J. App. Em. Sc
Vol 4, Issue 2, December 2013

Keyless Averaging Encryption Algorithm

Raza Ali, Muhammad Shoaib Ali, Syed Aurangzeb, Talha Mir, Zubair Zaland

Faculty of Information and Communication Technology, Balochistan University of Information Technology
Engineering & management Sciences, Quetta, Pakistan

Abstract

To achieve secure transmission during communication, secure transmission of data has great importance. Information can be encrypted to ensure security can be done with through number of ways, the most famous and reliable methods are symmetric key cryptography and asymmetric key cryptography. Both types of algorithms uses key, either shared key in case of symmetric cryptographic algorithms or public/private key in asymmetric cryptographic algorithms. In both cases, keys need to be share between sender and receiver through a secure channel. In this paper an alternative approach, based on mathematics, is used which eliminates the concept of key in encryption/decryption algorithm. This algorithm does not need any sort of extra information for decryption of cipher text. Receiver only uses the cipher text to produce plaintext.

Keywords: Encryption, Decryption, Symmetric.

Corresponding author's email: *raza.ali@buitms.edu.pk*

INTRODUCTION

Network security is the crucial element to protect the network against intruder and if an unauthorized person still manages to break the initial security of network, the secondary security elements such as encoding, encryption etc., provides security. Through encryption, the intercepted intelligence present in the information can be diverted to avoid it from being used by other than authorized entities and cannot understand the interrupted cipher data. Information converted into cipher text through an encrypting algorithm and secret key and transmitted to the receiver. The received information (cipher text) is decrypted back to plain text via same secret key (Schneier, 1995). Number of cryptographic algorithms has been invented on the bases of different techniques such as feistel cipher and non feistel, to provide secure communication, figure 1. Securing the information during transmission is an appealing activity. No. of algorithms has been designed to achieve this objective (Nadeem et al., 2005).

The two broad categories based on key types in security algorithms are symmetric key and asymmetric key cryptographic algorithms. Symmetric algorithms uses single key (shared or secret key). This secret key is shared and used with both encrypting and decrypting algorithm (Sudha et al., 2012) (Forouzan, 2004). Asymmetric algorithms uses two different type of keys, the shared public key is used to encrypt the information and for decryption of information private key is used. In both types the key is shared or publicly announced. For sharing the secret key, a secure channel is used or any other means of secure communication is utilized to perform this sharing. While for the announcement of public key, there is no need to use secure channel. In both categories, some extra activities are required to accomplish secure communication such as, generation of key, exchange of key through trusted and secure channel and key management. In this paper another method for encryption and decryption of information is purposed, which is simple but secure and which encrypt and decrypt the data without use of any key. This only need an encrypting algorithm which converts the plain text into cipher text and the decryption algorithm performs opposite process by converting the cipher text back to plain text. Keyless algorithms can save time, memory, cost associated with key generation procedure, key transmission and key management (Jiwan et al., 2012).

The other ways to differentiate between cryptographic algorithms are block cipher and stream cipher. In block cipher data is encrypted or decrypted in a group of fix length (Hoffstein et al., 2010). It is fast but has some issues. The stream is considered more secure than block cipher but it is slower than block cipher. in stream cipher the starting value of key must be alternately use. In stream cipher text is encrypted individually (Menezes, 2001). The complexity of stream cipher is less than block cipher in terms its hardware and mathematics involved in stream cipher (Brassard, 2000).

Proposed keyless algorithms

Symmetric and asymmetric, both algorithms uses key which shared between two parties before transmitting the information. In this paper, keyless algorithm is designed in order to save certain resources and avoid extra processing of key generation, management and transmission.

Encryption procedure

The proposed algorithm is based on addition of averaged value of all character's, in the plain text. The step by step encryption process of keyless algorithm is:

Step 1: Take the plain text and divide the text into multiple blocks of 128 bits (16 characters). If the block size is less than 128 bits, padding are added to make it 128 bit block. Convert these characters into their respective decimal value.

Step 2: Take average value by summing up all the decimal value divided by 16.

Step 3: Add the average value in original decimal values of plain text characters.

Step 4: After adding the average value, convert these decimals into characters, which is the cipher text.

