International Journal of Information, Control and Computer Sciences
ISSN: 2517-9942
Vol:2, No:2, 2008

Introducing a Platform for Encryption Algorithms

Ahmad Habibizad Navin, Yasaman Hashemi, and Omid Mirmotahari

***Abstract*—**In this paper, we introduce a novel platform encryption method, which modify its keys and random number generators step by step during encryption algorithms. According to complexity of the proposed algorithm, it was safer than any other method.

***Keywords*—**Decryption, Encryption, Algorithm, security.

I. Introduction

DATA encryption is the base of cryptography, by which the data will be unknown to other users[1]. The easiest and most fundamental ways for cryptography are substitute and permute data by combining them together; more effective ways will be produced. There are two kinds of cryptography, Classic method (Substitution, Permutation and Product) and Modern method (Symmetric key, Asymmetric key). The classic methods are the base of modern methods [5]. In the classic methods we always use substitute or permute data for encryption, but in the modern methods we use difficult and complex ways to encrypt data. In that manner we believe that the hackers will not be able to find the original data and the way of encryption. In classic method the keys in encryption and decryption parts are equal, i.e. it's easy to find the second key from the first one. The key must be sent to the receiver through a safe channel. In public key method, finding Encryption and Decryption key isn't easy .In these methods you can easily find a key without causing any problem for another key. In modern and complex encryption methods you can find some rules, which are used, in classic methods [6-7]. In the past cryptographers used simple methods for encryption, but today we make difficult and complex keys, so the attackers can not do anything with the received text until the key and the method of encryption is found.

Stream cipher is one the symmetric ciphers [8]. There were a group of encryption algorithms in these systems, which encrypt the characters of the plain text in one time, and the text is viewed as a strong of characters.

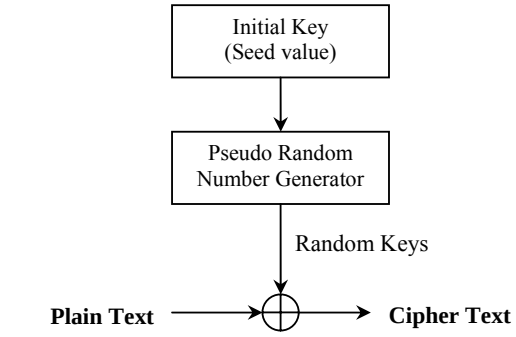
A. H. Navin is a member of Islamic Azad University Tabriz Branch, Tabriz, Iran, Computer Department. He is also collaborated with computer Research laboratory, IAUT-CRL He is also a part time member of Islamic Azad University Mamaghan branch, Mamagan, Iran.

Y. Hashemi is a member of Islamic Azad University Varamin Branch, Varamin, Iran.

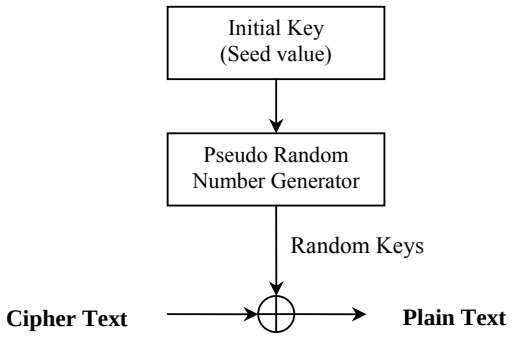
O. Mirmotahari, is with the Nanoelectronic system group at the Department of Informatics, University of Oslo, Norway.

Plaintext	1 1 0 0 1 1 0
Key stream	0 1 0 1 1 0 1
Cipher text	1 0 0 1 0 1 1

One of the stream ciphers is One-time-pad that in this algorithm first of all a random serial of bits are selected as key, then the plain text is converted to a serial bits and finally these serial bit strings is XOR-ed together. The stream cipher will be created which cannot be broken [6, 9-10], illustrated in Fig. 1.



a) Encryption



b) Decryption

Fig. 1 Stream cipher

This kind of encryption is secured against all attacks and clever vender can not break this key, this algorithm comes from information theory, but it have some problems as follow:

- The key cannot be saved, sender and receiver must carry the key and if each of them is attacked with the

sniper then, key will be discovered.
- The capacity of the string length depends on the length of the key.
- This method is sensitive to lost or added characters.

