.75}$$

Step 3: Assuming the values obtained in step 1 as BB, the values of TT are obtained and listed in the following table.

B	**13**	**27**	**46**	**34**	**31**	**39**
T	1.6875	1.83333	1.89796	1.86486	1.85294	1.88095
B	**27**	**46**	**35**	**29**	**45**	**0**
T	1.83333	1.89796	1.86842	1.84375	1.89583	0.3333333

Step 4: Each value of TT is multiplied by 100,000 and assigned to E_nE_n.

T	1.6875	1.83333	1.89796	1.86486	1.85294	1.88095
E_nE_n	168750	183333	189796	186486	185294	188095
T	1.83333	1.89796	1.86842	1.84375	1.89583	0.333333
E_nE_n	183333	189796	186840	184375	189583	33333

Step 5: Now, to each E_nE_n modulo 54 is obtained and assigned asC_nC_n. Also, the corresponding K_nK_n is obtained.

E_nE_n	168750	183333	189796	186486	185294	188095
C_nC_n	0	3	40	24	20	13
K_nK_n	3125	3395	3514	3453	3431	3483
E_nE_n	183333	189796	186840	184375	189583	33333
C_nC_n	3	40	0	19	43	15
K_nK_n	3395	3514	3460	3414	3510	617

Step 6: With the E_nE_n values obtained, the corresponding cipher text is obtained using the coding table.

0	3	40	24	20	13	3	40	0	19	43	15
.	C	n	X	T	M	C	n	.	S	q	O

The plain text ‘Mathematics’ is now converted to the cipher text ‘.CnXTMCn.SqO’. The coding table, the key values K_nK_n and the probability values $a_1, a_2, a_3a_1, a_2, a_3$ and a_4a_4 chosen for framing bilinear transformation are shared only between the sender and the receiver.

7 Decryption—Worked Example

The decryption process is explained with the same cipher text ‘.CnXTMCn.SqO’ as follows.

Step 1: Using the coding table, the numerical values corresponding to '.CnXTMCn.SqO' are obtained.

.	C	n	X	T	M	C	n	.	S	q	O
0	3	40	24	20	13	3	40	0	19	43	15

Step 2: With the values of C_nC_n and K_nK_n, the values of E_nE_n are obtained using the relation $E_n = K_n * 54 + C_nE_n = K_n * 54 + C_n$.

C_nC_n	0	3	40	24	20	13
K_nK_n	3125	3395	3514	3453	3431	3483
E_nE_n	168750	183333	189796	186486	185294	188095
C_nC_n	3	40	0	19	43	15
K_nK_n	3395	3514	3460	3414	3510	617
E_nE_n	183333	189796	186840	184375	189583	33333

Step 3: Divide each value of E_nE_n by 100,000 which gives the values of TT.

E_nE_n	168750	183333	189796	186486	185294	188095
TT	1.6875	1.83333	1.89796	1.86486	1.85294	1.88095
E_nE_n	183333	189796	186840	184375	189583	33333
TT	1.83333	1.89796	1.86842	1.84375	1.89583	0.333333

Step 4: The inverse bilinear transformation related to TT is

$$B = \frac{0.25 - 0.75T}{0.25T - 0.5} B = \frac{0.25 - 0.75T}{0.25T - 0.5}$$

Using the values of TT, the values of BB are obtained as listed below.

TT	1.6875	1.83333	1.89796	1.86486	1.85294	1.88095
BB	13	27	46	34	31	39
TT	1.83333	1.89796	1.86842	1.84375	1.89583	0.3333333
BB	27	46	35	29	45	0

Step 5: With the help of the coding table, the plain text is obtained from the values of BB as follows.

13	27	46	34	31	39	27	46	35	29	45	0
M	a	t	h	e	m	a	t	i	c	s	.

8 Conclusion

A new cryptographic algorithm applying probability and bilinear transformation has been proposed in this paper. The plain text 'Mathematics' has been converted to cipher text using the proposed encryption algorithm. Also its reverse process using decryption algorithm has been furnished to get the plain text. This paper proposes a cryptographic technique using probability and bilinear transformation for encryption and decryption of a message. The algorithm for encryption and decryption is expressed in detail. The probability concept is used to secure the key between the communicator and recipient. The advantage of this method is that the process carries out protection at two stages one at choosing probability and the other at finding the key points. The methodology is useful to get a safe communication between communicator and recipient. The bilinear transformation gives more secure for the process in key transformation. The bilinear transformation is used to encrypt the message. The inverse bilinear transformation is used to decrypt the message. The example is presented to validate the theory part.

References

1. Hiwarekar, A.P. 2014. New mathematical modeling for cryptography. *Journal of Information Assurance and Security, MIR Lab USA* 9: 027–033.
2. Gençoğlu, M.T. 2017. Cryptanalysis of a new method of cryptography using laplace transform hyperbolic functions. *Communications in Mathematics and Applications* 8 (2): 183–189.
3. Hiwarekar, A.P. 2013. A new method of cryptography using laplace transform of hyperbolic functions. *International Journal of Mathematical Archive* 4 (2): 208–213.
4. Undegaonkar, Hemant K. 2019. Security in communication by using laplace transform and cryptography. *International Journal of Scientific & Technology Research* 8 (12): 3207–3209.
5. Sujatha, S. 2013. Application of laplace transforms in cryptography. *International Journal of Mathematical Archive* 4: 67–71.
6. Jayanthi, C.H., and V. Srinivas. 2019. Mathematical modelling for cryptography using laplace transform. *International Journal of Mathematics Trends and Technology* 65: 10–15.
7. Nagalakshmi, G., A.C. Sekhar, and D.R. Sankar. 2020. Asymmetric key cryptography using laplace transform. *International Journal of Innovative Technology and Exploring Engineering* 9: 3083–3087.
8. Dhingra, S., A.A. Savalgi, and S. Jain. 2016. Laplace transformation based cryptographic technique in network security. *International Journal of Computer Applications* 136 (7): 0975–8887.
9. Saha, M. 2017. Application of laplace-mellin transform for cryptography. *Rai Journal of Technology Research & Innovation* 5 (1): 12–17.
10. Sedeeg, A.K.H., M.M. AbdelrahimMahgoub, and M.A. SaifSaeed. 2016. An application of the new integral "Aboodh Transform" in cryptography. *Pure and Applied Mathematics Journal* 5 (5): 151–154.
11. Abdalla, M., J.H. An, M. Bellare, and C. Namprempre. 2008. From identification to signatures via the Fiat-Shamir transform: Necessary and sufficient conditions for security and forward-security. *IEEE Transactions on Information Theory* 54 (8): 3631–3646.
12. Aliyu, A.A.M., and A. Olaniyan. 2010. Vigenere cipher: Trends. *Review and Possible Modifications. In PiE* 101: 1.

13. Sanchez, J., R. Correa, H. Buena, S. Arias, and H. Gomez. 2016. Encryption techniques: A theoretical overview and future proposals. In *2016 Third International Conference on eDemocracy & eGovernment (ICEDEG)*, 60–64. IEEE.
14. Diffie, W., P.C. Van Oorschot, and M.J. Wiener. 1992. Authentication and authenticated key exchanges. *Designs, Codes and Cryptography* 2 (2): 107–125.
15. Chatterjee, D., J. Nath, S. Dasgupta, and A. Nath. 2011. A new symmetric key cryptography algorithm using extended MSA method: DJSA symmetric key algorithm. In *Communication Systems and Network Technologies (CSNT), International Conference*, 89–94.