International Journal of Computer Applications Technology and Research
Volume 5– Issue 6, 391 - 394, 2016, ISSN:- 2319–8656

A New Method for Encrypting Digital Data Using Symmetric Key in Information Exchange Spaces

Hadi Hajilar Lahrod
Department of Electrical Engineering, Ahar Branch, Islamic Azad University, Ahar, Iran.

Ali Rahnemaei
Department of Electrical Engineering, Ardabil Branch, Islamic Azad University, Ardabil, Iran.

Seyed Hadi Seyed Hatami
Department of Electrical Engineering, Ardabil Branch, Islamic Azad University, Ardabil, Iran.

Abstract: with the arrival of the information age and much more important information systems and communication in human everyday life, necessity immunization information and communication strategy were also raised. The easiest way to meet this necessity is conventional encryption algorithms. Encryption is a right tool for data protection in an unsecure channel. To this end, from two-method symmetric key encryption and public-key cryptography are used. In this paper we examine text cryptography, one of the most important topics in cryptography. A unique attribute of this kind of encryption has been of interest to many researchers in this field. This paper, considering the symmetric encryption algorithm, provides a text encryption algorithm using a 128-bit key. The proposed algorithm uses a 128-bit key, the text data using the XOR operator to convert the encrypted information. Therefore, the aim of this method is to provide a convenient method for symmetrically encrypting data not to be easily decoded, and finally, the results of the tests show that the proposed method is better in terms of security and speed of execution.

Keywords: Encryption; symmetric; XOR operator; text information; key.

1. INTRODUCTION

One way to provide safety information is encryption. With encryption, confidentiality and message authenticity are preserved. The main problem in cryptography is that the threats neither cannot obtain the original text of encrypted text, nor cannot find the decoding converters even by accessing the original text. In this case, the amount information obtained from the encrypted text and encoding method are important [1]. Cryptography includes of two major components, an algorithm and a key. Algorithm is a converter or mathematical formula. There are a few powerful algorithms that most of them have been published as standards or mathematical papers. Key is a string of binary digits (ones and zeros) which is meaningless by itself. Modern cryptography assumes that an algorithm is known or can be discovered. Key must be kept secret and changed in any stage of implementing. Decryption may use the same pair of algorithms and key. Data encryption algorithms are generally divided into two categories. The first batch contains symmetric encryption algorithms while the second category contains asymmetric cipher algorithms. Asymmetric key encryption algorithms use different keys for encryption and decryption. Many systems allow the one of publicly keys to be released while another private key is kept by its owner. Sender of the message codes the text with the recipient's public key and receptor encrypts it with their private key. In other words, only recipient's private key makes it possible to turn the coded text to the original one. It means that even if the sender accesses the main content text, they cannot achieve to the original text via cipher text. Therefore the coded message will be meaningless for any recipient rather than the real one [2]. Therefore, with studying algorithms that has been used before in this context, a new solution for encrypting confidential information can affect and help establishment of security in communications. In this paper we propose a new method for encrypting digital data using asymmetric key in the exchange of information spaces.

2. SECURITY REQUIREMENTS

Each encryption algorithm that is used to create data security should ensure some specific security requirements which are as follows:

2.1 Confidentiality of data's

The main purpose in security issues is to maintain data confidentially from unauthorized user accesses. In fact, data confidentiality is means maintenance of information secretly. Different protocols use various cryptographic methods.

2.2 Data integrity

Making information confidential, external factors cannot steal information, but it does not meant the secure and healthy data. Data integrity ensures that the received data has been remained unchanged during transmitting.

2.3 Data Novelty

Data novelty ensures that received data is new and is not a repeat of previous messages.

2.4 Authentication

Encryption algorithms must have the authentication ability of the received data, and can ensure the accuracy of the transmitter. The sender of information cannot, in the future, deny sending or its provisions. Various security protocols use different encryption algorithms to meet these requirements.

3. CLASSIFICATION OF ENCRYPTION METHODS

An encryption algorithm is a set of rules and mathematical relationships which ends in a difference and clutter in the data. Modern encryption algorithms can be classified based on two criteria; functional keys and type of input. Data encryption method is divided, based on input data type, into two blocks and streams. Most of the techniques presented are based on the image encryption [3][4].

