Turkish Journal of Science & Technology
Volume 12 (1), 5-9, 2017

A Novel Symmetric Encryption Algorithm and its Implementation

Muhammet BAYKARA[1], Resul DAŞ[1], Gürkan TUNA[2]
[1]Fırat University Faculty of Technology Software Engineering Department, 23119, Elazığ
[2]Trakya University, Technical Sciences Vocational School, Edirne
mbaykara@firat.edu.tr

(Received: 09.08.2016; Accepted: 12.12.2016)

Abstract

Confidentiality of digital data stored on computer systems or transmitted via computer networks is very important in the digital era and it can be addressed with a variety of solutions such as encryption. In this respect, in this study we propose a new encryption algorithm based on a number of mathematical terms, formulas and operations. The proposed algorithm is a general purpose symmetric encryption algorithm; hence, it can be used for various purposes. The proposed algorithm is implemented an application called Secure Text. Although the developed application encrypts text, the algorithm is suitable for encrypting several file types including .txt, .rtf, .doc, .docx, .xls, .xlsx, .ppt, .pptx, .pdf, .png, and .bmp. A set of evaluation study carried out using the developed application shows that although the proposed algorithm is simple and performs very quickly, it is complicated enough and robust against potential unorganized threats.

Keywords: Encryption; symmetric encryption; encryption algorithm; file encryption.

Yeni Bir Simetrik Şifreleme Algoritması ve Uygulanması

Özet

Bilgisayar sistemlerinde depolanan ya da bilgisayar ağları üzerinden iletilen dijital verilerin gizliliği günümüz dijital çağında oldukça önemlidir. Gizliliğin sağlanması için şifreleme gibi birçok çözüm yolu mevcuttur. Bu bağlamda, bu çalışmada bir dizi matematiksel terim, formül ve işlemlere dayalı yeni bir şifreleme algoritması önerilmiştir. Önerilen algoritma genel amaçlı simetrik bir şifreleme algoritması olduğundan çeşitli amaçlarla kullanılabilmektedir. Önerilen uygulama Secure Text adlı bir uygulama içerisinde kodlanmıştır. Geliştirilen uygulama, metinleri şifrelemesinin yanı sıra. txt, .rtf, .doc, .docx, .xls, .xlsx, .ppt, .pptx, .pdf, .png, ve bmp vb. birçok dosya tipindeki dosyaların da şifrelenmesi için kullanılabilmektedir. Önerilen uygulama üzerinde gerçekleştirilen bir dizi deneme testi sonucunda, önerilen algoritmanın basit, hızlı uygulanabilir olduğu ve özellikle olası kırma ataklarına karşı yeterince sağlam olduğu gözlenmiştir.

Anahtar Kelimeler: Şifreleme, simetrik şifreleme, şifreleme algoritması, dosya şifreleme

1. Introduction

Nowadays, with the rapid development of communication technologies and mobile devices, the Internet has become indispensable and it is now a mass communication medium. However, the Internet is a public network and hence is not a secure communication medium [1]. Therefore, the use of the Internet for information exchange may cause information security threats if potential threats are not addressed. This is even more important for financial institutions and government services.

Encryption methods are commonly used to secure data transfers [2]. Their primary purpose is to protect the confidentiality of digital data stored on computers or transmitted via computer networks. They play a key role in the security assurance of information technology (IT) systems and communications since they can provide not only confidentiality, but also authentication, integrity and non-repudiation. There are three basic encryption methods, namely hashing, symmetric cryptography, and asymmetric cryptography. Each of these has their own uses, advantages, and disadvantages. Hashing algorithms create a hash value, a unique and fixed-length signature for a data set. Hashes are commonly used to compare sets of data since even minor changes to the data set result in a different hash.

2. Related Works

In recent years several symmetric and asymmetric encryption algorithms have been proposed and some of them have been implemented and used successfully. A symmetric encryption algorithm, sometimes called secret key algorithm, is a cryptographic algorithm which uses the same key to encrypt and decrypt data. On the other hand, an asymmetric encryption algorithm uses public and private keys to encrypt and decrypt data. The keys are large numbers which have been paired together but they are not identical. In the pair, the public key can be shared with everyone but the private key is kept secret. Either the public or the private key can be used to encrypt a message, and the opposite key is used for decryption.

The problem with symmetric encryption algorithms is how to securely get the secret keys to each end of the exchange and keep them secure after that. Therefore, when the distribution of secret keys constitutes a problem, asymmetric encryption algorithms are preferred.

Although in the literature there are many well-known symmetric and asymmetric encryption algorithms such as Data Encryption Standard (DES) [3], Triple DES (3DES) [4], AES [5, 6, 7], Blowfish [8], Serpent [9], Twofish [10], RSA [11], ElGamal [12], and Paillier [13], there is a need for an easy-to-use, simple, free and general purpose encryption tool to secure data transfer needs of people. There are different many security applications in literature [14-15].

