IOSR Journal of Engineering (IOSRJEN) **www.iosrjen.org**
ISSN (e): 2250-3021, ISSN (p): 2278-8719
Vol. 09, Issue 2 (February. 2019), ||V (I) || PP 01-04

Evaluation of Symmetric Key Cryptosystem Based On Randomized Key Block Cipher Algorithm to Cryptanalytic Attacks

Dr. S. Arul Jothi
Assistant Professor, Department of Computer Science,
Fatima College, Madurai, Tamil Nadu, India, 625018
Corresponding Author: Dr. S. Arul Jothi

Abstract: In a world of interconnected computers and networks, security is a major challenge in relation to data exchange among them. The information security through encryption has been evolved to address different issues in such process. In this context the evolution and evaluation of new encryption system is inextricably linked to the process of realizing ever increasing network security needs. A continuous development of new encryption systems are necessitated with the advancement in security and efficiency needs. In the paper symmetric key cryptosystem based on randomized key block cipher a novel dynamic cryptographic key generation scheme is proposed. This paper proposes to evaluate the enduring capacity of this algorithm to various cryptanalytic attacks viz., Differential Cryptanalysis, Linear Cryptanalysis and Poly-alphabetic Nature Test. None of the traditional attacks are designed to decrypt this encryption algorithm as the use of key scheme is different in it and therefore robust to the conventional cryptanalytic attacks.

Date of Submission: 22-01-2019 Date of acceptance: 05-02-2019

I. INTRODUCTION

Twenty first century is known as an age of information. In this era information is an economic commodity. Information has economic value and production of it incur cost. Securing the information has become one of the most significant problems for distributing new information. The cryptographic technology plays a leading role in securing the owners right on produced information. The technique used to convert the original data into secret code or data is called data encryption technique for all kinds of data such as textual data, image data or multimedia data for secured communication over a network as explained in [1]. While the decryption is the reverse process. An important ingredient of encryption/ decryption process is the idea of key. To decipher an encrypted file, a key is required that was used to encrypt it.

The Key is an input to the encryption algorithm, and this value must be independent of the plaintext, this input is used to transform the plaintext into cipher text. In the decipher side, the inverse of the key will be used inside the algorithm instead of the key. In [2] different keys are also used in other cryptographic algorithms, such as digital signature schemes and keyed-hash functions, often used for authentication. For a well-designed algorithm, enciphering the same plaintext but with a different key should produce a totally different ciphertext. Similarly, decrypting should produce the same plaintext.

Key generation is the process of generating keys for cryptography. A key is used to encrypt and decrypt whatever data is being encrypted/decrypted as discussed in [2]. Computer cryptography uses integers for keys. In some cases keys are randomly generated using a truly random number generator (RNG) or pseudorandom number generator (PRNG). A PRNG is a computer algorithm that produces data that appears random under analysis as discussed in [3]. PRNGs that use system entropy to seed data generally produce better results, since this makes the initial conditions of the PRNG much more difficult for an attacker to guess.

The need for random and pseudorandom numbers arises in many cryptographic applications as described in [4]. Common cryptosystems employ keys that must be generated in a random fashion. Cryptographic protocols also require random or pseudorandom inputs at various points, e.g., for auxiliary quantities used in generating digital signatures, or for generating challenges in authentication protocols. Security of an algorithm rests in keys. If cryptographically weak process is used to generate keys then the whole system will be weak. Only the key should be secret. Cryptographic mechanisms depend on the confidentiality of keys. In this paper, basic tests have been conducted for the qualitative evaluation of the encryption algorithm and the results have been discussed. Test has been conducted to obtain cipher text generated by the encryption algorithm, to reveal the poly-alphabetic property of the encryption algorithm and to obtain image encryption and decryption. They are explained in the following sub sections.

