Text Cryptography via Special Polynomial Technique

Adil AL-Rammahi
Dep. of Mathematics,
Faculty of CSM, Uinversity of Kufa,
Najaf, Iraq
adilm.hasan@uokufa.edu.iq

DOI : http://dx.doi.org/10.31642/JoKMC/2018/090102
Received Dec. 12, 2021. Accepted for publication Feb. 24, 2022

Abstract*— *Discrete cryptographic such as RSA, knapsack, and discrete logarithms are the oldest and best cryptographic techniques. They are worked during finite field. In this paper, an attempt to another branch of cryptography was introduced. In this proposed method, the interpolation branch of mathematics is used for text cryptography. Proposed method was introduced to cipher the plaintext message as word by word. In encryption part, three steps are implemented for product cipher word. First, each letter of the word transformed to decimal number, then to binary. Second, the binary codeword transformed to decimal. Third, the finally cipher word is represented as triple. So it transformed to three numbers by descending the original number. A quadratic polynomial is constructed where the three numbers are represented in the coefficients of the polynomial. By choosing of three temp small independent values, three dependent values are calculated as the code word. For decryption part, the special polynomial technique is used for recover the quadratic polynomial. The rest steps are deduced conversely with the encryption part procedure.

***Keywords*— Text Cryptography, Polynomial and Interpolation.**

I. INTRODUCTION

The recent and most studies of text cryptography theory are depending on high, complex, and difficult information of mathematics such as cyclic groups [1], rings[2], elliptic curve [3], finite fields [4], Fermat equation [5], factorization [6], Euler phi equation [7], composite public key [8], Galio field [9], and others. For instance the recent update common cipher methods such as discrete logarithm [10] and knapsack [11]. They are depending on algebraic mathematical branch. For working another branch of text cryptography, interpolation technique is used. In encryption part, three steps are implemented for product cipher word. First, each letter of the word transformed to decimal number, then to binary. Second, the binary code word transformed to decimal, say (y). Third, the finally cipher word is represented as [(y-2), (y-1), y]. It transforms to three numbers by descending the original number. A quadratic polynomial is constructed where the three numbers are represented in the coefficients of the polynomial. By choosing of three temp small independent values, three dependent values are calculated as the code word. For decryption part, the special polynomial technique is used for recover the quadratic polynomial. The rest steps are deduced conversely with the encryption part procedure.

For fast survey of last updates works of text cryptography, Mahajan and Easo studied the Jordon-Totient function and applied them to RSA public key cryptosystem [12]. Matkar and Dole implements Elliptic curve cryptography for encryption and decryption of data in Wireless sensor networks consist of sensor nodes [13]. Jain et al present a comparison and optimization of Galois field algorithm and International data encrypted algorithm [14]. Alanazi et al present a comparison and optimization of data encryption standard, triple data encryption standard, and advance encryption standard [15]. Anjaneyulu et al introduced a secured digital signature scheme using polynomials over non-commutative division semi rings [16]. Taqa et al introduced a collaborate approach between steganography and cryptography using secret key steganography and advanced encryption standard method of Rijndael technique [17].

With respect to numeric concepts of text cryptography, Buba and Wajiga introduced cryptographic algorithms for secure data communication using Newton-Raphson's method for solving nonlinear equations [18]. Ranjani et al introduced a secure message transmission using Lagrange polynomial interpolation and Huffman coding tree [19]. Sahana et al proposed an algorithm of secure dual multilayered encryption and data hiding as well as decryption data extraction [20]. Kaur et al makes a comparison between classical cryptography and quantum cryptography [21]. Khaled and Jalab study the Data security based on neural networks [22].

In this paper a novel text cryptography was introduced. In encryption part, three steps are implemented for product cipher

word. First, each letter of the word transformed to decimal number, then to binary. Second, the binary codeword transformed to decimal, say (y). Third, the finally cipher word is represented as triple [(y-2), (y-1), y].template, modified in MS Word 2007 and saved as a "Word 97-2003 Document" for the PC, provides authors with most of the formatting specifications needed for preparing electronic versions of their papers. All standard paper components have been specified for three reasons: (1) ease of use when formatting individual papers, (2) automatic compliance to electronic requirements that facilitate the concurrent or later production of electronic products, and (3) conformity of style throughout a conference proceedings. Margins, column widths, line spacing, and type styles are built-in; examples of the type styles are provided throughout this document and are identified in italic type, within parentheses, following the example. Some components, such as multi-leveled equations, graphics, and tables are not prescribed, although the various table text styles are provided. The formatter will need to create these components, incorporating the applicable criteria that follow.