4. SYMMETRIC ENCRYPTION

In general, symmetric encryption has two parts, sender and receiver, which want to communicate with each other in an insecure channel, without letting someone else to get any information on the relationship. The purpose of encryption algorithms is to protect the security of a message that is transmitted through an insecure channel. In general an organization symmetric encryption has two functions, encryption E and decryption D. The Encryption function E receives the inverse of the original text as an input, and transforms it under the key K to cipher text$C = E_k(P)$. The encryption function $D = E^{-1}$ is reverse function of encryption function, so $P = D_K(C)$. the key B is also called secret key or shared key. In Fig.1, a general block diagram of symmetric encryption system has been shown.

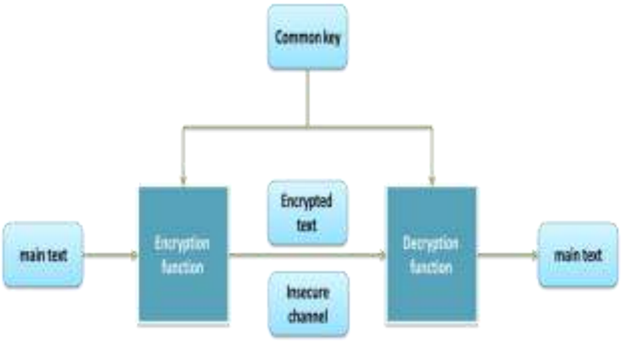


Fig.1 Block diagram of symmetric encryption system

5. RELATED WORKS

Security information in communication technology is one of the issues that has occupied scholars of this area, because with compromising information security, serious problems happen to come for the message and threaten its integrity. Due to this problem, scientists went on to make secret before exchanging information and in the consequent, they reduce or neutralize the effect of inhibiting factors. With technological advances and the advent of modern communications, the need to provide new methods in this area is greater than ever. Thus, according to expand of the use of communication technology in transmitting critical data, the privacy and data security are of utmost importance. There have been done multiple algorithms to encrypt data too [5][6][7]. In some other activities encryption of data has been investigated for various methods [8][9]. Various proposed methods in encryption information are divided generally into two categories: stream encryption and blocks encryption [10][11]. In the first kind, at any moment, encryption is done bit by bit or character by character, but in the second the entire string is encrypted and transmitted at once. Generally, for both encryption methods, the keys are used which are made of pseudorandom numbers. There are several methods for generating random numbers such as modular arithmetic generators, linear and non-linear, linear recurrence registers (LFSR) and a non-linear Cellular Automata (CA) and so on [12]. Access to information stored in computer databases has greatly increased. Much of the information stored is highly confidential, which is not visible to the public. Data security is studied using encryption techniques research conducted in an article with this theme, a new encryption algorithm is provided based on concept of block encryption, and logical operations such as XOR and shift operations are used as well. The proposed algorithm improves encryption security by symmetric putting layers [13]. Visual secret sharing (VAS) is a visual encryption scheme which decodes secret messages to several big stocks [14].

6. ENCRYPTION APPROACH

The proposed encryption system is one of the symmetric systems that guarantee an absolute security. Overall approach of this system is to generate key length of plain text and XOR keys with text. In this method, the receiver of the message must have the encryption key up with XOR again, restore the original text. Totally randomness key, full security for the proposed system ensures this approach also high computational security in the face of the enemy. In building public key cryptography systems, objective of securing is computational. In this case, although these systems are not secure against invaders, such strikers do not exist in the real world.