Accordingly, in this study we developed an open source application called Secure Text. The application can encrypt text messages but the algorithm is suitable for encrypting several file types including .txt, .rtf, .doc, .docx, .xls, .xlsx, .ppt, .pptx, .pdf, .png, and .bmp. The rest of this paper is as follows. Proposed symmetric encryption algorithm, its implementation and how the proposed algorithm is implemented are given in Section II. The design of the application which was developed to implement the proposed algorithm is also given in Section II. Finally the paper is concluded in Section III.

3. Proposed Algorithm, Implementation and Developed Application

The proposed algorithm's encryption and decryption steps are different. The algorithm follows the steps explained below to encrypt a given text and to decrypt an encrypted text. To implement the proposed algorithm, its flow is given in Fig. 1, an application called Secure Text was developed using C#.

Encryption Model of the Proposed Algorithm:

Step 1: The algorithm first receives original text and key which will be used to encrypt the original text. The original text cannot be less than 3 characters and the key cannot be empty.

Step 2: Each character of the original text is converted into ASCII code and then binary equivalent of each sixteen-digit sequence is created.

Step 3: The number of digits of each character is multiplied by the character's value and then the total is calculated. Using the total, variance (V) is calculated.

Step 4: Mode operation is applied on V using the array's column number and then the mix operation is applied.

Step 5: The key is converted to binary system taking care that the obtained value will have 16 binary digits. Then, its decimal equivalent is calculated to find K.

Step 6: A is calculated using the following equation.

$$A=((1/|\sin K|)+(\log 10V))*1000000000000$$

Step 7: A is converted to binary system and then an array is built.

Step 8: A is compared with the dimension of the array obtained in Step 4. Zero bits are added to the beginning of the fewer one until their dimensions are the same.

Step 9: A new array is created by mixing the arrays obtained in Step 8. Depending on the value

of K, mode operation is applied on the new array and the new array is mixed again.

Step 10: Eight digits of the array obtained in Step 9 are taken and converted to decimal system. Then, they are added to K.

Encrypted text is created after obtaining ASCII characters of the sums.

Decryption Mode of the Proposed Algorithm:

Step 1: Text to be decrypted and key is taken from the user.

Step 2: The key is converted to ASCII code system. Then, the result is converted to binary system taking care that the obtained value will have 16 binary digits. Each of the digits is multiplied with the order of the digit to calculate sum. The obtained sum is K. The text's ASCII equivalent is created and then individually subtracted from K.

Step 3: The obtained values are converted to binary system taking care that they will have 8 digits and an array is built.
Reverse mode operation is applied on K based on the array's dimension.

Step 4: The array and mixed array is separated by the inverse of the encryption

Step 5: Zero bits are removed from the beginning of A and then A is converted to decimal system.

Step 6: Using the following equation, variance (V) is calculated.
V=10^((A/1000000000000)-(1/|sinK|))

Step 7: A new array is built after reverse mode operation has been applied to V based on the mixed array's dimension. Sixteen characters from the new array are selected to obtain decrypted (original) text.