II. TEXT CRYPTOGRAPHY USING SPECIAL POLYNOMIAL TECHNIQUE

In the branch of text cryptography, the axiom benefits that the errors between plain text and encrypted text are all zero [25]. This section was concerned for showing the proposed interpolated algorithm of text cryptography. In this method, the encrypted operations deal with word by word. So it is faster than methods deal with letter by letter. In encryption part, the word transformed to three integer numbers. A polynomial of second degree is constructed where its coefficient represented by these three numbers. The numerical method of special polynomial used in the part of decryption. The procedure of our algorithm is written as follows.

1) Transform the letters (L_1, L_2, …, L_n) of n-word to binary forms (B_1, B_2,…, B_n) with its corresponding weights (W_1, W_2,…, W_n).
2) Compose the cod word C= $B_1B_2…B_n$
3) Transform C to decimal form named as y.
4) Compute the key $x = W_1 + W_{2+}…+ W_n$.
5) Take the polynomial $p(x)=(y-2)+(y-1)x+yx^2$
6) Transform p(x) as the ciphered word of (L_1, L_2, …, L_n).

III. IMPLEMENTATIONS

explaining our algorithm, the plaintext (adil) is ciphered in detail via our text crypto method. Many examples are token in TABLE I.

Example 1: To cipher the plaintext (adil)

Encryption part:
1) Transform (adil) to decimal (1,4,9,12).
2) Transform (1,4,9,12) to binary (01,100,1001,1100).
3) Transform the code word (0110010011100) to decimal with weights (3228,2,3,4,4).
4) Compute the key x = 2 + 3 + 4 + 4 = 13 .
5) Compute the polynomial $p=p(x)=3226+3227x+3228x^2 = 590709$.

Decryption part:
1) Receive code word with weights (590709,2,3,4,4).
2) Input the key x = 2 + 3 + 4 + 4 = 13 .
3) Deduce y from $y = (p+x+2)/(x^2+x+1) = 3228$.
4) Transform (3228,2,3,4,4) to binary (01,100,1001,1100).
5) Transform (01,100,1001,1100) to decimal (1,4,9,12).
6) Transform the decimal (1,4,9,12) to plaintext (adil)

Other words are ciphered and the results are showed in TABLE 1

TABLE 1
Test Words

Plain Word	**Tuka**	**He**	**the**
Decimal Letters	20,21,11,1	8,5	20,8,5
Binary Letters	10100,10101,1011, 01	1000,0101	10100, 1000,0101
Binary Code Word With Weights	1010010101101101, 5,5,4,2	10000101,4,4	1010010000101,5,4,4
Decimal Code Word	42349,5,5,4,2	133,4,4	5253,5,4,4
Cipher Word With Weight	11561259,5,5,4,2	9699,4,4	961284,5,4,4

IV. COMPARISONS WITH RELATED WORKS

For comparisons our work with update related works, Buba and Wajiga [18] proposed encryption algorithm consists of a three level cipher attempt . The first level is achieved through the words compression manner, the second level is realized by transforming the compressed words into systems of nonlinear equations and the third level is achieved by the applying the special delta encoding principles. So it deals with complicated nonlinear equations in encryption part and needed high numerical method for solving nonlinear equations in decrypted part. It deals with equations , while our algorithm deals with numbers.

In the work of Ranjani et al [19], every word needed Huffman dictionary and two random numbers generating (RNG). Then the plain word is transformed to eight points in (x,y)-plane. For decrypted part, the classic Lagrange polynomial interpolation (LPI) of seventh degree is used.

While in our method there is no any RNG. The second degree LSA interpolated method. Clearly LSA is more efficient than LPI was used.