II. CIPHERTEXT GENERATION FROM PLAINTEXT MESSAGE

In this section, results are generated to show the difference in cipher text produced for the proposed algorithms using the same plain text message. For a given plaintext message, the proposed encryption algorithms have been executed and the ciphertext messages are obtained. Figure 3.1 shows plain text message used for the test and Figure 3.2 is the ciphertext got after encryption for RKBC algorithm.

DBMS

A Database Management System (DBMS) is a software system designed to efficiently store, retrieve, manipulate, and query large amounts of data. Since the introduction of the relational data model in 1970, the database management system industry has grown to $100 billion dollars a year and increases by more that 25% every year. With the new and emerging internet applications posing new requirements in the DBMS design and implementation, the database market is expected to grow even faster, and database design and implementation techniques are constantly evolving to meet the new requirements.

¹•Ñ‹íÍb/5UîY4½‹8ð§%Ú&B.€¡emùCO²I^êÔf+ñ®šî-i - • €¸Ê˜[Ž;=²#ÊòH*ƒ*ÿä ñ #N¶=Z; úÝÔ&ÞÖèéÏ3^‹kµª ë„ïn# ýeP7.FÄK¹1Z÷9±þ$}8<¾q ÓHaÔeís5”u9cp+BySîâ×Ù×óÿm%ûV”'4çX…8Dd÷o /íĺÿÁ$»W¤òITçV)½ûš67ãÝmXå¤n½Ô^¨ôhÂn2{TÕ »€7ªÓ¡’X åÔÜªzët°!7□Jì'X Đó·T DijË ®¾&ÆÍ+ ú’(ö*pÍÿü‘:k—Oó¦1 5A0ãÍåæ hwa)Ö □ ÿ‘.3àý¨~Âg¶MTÝ)»ìÕeÈ□ âÕ*©Đ>hOå¤$i y‘wabýĐh]œ Đ¨¾›□ Þ¨ Ÿ OÚøŽ”™ õcx,)›?Qð-€¾ÚµÃ^Í¹K® □ ¤àIøPh¥i'XĐî± ö‡¼½8Ê øª} L2I-µ®^Äâ»›®!_Ç¦:h =°Và ä¥ V M Œ …Á — > ¾”ÛÀ^¿J¯² ¼JZC§: à.Üd±”¸ ®×O

Figure 2.1 Plaintext message used for encryption Figure 2.2 Ciphertext message for RKBC algorithm

It is noted that the number of lines of text in plaintext and apparent number of lines of ciphertext generated are not same. It is because of the fact that in the ciphertext generated, there exists special control characters such as carriage return and line feed etc. Wherever there is a linefeed character in the ciphertext output, it goes to the next line in the ciphertext printout. This can cause more lines in the ciphertext printout. Similarly, after every line of plaintext there is a line feed character and thus the plaintext printout will show exact number of lines as found in the plaintext message. But the number of characters including special characters will be same in both plaintext message and ciphertext message.

III. POLY-ALPHABETIC NATURE TEST

In a block cipher with block size of 256 bits (32 characters), blocks of 32 plain text characters are converted to cipher text characters at a time. In this test the poly-alphabetic substitution capability of the encryption is revealed in [5]. For the same plain text characters within one block, a poly-alphabetic encoding should produce distinct cipher text characters in the ciphertext output block. To test this feature, a block of plaintext input data with two 16 identical characters (‘J’,’P’) is chosen. The cipher is executed with 8 different keys and output data block of each round is obtained. The ciphertext output block is shown in figure 3.3 for RKBC algorithm.

In a block cipher that is said to have better cryptographic strength, a change of one bit in the key as in [6] or in the plain text block affects many bits in the cipher text output block. First a block of plaintext characters is converted into cipher text characters and the corresponding bit pattern is obtained. Then with a change of only one bit in the key and using the same plain text character block the output cipher text character block is obtained and the corresponding bit pattern is analyzed. The number of bits changed with one bit change in the key can be determined. Similarly, a change of one bit in the plain text block is introduced to determine the changed number of bits for the same encryption key.