In encryption, floating point values are round off to make it decimal values.

Decryption procedure

The most favorable point in this algorithm which makes it slightly different from other keyless algorithms is that the encryption and decryption process is a bit different. The encryption and decryption algorithms are not exact reverse of each other as there are some keyless algorithms that have exact reverse case between encryption and decryption algorithm (Jiwan et al., 2012) (Akhil et al., 2012). The step by step decryption process of keyless algorithm is:

Step 1: Take the cipher text and make chunks of 128 bits (16 characters). Convert these characters of cipher text into their respective decimal values.

Step 2: Add all the decimal values of cipher text and divide there sum by 2, this gives a new number.

Step 3: Divide this new number by 16.

Step 4: After dividing by 16, subtract it from the decimal value of received cipher text.

Step 5: After subtracting, convert these decimals into characters, which the required plain text.

In decryption, floating point values are round off to make it decimal values. (Hunt et al., 2006).

Performance Analysis

The key concept behind the emergence of cryptographic algorithm is to protect the information during transmission through an unreliable path. The regulation of an encryption algorithm depends upon the adjustment between speed and security (Jiwan et al., 2012). Algorithms which possess high security with better speed against different attacks are considered as good. The proposed algorithm is testes and analyzed against different attacks.

Pattern Attack

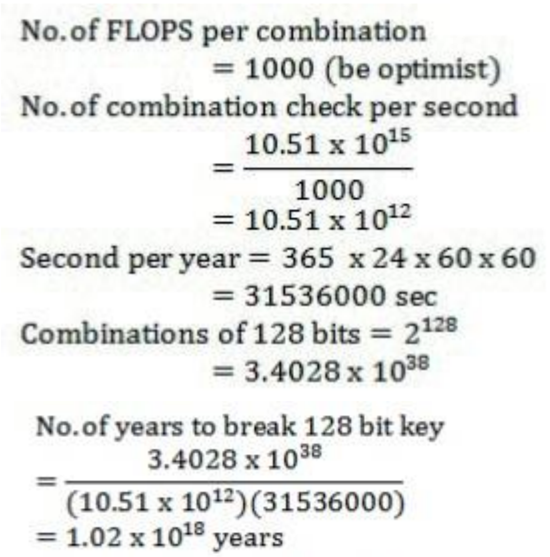
Block cipher encryption algorithms has an issue that for same key and input text they produces same output text. Using this weakness, an intruder can use pattern attack and replay attack to find the plain text (Al-Abiachi et al., 2011). This issue is eliminated in stream cipher but stream cipher takes time to encrypt or decrypt the text, as stream cipher has large execution time (Mathew et al., 2005). The proposed algorithm takes small amount of time to encrypt the data as the consecutive blocks does not depend on each other.

Avalanche Effect

In cryptography, to design or analyze any algorithm, avalanche effect must be taken into account. It is one of the desired properties for any successful algorithm. In proposed algorithm, change in single character of plain text, completely change the cipher text.

Brute Force Attack

Brute force attack uses all combinations to deduce the information (Ahmad et al., 2009). In this type of attack, attacker or intruder tries every single possible key or plaintext to decrypt the cipher text or uses all combinations to sort out the plaintext or key. Exhaustive key search needs 2n operations to find the appropriate key where n is the number of bits. The number of key bits used in this algorithm is 128, so the number of combinations is 2128 = 3.04 x 1038. The fastest computer can perform 10.51 x 1015 FLOPS (Floating point Operations per Second) (FLOPS, 2014).



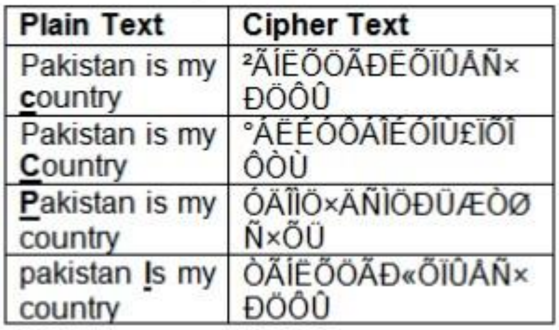
$$\text{No. of FLOPS per combination} = 1000 \text{ (be optimist)}$$

$$\text{No. of combination check per second} = \frac{10.51 \text{ x } 10^{15}}{1000} = 10.51 \text{ x } 10^{12}$$

$$\text{Second per year} = 365 \text{ x } 24 \text{ x } 60 \text{ x } 60 = 31536000 \text{ sec}$$

$$\text{Combinations of 128 bits} = 2^{128} = 3.4028 \text{ x } 10^{38}$$

$$\text{No. of years to break 128 bit key} = \frac{3.4028 \text{ x } 10^{38}}{(10.51 \text{ x } 10^{12})(31536000)} = 1.02 \text{ x } 10^{18} \text{ years}$$