In the work of Sahana et al [20], the plain word is transformed to ASCII, binary, reverse form, and finally to complement form. Then the XOR operation is applied to odd and positions. In the last step the $2^n x 2^n$ image is constructed for word with length (n) using Data Block algorithm where the "0" is representing unchanged bits and "1" is the changed one. So there are no any new method with respect to algebraic or numerical types.

Volna et al [26] used the artificial multilayer neural networks(MNN) for text crypto. Both systems were designed as follows: 6 units on the input layer and 6 output units were trained on binary representations of symbols. The plain message is transformed to 6-digits binary sets. Then each ANN contains 6 input and 6 output elements. The plain text represented as the output. The key is used as the weights of ANN. Really ANN is one of approximated methods which causes non small errors. So it appropriates for image cryptography more than text cryptography. In the other hand ANN is not considerable as invertible model.

ROBUSTNUS OF PROPOSED METHOD

Assume that the attacker can gain access and read the crypto values [9699,4,4]. Suppose that the attacker is knowledgeable about the presented algorithm in this study, with respect to the method's algebraic type and key, the attacker has to manipulate the following options for calculating y, arranged in TABLE 2,

TABLE 2 : The Options Of Attacker

Option No.	P(x)
(1)	$p(x) = yx^2 + (y-1)x + y - 2$
(2)	$p(x) = yx^2 + (y-1)x + y + 1$
(3)	$p(x) = yx^2 + (y-1)x + y + 2$
(4)	$p(x) = yx^2 + (y-2)x + y - 1$
(5)	$p(x) = yx^2 + (y-2)x + y + 1$
(6)	$p(x) = yx^2 + (y-2)x + y + 2$
(7)	$p(x) = yx^2 + (y+2)x + y + 1$
(8)	$p(x) = yx^2 + (y+2)x + y - 1$
(9)	$p(x) = yx^2 + (y+2)x + y - 2$
(10)	$p(x) = yx^2 + (y+1)x + y + 2$
(11)	$p(x) = yx^2 + (y+1)x + y - 2$
(12)	$p(x) = yx^2 + (y+1)x + y - 1$

and so on there are 12*6 = 70 options for each key x = 4+4 and x = 4*4. One can use the attacker's Table 2, to find the values of *y*.

V. CONCLUSIONS

Interpolated polynomial of special polynomial was used in decryption part for introducing a new method of text cryptography. It is an attempt to deal with special polynomial and cryptography of text word. The demands of our Algorithm are practical and simple. So the results have zero errors. For clearing our Algorithm , many words were taken where the first word is implemented by all details. Our method deals with the manner of word by word encryption. So it is faster than the methods deal with letter by letter encryption manner. Furthermore, our method needs common concepts of mathematics such as real polynomial, special polynomial, binary form, and interpolation theory. It is exceeding the information of discrete Galio field and Fermat equation problems.

ACKNOWLEDGMENT

This paper was supported by the faculty of computer science and mathematics of university of Kufa, Iraq. I thank all reviewers for deep reading on this paper.

REFERENCES

[1] B.S. Kaliski, R.L.Rivest, and A.T. Shermam, is the data encryption standard a group, result of cycling experiments on DES, cryptology, vol.1,1988, pp. 3-36.

[2] T. ElGamal, A public key cryptosystem and a signature scheme based on discrete logarithms, IEEE Transactions on Information Theory, 469-472, 1985.

[3] I. Biehl, B. Meyer, and V. M□uller. Differential fault attacks on elliptic curve cryptosystems. In M. Bellare, editor, CRYPTO, volume 1880 of Lecture Notes in Computer Science, pp. 131-146. Springer, 2000.

[4] M. Prabu and R. Shanmugalakshmi , A Comparative and Overview Analysis of Elliptic Curve Cryptography over Finite Fields, International Conference on Information and Multimedia Technology, ICIMT '09,2009, PP. 459-499.

[5] X. Guangli; C. Zhuxiao; , The Algebra Homomorphic Encryption Scheme Based on Fermat's Little Theorem, International Conference on Communication Systems and Network Technologies , vol.1, no.1, pp.978-981, 2012.

[6] B.R. Ambedikar and S.S. Bedi, A New Factorization Method to Factorize RSA Public Key Encryption, IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 6, No 1, November, 2011, pp. 242-247.