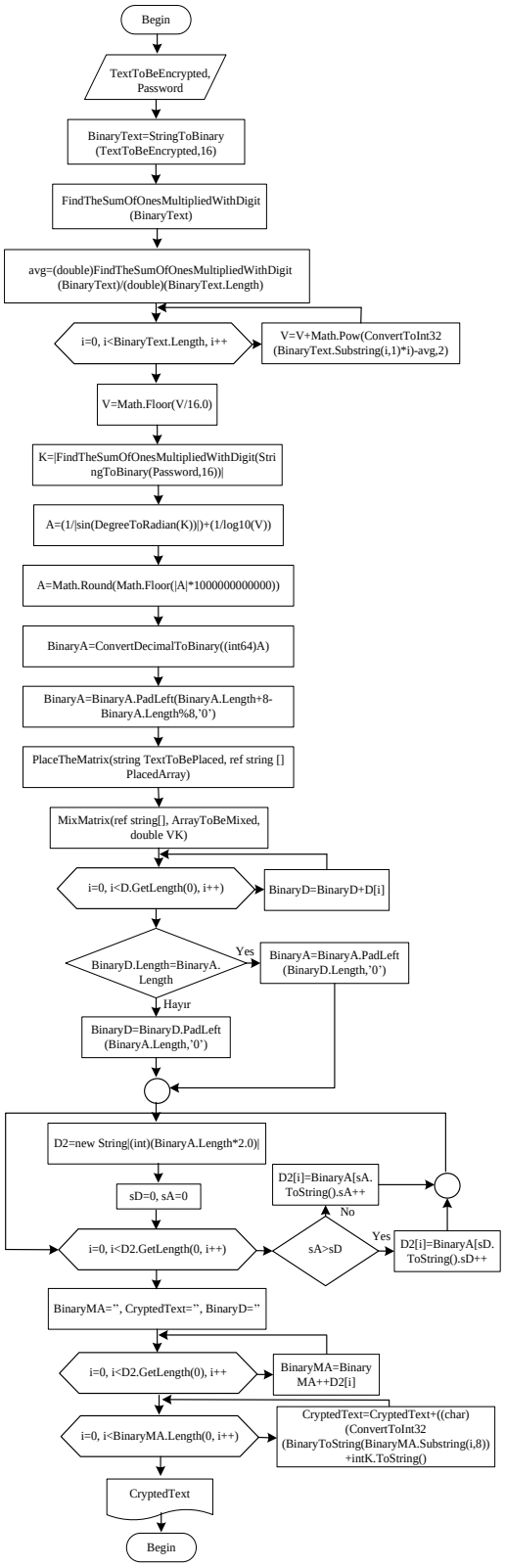

Fig. 1: Flowchart of the proposed algorithm.

Fig. 2: Graphical user interface of the developed application

4. Conclusion

To address confidentiality of sensitive data, in this study we proposed a novel encryption algorithm. The proposed algorithm is a symmetric encryption algorithm, can quickly encrypt a given file, and is robust enough for various purposes. To implement the proposed algorithm we developed an application called Secure Text. However, the proposed algorithm can encrypt different file types with different extensions such as .txt, .rtf, .doc, .docx, .xls, .xlsx, .ppt, .pptx, .pdf, .png, and .bmp.

The proposed algorithm presented several interesting features, such as a high level of security and an acceptable encryption speed. The algorithm has been successfully applied to and tested for the text and image encryption. Although the algorithm presented in this paper has focused on text encryption.

5. References

1. J. H. Allen, The CERT Guide to System and Network Security Practices, Boston, MA: Addison-Wesley, 2001.
2. C. A. Jan and V. D. Lubbe, Basic Methods of Cryptography, United Kingdom: Cambridge University Press, 2002.
3. W. Diffie and M. E. Hellman, "Exhaustive Cryptanalysis of the NBS Data Encryption Standard," IEEE Computer, vol. 10, no. 6, pp. 74-84, 1997.
4. ANSI-X9.52, Triple date encryption algorithm modes of operation, Revision 6.0, 1998.
5. J. Daemen and V. R. Vincent, AES Proposal: Rijndael, 2003. Available at: http://csrc.nist.gov/archive/aes/rijndael/Rijndael-ammended.pdf [Accessed 11 April 2016].
6. S. Murphy, "The Advanced Encryption Standard (AES)," Information Security Technical Report, vol. 4, no. 4, pp. 12-17, 1999.
7. R. Daş, G. Tuna, "Design and Implementation of a Simple, AES-Based Secure Messaging Platform", 2nd International Conference on Engineering and Natural Sciences (ICENS), 24-28 Mayıs 2016, Sarajevo (Saraybosna), Bosnia and Herzegovina (Bosna ve Hersek)
8. B. Schneier, "Description of a New Variable-Length Key, 64-bit Block Cipher (Blowfish)," in Fast Software Encryption, Cambridge Security Workshop, R. J. Anderson (Ed.), Springer-Verlag, London, UK, 1993, pp. 191-204

9. J. A. Ross, “Serpent: A Candidate Block Cipher for the Advanced Encryption Standard,” University of Cambridge Computer Laboratory, 2006.
10. B. Schneier, J. Kelsey, D. Whiting, D. Wagner, C. Hall, and N. Ferguson, The Twofish Encryption Algorithm: A 128-Bit Block Cipher, New York City: John Wiley & Sons, 1999.
11. R. Rivest, A. Shamir, and L. Adleman, “A Method for Obtaining Digital Signatures and Public-Key Cryptosystems,” Communications of the ACM, vol. 21, no. 2, pp. 120-126, 1978.
12. T. ElGamal, “A Public-Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms,” IEEE Transactions on Information Theory, vol. 31, no. 4, pp. 469-472, 1985.
13. P. Paillier, “Public-Key Cryptosystems Based on Composite Degree Residuosity Classes,” EUROCRYPT, Springer, pp. 223-238, 1999.
14. M. Baykara, R. Daş, "A Steganography Application for Secure Data Communication", 10th International Conference on Electronics, Computer and Computation (ICECCO 2013), Turgut Özal University, pp. 309-313, 7-9 November 2013, Ankara.
15. A. Tuna, R. Daş, G. Tuna, “Design and Implementation of a Software Application for Secure Web-Based Communication for People with Speech Disorders”, pp.387-394, 28 June 2016, 24th International Academic Conference, Barcelona-Spain. International Institute of Social and Economic Sciences (IISES), ISSN 23365617, ISBN: 978-80-87927-25-0, DOI: 10.20472/IAC.2016.024.091