Plain Text	Cipher Text
Pakistan is my country	²ÃÍËÕÖÃĐËÕÏÛÂÑ× ĐÖÔÛ
Pakistan is my Country	°ÁËÉÓÔÁÎËÓÍÙ£ÏÕÎ ÔÒÙ
Pakistan is my country	ÓÄÎÌÖ×ÄÑÌÖĐÜÆÒØ Ñ×ÕÜ
pakistan Is my country	ÒÃÍËÕÖÃĐ«ÕÏÛÂÑ× ĐÖÔÛ

Limitations

The proposed algorithm is simple, secure, fast and has less complexity in terms of mathematics (addition of average value) and coding. In keyless algorithm, protection of encrypting and decrypting algorithm is important. If the idea behind encryption/decryption is revealed, than the algorithm losses its importance.

CONCLUSION

The proposed keyless algorithm is simple, fast and has eliminated the concept of key which needs extra resources for key generation, transmission and management. This algorithm can be used with other ciphers (with both symmetric and asymmetric) to improve the security.

REFRENCES

0 Ahmad AA, Biri HA, Zeghlache D. TIBC: Trade-off between Identity-Based and Certificateless Cryptography for future internet. *IEEE 20th International Symposium on Personal, Indoor and Mobile Radio Communications, Evry, France*, Sept. 2009, pp, 2866 - 2870.

0 Akhil KA, Satvika MB, Kumar A. (2012). Keyless user defined optimal security encryption. *International Journal of Computer and Electrical Engineering*. 4(2):99–103.

0 Al-Abiachi AM, Ahmad F, Ruhana K. A Competitive Study of Cryptography Techniques over Block Cipher. *13th International Conference on Computer Modelling and Simulation (UkSim),* 2011, pp. 415 – 419.

0 Brassard G. (2000). A note on the complexity of cryptography. *IEEE* Transactions. 232-233.

0 FLOPS. (n.d.). Retrieved October 13, 2014, from http://en.wikipedia.org/wiki/FLOPS

0 Forouzan BA. Cryptography and Network Security: McGraw-Hill, 2008.

0 Jiwan P, Saisumanth N, Rupa C, Saradhi TVA. (2012). Keyless JS algorithm. *in proceeding of International journal of engineering*

science and advanced technology. 2: 1397-1401.

0 Hoffstein JJ, Pipher, Silverman JH. *An Introduction to Mathematical Cryptography*, 1st ed. USA: Springer, 2010.

0 Hunt BR, Rosenberg LKR, Coombes JE, Osborn GJ. *A guide to MATLAB: for beginners and experienced users*. Cambridge University Press, 2006.

0 Mathew S and Jacob KP. A New Fast Stream Cipher: MAJE4. *Proc. of annual IEEE, INDICON 2005,* Dec 2005, pp. 60-63.

0 Menezes AJ, Oorschot PCV, Vanstone SA. *Handbook of Applied Cryptography*, 5th ed. USA: CRC Press Inc., 2001.

0 Nadeem A and Javed MY. *A Performance Comparison of Data Encryption Algorithms, in Information and Communication Technologies, 2005. ICICT 2005. First International Conference on*, 2005, pp. 84-89.

0 Schneier B. *Applied Cryptography: Protocols, Algorithms, and Source Code in C*, 2 Ed.: John Wiley and Sons, November 1995.

0 Sudha VMVS, Brindha K, Agilandeeswari L, Ramya G. (2012) Implementation of Enhanced Data Encryption Standard on MANET with less energy consumption through limited computation*. In Proceeding of International Journal of Engineering Research and Development.* 2: 46-52.