[7] R. Rivets, A. Shamir, and L. Adleman, A Method for Obtaining Digital Signatures and Public-Key Cryptosystems, Communications of the ACM 21 (2), pages 120-126,1978.

[8] A. AL-Rammahi and N. Ressol, On The Public Key Cryptography, J. Babil University, Vol.7, No.3, 2002, Pp.496-472.

[9] P. Kitsos, G. Theodoridis, and O. Koufopavlou, An efficient reconfigurable multiplier architecture for Galois Field GF(P^m), Microelectronics Journal 34, 2003, pp. 975–980.

[10] A. M. Odlyzko, Discrete Logarithms: The Past and the Future, Designs, Codes, and Cryptography 19, 2000, Pp. 129-145.

[11] R. C. Merkle & H. Hellman, Knapsack Problem, IEEE Inf. Th. It-24,No.5, Sept., 1978, Pp. 525-530.

[12] S. Mahajan and S. Easo, Performance Evolution of RSA and New Cryptosystem, International Journal of Emerging Technology and Advanced Engineering, Volume 2, Issue 3, March 2012, pp. 279-283.

[13] P. Matkar and L. Dole, Energy Aware Blind Data Aggregation For Data Integrity in Wireless Sensor Network, International Journal of Emerging Science and Engineering, vol.1, issue9, 2013, pp. 1-4.

[14] P. Jain, R. Jain and T. Verma, Comparison and Implementation of Cryptography Algorithm By Using VHDL, International Journal of Emerging Technology and Advanced Engineering, Volume 2, Issue 11, November 2012, pp. 120-124.

[15] H.O. Alanazi, B.B. Zaidan, A.A.Zaidan, H.A. Jalab, M.Shabbir and Y. Al-Nabhani, New Comparative Study Between DES, 3DES and AES within Nine Factors**,** Journal Of Computing, Volume 2, Issue 3, March 2010, pp. 152-157.

[16] G. S. Anjaneyulu, P.V. Reddy and U.M. Reddy, Secured Digital Signature Scheme using Polynomials over Non-Commutative Division Semi rings , International Journal of Computer Science and Network Security, 8, 2008, pp. 278–284.

[17] A. Taqa, A.A. Zaidan, and B.B Zaidan, New Framework for High Secure Data Hidden in the MPEG Using AES Encryption Algorithm, International Journal of Computer and Electrical Engineering, Vol. 1, No. 5 December, 2009, pp. 566-571.

[18] Z. P. Buba and G. M. Wajiga, Cryptographic Algorithms for Secure Data Communication, International Journal of Computer Science and Security , Volume 5, Issue 2, 2011, pp. 227-243.

[19] R. S. Ranjani, D. L. Bhaskari, P. S. Avadhani, Secure Message Transmission using Lagrange Polynomial Interpolation and Huffman Coding**,** International Journal of Computer Applications, Volume 55– No.1, October 2012, pp. 32-35.

[20] S. Sahana, J. Sen, and C. Mondal, Secure Adaptive N-Cryption (SAN) – A Secure Algorithm for Data Transmission, International Journal of Computer Applications in Engineering Sciences, volume 3, 2013, pp. 205-213.

[21] N. Kaur, A. Singh, S. Singh, Enhancement of Network Security Techniques using Quantum Cryptography, Navleen Kaur et al. / International Journal on Computer Science and Engineering, Vol. 3 No. 5 May 2011, pp. 1960-1964.

[22] M. N. Khaled, and H.A. Jalab, Data security based on neural networks, TASK Quarterly 9 No 4, 2005, pp. 409–414.

[23] R. L. Burden and J. D. Fairs, Numerical Analysis, Brooks/Cole Publishing Company,1984.

[24] B. Kolman, Introductory Linear Algebra with Applications, Macmillan Publishing Company, New York , 3e.

[25] A. Menezes, and P. V. Orschot, Handbock of Applied Cryptography, CRC Press, 1996, pp. 283-319.

[26] E. Volna, M. Kotyrba, V. Kocian, M. Janosek, Cryptography Based On Neural Network, Proceedings 26th European Conference on Modelling and Simulation 2011.