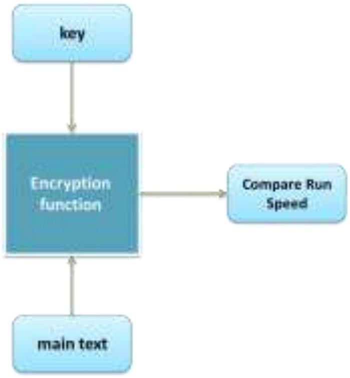


Fig. 2 Main operation the proposed algorithm

7. DESCRIPTION OF THE PROPOSED ALGORITHM

In some methods, particular keys are used to perform encryption and decryption. Used keys can be the same in encryption and decryption and/or are used differently in these two factors. There are other algorithms that do not use keys for encryption. These methods create kind of clutter in messages and through this prevent the discovery of information, by unauthorized persons. Different encryption algorithms, as symmetric, asymmetric and hash functions are used for hiding and for each of these algorithms there have been proposed various methods. In the proposed method, we consider a text file, according to the same text we convert it to an array of characters. Then these characters are converted to an array of bits. Key Length for encrypt information should be ideal, if key length is greater, the security is then better and speed is lower, and vice versa, if the key length is less, security is less and encryption speed increases. In this paper we consider 128-bit key length. After selecting key length, it will be applied on the bits array in the range of 2/128. We divide bits array to 128 bits, this is our method for performing encryption. In each stage, the XOR operation will be also applied; XOR operation is as follows: after division of bits array to 128 bits, the first part of the array of bits that is 128-bit with key is done by XOR. After encrypting the first part of the array, this time half a second part of the array with half of the first part of the array with XOR action key is done; we do this action until completing the array and cryptographic operation. In the proposed method we used XOR operator to easily perform the encryption and decryption. How to do encrypt text is shown in Fig. 3:

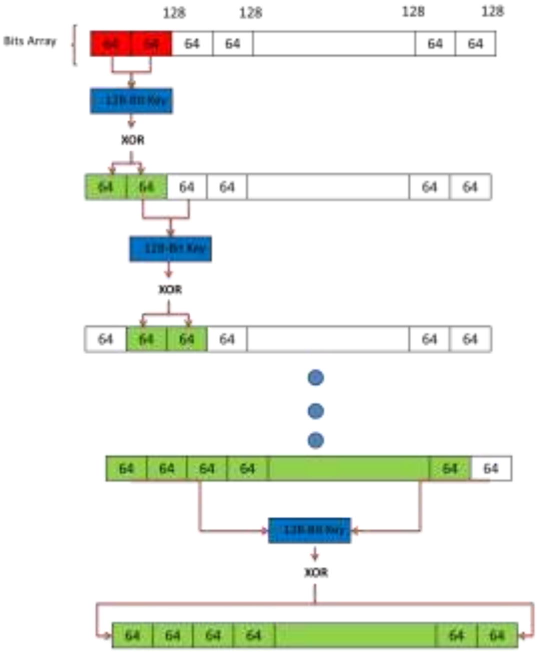


Fig.3 Description of the proposed approach

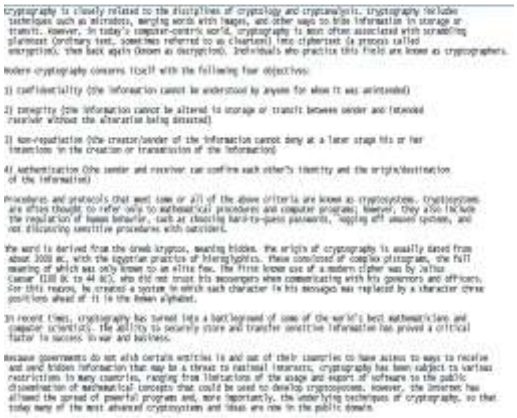
Encrypting the information

Data encryption algorithm in this method is very simple.

1. Converting secret text information to array of characters
2. Considering key length 128 bits
3. Key actions on array with range of 2/128
4. XOR perform on array with key consideration

8. IMPLEMENTATION RESULTS

For performing the test we used different texts for encryption. According to the results, it can be observed that the proposed algorithm is the fastest algorithm based on run-time. These results have been achieved using MATLAB 2009 software. The study of results shows that the encoded information output resulting from encryption method has been reported with security and high quality. We used "English" text in implementation of the proposed algorithm for encryption. In Fig.4 the English confidential text is used for encryption. Also Fig.5 and 6 show, respectively, English text information before the operation encryption and information encrypted after encryption. So after encryption operation and applying the proposed method, confidential data turns out to be in the shape of Fig.7.



Cryptography is closely related to the disciplines of cryptology and cryptanalysis. Cryptography includes techniques such as microdots, merging words with images, and other ways to hide information in storage or transit. However, in today's computer-centric world, cryptography is most often associated with scrambling plaintext (ordinary text, sometimes referred to as cleartext) into ciphertext (a process called encryption), then back again (known as decryption). Individuals who practice this field are known as cryptographers.