As we want one-time-pad so the string of the key must be completely random. But there is a problem that if the first string key is random, then the second generator (Decryption side) cannot generate the same string (RSQ). For this reason we should use pseudo random for encryption (PRSQ). In this algorithm by receiving a initial key the generator generates a stream of keys randomly, for decryption on other side it is enough the same generator start to generates keys from initial key. The generator will generate the same stream keys [11], [4], [13], such as LFSR (linear feedback shift register) [12].

Today many different methods are proposed for data encryption as follow:

- A novel encryption algorithm secure against chosen-plaintext attacks is proposed [14]. The method uses the original message itself as a time-varying key for encryption. As opposed to traditional key algorithms, one of the keys in the algorithm presented depends on the message itself. Two encryption matrices are generated by means of singular value decomposition (SVD)[15],[16], using a portion of the message.
- A novel image scrambling algorithm is proposed based **on Arnold transform Encryption Algorithm** [17].
- A new joint encryption and lossless compression technique designed for large image is introduced. The proposed technique takes advantage of the Mojette transform [20] properties, and can easily be included in distributed storage architecture. The basic crypto-compression scheme presented is based on a cascade of Radon projection [21] which enables fast encryption of a large amount of digital data.
- A structure-independent fault detection scheme for the AES [22] Sub Bytes transformation has been presented. It has been obtained new formulations to check the relationship between the input and output of the S-box and the inverse S-box. The presented scheme detects most of the random faults in the Sub Bytes and Shift Rows transformations independent of the location of the faults [22 - 25].

By combining the result of the research presented above a novel platform for data encryption is presented in the next section.

II. Proposed Encryption Method

The basic task of an encryption algorithm is converting plain text to cipher text in a manner that suggesting the plain text from cipher text is more complex. The security of it related to its complexity. For this propose we can use pseudo random sequence. In this method, the plain text is combined with keys to make the cipher text. The security is related to pseudo random keys complexity. For getting more security we need more complex keys for decryption. We suggest a method in the following.

A. Basic Algorithm

For generating more complex and unpredictable keys, we proposed a platform with three layers as shown in Fig. 2. The first layer by receiving the initial key selector generates a random selection of keys as initial keys for second layer. The second layer generates by receiving these keys and PRNG selector generates a random sequence. These random sequences applied to the Combination Rules of the third layer for generating the final key. Cipher text will be the exclusive-or of the final key and plain text.

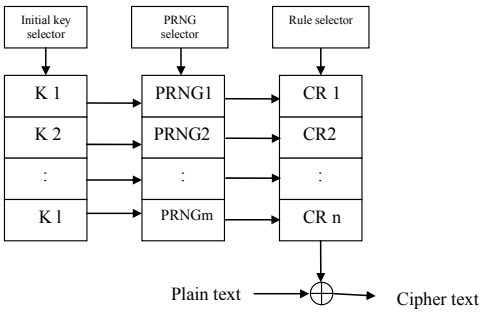


Fig. 2 Novel Encryption model

B. Increasing Security

To increase security of the basic method the presented platform sued the following properties:
- Select initial keys from the keys which are in Rom in the first layer.
- Generate some random sequence by Pseudo random generators with these keys in the second layer.
- Combine the pseudo sequence by combination rules to generate final key for encryption.

III. Evaluation

For evaluation of the new ones with traditional methods the number of experiments to break the methods is compared in Table I. Let *m* be the number of bits in the key, *l* be the length of the text and *n* be the number of the keys then the number of experiments for broken them are provided in Table I. The efficiency of proposed method is clear by comparison.

TABLE I
COMPARE OF ALGORITHMS

I=1024 m=8 n=32	Max Experience	Requirement	Solution
2^{8192}	$2^{I\times m}$	-Compound method	RSQ
2^{8}	2^{m}	-Compound method -Serial key generating of pseudo	PRSQ
2^{56}	2^{56}	-DES algorithm	DES
2^{256}	$2^{m\times n}$	-Number of basic keys in ROM -All algorithm for selecting basic key -All algorithm for generating key -All algorithm of compound circuit Selecting one of variable algorithm	Proposed Method

IV. CONCLUSION

In this paper we have proposed a new method for data encryption. The base of this method is by generating more complex keys during the encryption. Related to this method working in the following area have some valuable benefits:

1. Giving efficiency Rom structure,
2. Giving the better key selection algorithm,
3. Using removable ROM to achieving more security,
4. Giving the better combing method,
5. Modeling each layer with data oriented approach.