Table no 1: Poly-alphabetic test result for RKBC algorithm

JJJJJJJJJJJJJJJPPPPPPPPPPPPPPPP	← Input data block
–oÃL;íÇÂàE/ªÎBkVÊLO¥ I VÀQ7d*Æ	← Output data block for key1
@QdggÚ¢"~Ø¹L?ÓYpóúÔy#„UÏõ}ÀºH	← Output data block for key 2
$O/ç5œÊ$O/ç5œÊEý|ã‰ ¯–ýEý|ã‰¯–ý	← Output data block for key 3
• Ó[öQ-W%€)»óa¥ • —h+ÓRå%§e¦T³§z©	← Output data block for key 4
9À6æÄLˆ¢¯zHÚ0ÅÓ I • ÂA†à©ŠS	← Output data block for key 5

„¹?ç›A¯(#r}Æ—æ=M– ±b VdÉ[1€”×°5p	← Output data block for key 6
•ý‰@®” • d.JC#Á,ð7´ÑÑêd3ÇP&Žå³·	← Output data block for key 7
MøöwãSvU=e_`ê±¾µJÇËþ+Ú[IŽñ?‘¦œÎ	← Output data block for key 8

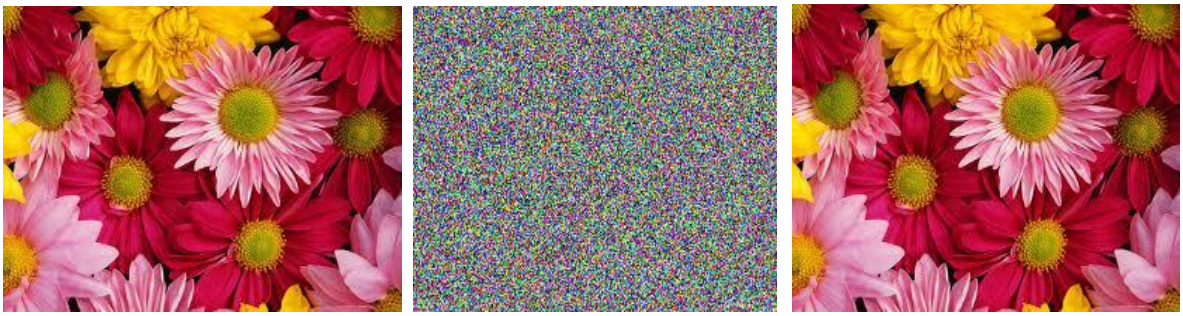
IV. IMAGE ENCRYPTION AND DECRYPTION

A digital image is defined as a two dimensional rectangle array. The elements of this array are denoted as pixels. Each pixel has an intensity value represented as a digital number and a location address in terms of row and column as discussed in [7].

An encryption scheme should be capable of encrypting plaintext messages and images to generate ciphertext messages and cipher images without leaving any trace of the plaintext or the image in the encrypted output as discussed in [8]. An image contains redundant information and there is strong correlation between adjacent pixels in horizontal, vertical and diagonal directions of the image. A weak encryption may not be able to hide these aspects of the original image in the ciphered image. Therefore, even if the ciphertext message generated from a plaintext message by an encryption scheme is secure, the cipher image generated from a plain image may not be hiding certain characteristics of the original image as discussed in [10]. This can give some clues to the crypt analyst regarding the nature of the original image there by making cryptanalysis easier as explained in [9]. Therefore, it is important that an encryption scheme should be analyzed using images. The following image encryption and decryption results are presented for the observation on the outcome of encryption and decryption processes.

a) Original image **(b) cipher image** **(c) decrypted image**

Figure 4.1 Encryption and decryption of gray scale image ‘Stone house’ for RKBC algorithm



(a) Original image **(b) cipher image** **(c) decrypted image**

Figure 4.2 Encryption and decryption of color image ‘Fish’ for RKBC algorithm

In this Examples, the original gray scale image and color image is encrypted as an image file by proposed RKBC encryption scheme, which loses its original outline, colors, and characteristics. It will be highly secured though the image file is placed in public transmission channel of computer internet. In [10] image file is decrypted with the reverse of the encryption keys and are able to recover complete original image. An intruder who selects different key or different methods to create encryption keys will not be able to obtain proper decryption keys, and thus unable to recover original images.