Modern cryptography concerns itself with the following four objectives:

1) Confidentiality (the information cannot be understood by anyone for whom it was unintended)

2) Integrity (the information cannot be altered in storage or transit between sender and intended receiver without the alteration being detected)

3) Non-repudiation (the creator/sender of the information cannot deny at a later stage his or her intentions in the creation or transmission of the information)

4) Authentication (the sender and receiver can confirm each other's identity and the origin/destination of the information)

Procedures and protocols that meet some or all of the above criteria are known as cryptosystems. Cryptosystems are often thought to refer only to mathematical procedures and computer programs; however, they also include the regulation of human behavior, such as choosing hard-to-guess passwords, logging off unused systems, and not discussing sensitive procedures with outsiders.

The word is derived from the Greek kryptos, meaning hidden. The origin of cryptography is usually dated from about 2000 BC, with the Egyptian practice of hieroglyphics. These consisted of complex pictograms, the full meaning of which was only known to an elite few. The first known use of a modern cipher was by Julius Caesar (100 BC to 44 BC), who did not trust his messengers when communicating with his governors and officers. For this reason, he created a system in which each character in his messages was replaced by a character three positions ahead of it in the Roman alphabet.

In recent times, cryptography has turned into a battleground of some of the world's best mathematicians and computer scientists. The ability to securely store and transfer sensitive information has proved a critical factor in success in war and business.

Because governments do not wish certain entities in and out of their countries to have access to ways to receive and send hidden information that may be a threat to national interests, cryptography has been subject to various restrictions in many countries, ranging from limitations of the usage and export of software to the public dissemination of mathematical concepts that could be used to develop cryptosystems. However, the Internet has allowed the spread of powerful programs and, more importantly, the underlying techniques of cryptography, so that today many of the most advanced cryptosystems and ideas are now in the public domain.

Fig.4 Confidential information for encrypting

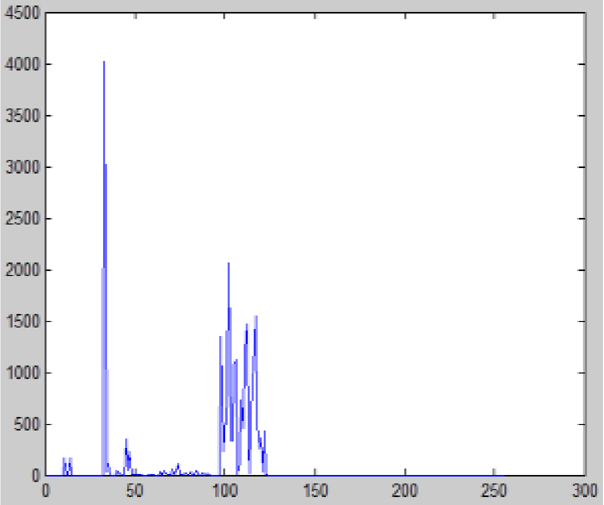


Fig.5 Text information for encryption

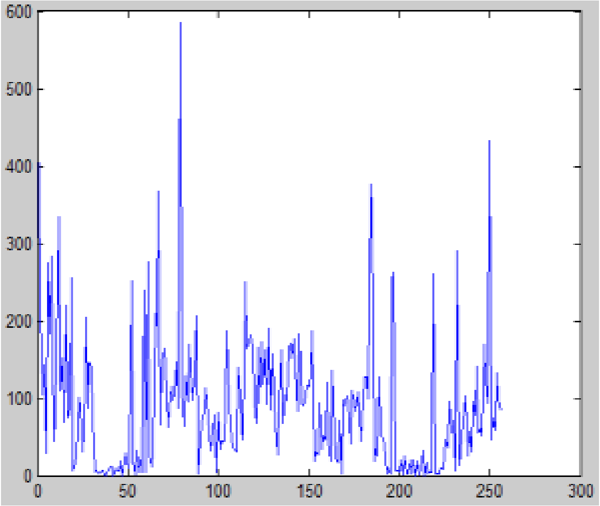


Fig.6 information encrypted

Fig.7 information encrypted

In comparison between different encryption algorithms with data size and various keys size, the proposed algorithm represents the best performance. Table 1 compares the processing speed of the proposed encryption algorithm with different key lengths with three known block ciphers. As the table shows the proposed algorithm, with length 128-bit, runs faster than other encryption methods and can serve up operations. The proposed algorithm, due to speed and simpler being implemented, is a type of symmetric cryptography for protecting information in network communication and can be used for protection of data on public channels. Time speed of encrypting and decrypting depends largely on encryption key length and file size. For obtaining confidential information and decoding it, decryption key is generated as the same generation method of encryption key, and output encrypted text being XOR to obtain a plain text.