REFERENCES

[1] U. D. Block, "Data Communication and Distributed Networks", Reston Block, 1992.
[2] J .E. Ettinger, "Information Security", Chapman & Hall, 1993.
[3] Charles P. Pfleeger, "Security in Computing", Prentice Hall, 1989 William L. Schweber. "Data Communication", MC Grew-Hill 1988.
[4] D. Elizabeth, R. Denning, "Cryptography and Data Security ", Addition – Wesley 1983W.-K. Chen, *Linear Networks and Systems* (Book style). Belmont, CA: Wadsworth, 1993, pp. 123–135.
[5] Yongdae Kim, "PRNG, Block and Stream" September 4, 2001.
[6] Prof. Benny Chor, "Introduction to Modern Cryptography", School of Computer Science, 1987.
[7] Mitchell Chris J., "Some Observation on the Bit _ Search Generator", Technical Report RHUL – MA- 2004-3, 20 October 2004.
[8] K. C. Zeng, C. H. Yang, D. Y. Wei , and T. R. N. Rao, " Pseudo Random Bit Generators in Stream – Cipher Cryptography " , IEEE Computer , February 1991 , PP. 8-17.
[9] Chris J. Mitchell, Alexander W. Dent, "International Standards for Stream Cipher", Information Security Group, Royal Holloway, University of London, 1998.
[10] A. Menezes, P. Van Oorschot, S. Vanstone, "Block Cipher", CRC Press, 1996, www.cacr.math.uwaterloo.ca/hac.
[11] Kim Yongdae, PRNG, "Block and Stream Cipher", September 4, 2002.
[12] Nguyen Cao Dat, "Network Security", dat@dit.hcmut.edu.vn.
[13] C. Chan, J. M. Eng, "Global Corporate Communications with Integrated Services Digital Networks", International Journal of Satellite Communications, Vol .9 No.5, Sep- Oct 1991, pp.267- 277.
[14] Chung-Ping Wu and C. C. Jay Kuo, "Design of integrated multimedia Compression and encryption systems," IEEE Transactions on Multimedia, vol. *7,* no. 5, 2005, pp. 828–839.
[15] S. H. Jensen, P. C. Hansen, S. D. Hansen, and J. Aa. Sŕensen, "Reduction of broad-band noise in speech by truncated qsvd," IEEE Transactions on Speech and Audio Processing, vol. 46, no. 6, 1995, pp. 1737–1741.
[16] P. C. Hansen and S. H. Jensen, "FIR filter representations of reduce-rank noise reduction," *IEEE* Transactions on Signal Processing, vol. 46, 1998, pp. 1737–1741.
[17] Zou Jian-cheng, Tie Xiao-yun. Arnold transformation of digital image with two- dimensions and its periodicity [J]. Journal of North China University of Technology, 2000, pp. 12-15.
[18] Yang Ya-li, CAI Na, NI Guo-qiang. Digital image scrambling technology based on the symmetry of Arnold transform. Journal of Beijing Institute of Technology, 2006, Vol.15, No.2: pp. 216-220.
[19] Chen Ming, PING Xi-jian. Image steganography based on Arnold transform. Computer application research, 1, 2006, pp. 235-238.
[20] F. Autrusseau, JP. Guedon, and Y. Bizais, "Watermarking and cryptographic schemes for medical imaging," in *SPIE Medical Imaging*, 2003, pp. 532–105.
[21] F. Autrusseau, B. Parrein, and M. Servieres, "Lossless compression based on a discrete and exact radon transform: A preliminary study," in *ICASSP*, 2006, pp. 466 – 468.
[22] G. Bertoni, L. Breveglieri, I. Koren, P. Maistri, and V. Piuri, "Error Analysis and Detection Procedures for a Hardware Implementation of the Advanced Encryption Standard," *IEEE Trans. on Computers*, vol. 52, no. 4, April 2003, pp. 492-505.
[23] G. Bertoni, L. Breveglieri, I. Koren, and P. Maistri, "An Efficient Hardware-based Fault Diagnosis Scheme for AES: Performances and Cost," *In Proc. of DFT2004*, Oct. 2004, pp. 130-138.
[24] L. Breveglieri, I. Koren, and P. Maistri, "Incorporating Error Detection and Online Reconfiguration into a Regular Architecture for the Advanced Encryption Standard," *In Proc. of the DFT2005*, Oct. 2005, pp. 72-80.
[25] K. Wu, R. Karri, G. Kuznetsov, and M. Goessel, "Low Cost Concurrent Error Detection for the Advanced Encryption Standard," *In Proc. of the 2004 International Test Conference*, Oct. 2004, pp. 1242-1248.