Clearly from the above experiments results, the proposed RKBC encryption method was lossless, since the decrypted image is exactly similar to the original images without any loss of data through encryption and decryption operations of this method.

V. CONCLUSION

Different characteristics of the RKBC algorithms are presented with mathematical proof. The proposed algorithms are tested on text and images. With a change of only one bit in the key and using the same plaintext character block the output ciphertext character block is obtained and the corresponding bit pattern is analyzed. The number of bits changed with one bit change in the key is determined, as a result good avalanche effect is achieved which is one of the desired properties of encryption algorithm. Different standard images are used as input and the encrypted images and decrypted images were obtained. Thus the proposed scheme can shuffle the plain image efficiently in the permutation process.

REFERENCES

[1]. Aniket Kesharwani, Hemant Gupta. Survey on Data Hiding in Encrypted Images. International Research Journal of Engineering and Technology (IRJET). 2015; 2(3): 144 – 150.
[2]. Harshala B. Pethe, Dr. S. R. Pande. A Survey on Different Secret Key Cryptographic Algorithms. IBMRD's Journal of Management and Research. 2014; 3(1): 142 – 150.
[3]. Mihir Bellare, Shafi Goldwasser, Daniele Micciancio. Pseudo-Random Number Generation within Cryptographic Algorithms: the DSS Case, Advances in Cryptology - Crypto 97 Proceedings. Lecture Notes in Computer Science. Springer Verlag. 1997;1294.
[4]. Makoto Matsumoto, Takuji Nishimura. Dynamic Creation of Pseudorandom Number Generators. Monte Carlo and Quasi-Monte Carlo Methods. Springer. 2009; 589-602.
[5]. YekiniN. Asafe, Aigbokhan E. Edwin, Okiki F. Mercy. Cryptography System for Online CommunicationUsing polyalphabetic Substitution Method. Int. J. Advanced Networking and Applications. 2014; 6(1): 2151-2157.
[6]. Chandra Prakash Dewangan, Shashikant Agrawal. A Novel Approach to Improve Avalanche Effect of AES Algorithm. International Journal of Advanced Research in Computer Engineering & Technology. 2012; 1(8): 248–252.
[7]. Varsha Bhatt, Gajendra Singh Chande. Implementation of new advance image encryption algorithm to enhance security of multimedia component. International Journal of Advanced Technology & Engineering Research (IJATER). 2012; 2(4): 13-20.
[8]. Li C and L. Hong, "A New Image Encryption Scheme based on Hyperchaotic Sequences", IEEE International Workshop on Anti-counterfeiting, Security, Identification. pp. 237-240, 2007.
[9]. Changjiu Pu, "An Encryption Scheme for Color Image", International Review on Computers & Software, Vol. 7, pp. 3719-3723, 2012.
[10]. Hiral Rathod, Mahendra Singh Sisodia, Sanjay Kumar Sharma. Design and Implementation of Image Encryption Algorithm by using Block Based Symmetric Transformation Algorithm. International Journal of Computer Technology and Electronics Engineering (IJCTEE). 2011; 1(3): 7-13.

Dr. S. Arul Jothi. "Evaluation of Symmetric Key Cryptosystem Based On Randomized Key Block Cipher Algorithm to Cryptanalytic Attacks." IOSR Journal of Engineering (IOSRJEN), vol. 09, no. 02, 2019, pp. 01-04.