Table 1. Comparison symmetric ciphers processing speed with the proposed algorithm

Length key	Type code	(Mbps) speed
56	DES	9
168	3DES	3
Variable	RC2	0.9
Variable	RC4	45
128	Proposed method	52

9. CONCLUSION

This article provides a secure method for encrypting text with respect to the symmetric key and XOR operator. The proposed method converts confidential information into an array of characters, then using a 128-bit symmetric key encrypts information via XOR operator, In fact the main stage is to use key and to take the XOR operator. For decryption we act in contrast to encryption. In the decode step, in first, we have a symmetric key along with the encrypted information. And according to encryption routine, we select the text again character by character and, using XOR operator, decrypt confidential information. Evaluation of the proposed method showed that encryption of confidential information is better than other methods. Security and data confidentiality in the proposed algorithm is maximum. After implementation and testing various data on the proposed algorithm we reached the conclusion that our proposed algorithm, compared to algorithms provided in the field, is more efficient and decryption of it, without the key, is more difficult and even impossible to solve. Also the algorithm speed, due to the simplicity of the method, is of high operating and computing speed. As suggestions for future studies we can note to examine asymmetric algorithms and data hiding by the algorithm.

10. REFERENCES

[1] A. Menezes, P.van Oorschot and S. Vanstone, "Handbook of Applied Cryptography", CRC Press, 1996.

[2] Jacob John, “Cryptography for resource constrained devices :A Survey”, Article in a regular journal, International Journal on Computer Science & Engineering, 2012.

[3] Ching-Nung Yang, Pin-Wei Chen, Hsiang-Wen Shih, Cheonshik Kim, Aspect ratio invariant visual cryptography by image filtering and resizing, Personal Ubiquitous Comput. 17 (5) (2013) 843–850.

[4] Kai-Hui Lee, Pei-Ling Chiu, Image size invariant visual cryptography for general access structures subject to display quality constraints, IEEE Trans. Image Process. 22 (10) (2013) 3830–3841.

[5] Ching-Nung Yang, Ting-Hao Chung, " A general multi-secret visual cryptography scheme", Elsevier, Optics Communications 283 (2010) 4949–4962.

[6] Jasdeep Singh Bhalla, PreetiNagrath ,Article in a regular journal, International Journal of Scientific & Research publications,”Nested Digital Image Watermarking Technique Using Blowfish Encryption Algorithm”, Volume 3, Issue 4, April 2013.

[7] A.Nath, S.Ghosh, M.A.Mallik, "Symmetric key cryptography using random key generator", Proceedings of International conference on SAM-2010 held at Las Vegas (USA) 12-15 July, 2010, Vol-2, P-239-244.

[8] Sui L, Duan K, Liang J, "Double-image encryption based on discrete multiple-parameter fractional angular transform and two-coupled logistic maps", Optics Communications Volume343, Elsevier ,2015, PP. 140–149.

[9] Sajasi S, Eftekhari Moghadam A.M, "An adaptive image steganographic scheme based on Noise Visibility Function and an optimal chaotic based encryption method", Applied Soft Computing, Volume 30, Elsevier, May 2015, PP. 375–389.

[10] Nikita Arora,Yogita Gigras, "Block and Stream Cipher Based Cryptographic Algorithms: A Survey", International Journal of Information and Computation Technology, ISSN 0974-2239 Volume 4, Number 2 (2014), pp. 189-196.

[11] D.J.C. MacKay, "Information Theory, Inference, andLearning Algorithms", June 26, 2003, Cambridge university Press.

[12] S. Haykin, "Neural Networks – A Comprehensive Fundation", 2th Edition, Prentice Hall, 1999.

[13] Vishwa gupta, Gajendra Singh, Ravindra Gupta, "Advance cryptography algorithm for improving data security", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 1, January 2012.

[14] Lee, CH, Chen H, Liu H, Chen G, "A new visual cryptography with multi-level encoding", Journal of Visual Languages and Computing, Elsevier, Volume 25, Issue 3, June 2014, PP 243–250.