A performance analysis of Generalized Key Scheme Block Cipher (GKSBC) algorithm to Cryptanalytic Attacks

Dr. S. Arul Jothi

Department of Computer Science, Fatima College, Tamilnadu, India

Abstract— *Information is a commodity. Information has economic value and production of it incurs cost. Securing the information is posing a considerable challenge. The cryptographic technology plays a leading role in securing the owners right on produced information. A continuous development of new encryption systems are necessitated with the advancement in security and efficiency needs. Cryptanalytic studies have demonstrated the superior capability of recently developed Generalized Key Scheme Block Cipher (GKSBC) algorithm in terms of stability, execution time and encryption quality compared to standard security algorithms. This paper proposes to evaluate the enduring capacity of GKSBC to various cryptanalytic attacks viz., Brute – Force Attack, Differential Cryptanalysis, Integral Cryptanalysis, Linear Cryptanalysis and Rectangle attack. None of the traditional attacks are designed to decrypt GKSBC encryption as the use of key scheme is different in it and therefore robust to the conventional cryptanalytic attacks.*

Keywords— AES, Cryptanalysis, DES, block cipher, symmetric, differential, linear.

I. INTRODUCTION

Information is an important input as well as an end product; the production of it involves cost. This necessitates the commodification of information which includes exclusive use of it. In this process, securing the information as commodity posses a challenge as the property right over the information is still a problem. This scenario leads to free rider problem and reducing the incentive to invest in information production and recovering a nominal rate of profit. The role of encryption in securing the owners right on produced information is well acknowledged.

A continuous development of new encryption systems are necessitated with the advancement in security and efficiency needs. Development of new encryption systems and evaluation of its relative performance in terms of its characteristics viz., stability, execution time, encryption quality and endurance to cryptanalytic attacks are part of advancement. Cryptanalytic studies have demonstrated the superior capability of recently developed Generalized Key Scheme Block Cipher (GKSBC) algorithm in terms of stability, execution time and encryption quality[1,2] compared to standard security algorithms. The prevailing cryptsystems using symmetric block ciphers either manipulate the original file with keys or manipulate the positions. A hybrid cryptscheme GKSBC manipulates the positions using keys this cryptscheme was found to be stable, producing quality and efficient encrypts. GKSBC crypt algorithm combines the idea of keys as position pointers and input matrix as co operand in the encryption/decryption process. This paper proposes to evaluate the enduring capacity of GKSBC to various cryptanalytic attacks.

II. RELATED STUDIES

Cryptology comprises two complementary fields: cryptography and cryptanalysis. In cryptography one is concerned with the development of techniques for providing services such as data confidentiality, and entity authentication. In cryptanalysis one is concerned with methods to attack these cryptographic algorithms, that is, to assess and explore design features that may lead to the discovery of some piece of secret information.

The two widely accepted and used cryptographic methods are symmetric and asymmetric. Symmetric key encryption is also known as shared-key, single-key, secret-key, and private-key or one-key encryption. In this type of message encryption, both sender and receiver share the same key which is used to both encrypt and decrypt messages. Sender and receiver only have to specify the shared key in the beginning and then they can begin to encrypt and decrypt messages between them using that key. The 3DES and AES ideally belong to the category of symmetric key cryptosystem.

Symmetric encryption techniques are almost 1000 times faster than asymmetric techniques as they require less computational processing power. Symmetric key ciphers use the same key for encryption and decryption, or the key used for decryption is easily calculated from the key

used for encryption. Symmetric key ciphers can be grouped into block ciphers and stream ciphers.

Block ciphers [2] encrypt blocks of data (typically 64 or 128 bits) in a fixed key-dependent way. The design of block ciphers is a well-studied area of research.

Block ciphers play an important role in many cryptographic and security protocols. They are used to conceal confidential information, not only during its broadcast over a public channel, but also when it is stored. The security of these protocols and storing procedures relies on the security of the underlying block ciphers against various attacks. The field of cryptanalysis of block ciphers focuses on assessing the security of block ciphers. The process of assessment of the security of a given block cipher is mostly concerned with applying various cryptanalytic techniques to the block cipher. Each of these techniques has a different attack model and aims at exploiting different design flaws.

III. CRYPTANALYSIS

Cryptanalysis is a process of finding weaknesses in cryptographic algorithms and using these weaknesses to decipher the ciphertext without knowing the secret key (instance deduction). Sometimes the weakness is not in the cryptographic algorithm itself, but rather in how it is applied that makes cryptanalysis successful. An attacker may have other goals as well, such as:

- Total Break - Finding the secret key.
- Gobal Deduction - Finding a functionally equivalent algorithm for encryption and decryption that does not require knowledge of the secret key.
- Information Deduction - Gaining some information about plaintexts or ciphertexts that was not previously known.
- Distinguishing Algorithm - The attacker has the ability to distinguish the output of the encryption (ciphertext) from a random permutation of bits.

The goal of the attacker performing cryptanalysis [4] will depend on the specific needs of the attacker in a given attack context. In most cases, if cryptanalysis is successful at all, an attacker will not be able to go past being able to deduce some information about the plaintext. However, that may be sufficient for an attacker, depending on the context.

There are several types of attacks that a cryptanalyst may use to break a code, depending on how much information they have. There are numerous techniques for performing cryptanalysis, depending on what access the cryptanalyst has to the plaintext, ciphertext, or other aspects of the cryptosystem. Below are some of the most common types of attacks:

3.1. Brute – Force Attack

Brute force attack is a strategy that can be used against any encrypted data by an attacker who is unable to take advantage of any weakness in an encryption system. It involves systematically checking all possible keys until the correct key is found. The key length used in the encryption determines the practical feasibility of performing a brute force attack, with longer keys exponentially more difficult to crack than shorter ones. If n is large then the key space is of n^2 dimension and it is impossible to search the key space.

In our GKSBC algorithm if the block size is 8, $nP_n = 8P_8$ permutations is possible. For each block (or) 8×8 matrix 8^2P8^2 key set may be possible (i.e.) $64P_{64} = 64! = 1.26887 \times 10^{89}$ key sets may be possible. In a file if there are m blocks of $n \times n$ matrix, the number of possibilities multiplied by factor of M and therefore deciphering the key would get complicated by that factor.

3.2. Differential Cryptanalysis

Differential cryptanalysis [16,17] is a chosen plaintext attack where the attacker encrypts two chosen plaintext blocks and uses the differences between the chipertext to deduce the key. An attackér chooses the difference ΔP, between plaintexts (P_1, P2) and studies the propagation of the changes in the encryption process.

Sort the array of N known plaintext/cipher texts by plaintexts and then search for pairs, with particular useful input differences the total time complexity is O (nlogn). Here we will not get any useful input differences since our key is random positions of a matrix the difference cannot be compared and analyzed.

Let us proceed with an important but simple to analyze example of plaintext redundancy. Suppose that the plaintext source produces block of w bytes and has entropy of e bytes. So that there are w – e redundant bytes per block. For example

Plaintext w = {noeljose} and e = 4 = {nljs}

r = w – e = 8 – 4 = 4 = {o,e} repeated.

Cipher text = {∂Þ@ {Q5N&}

Here in the above redundant character o & e changes to different characters. {o→ Þ , o → 5, e →@, e → &}. We have made a fast differential attack on the cipher which succeeds with 2 chosen pairs {o, e}. We cannot guess the difference though there are redundant characters. Our GKSBC Cipher is more secure against this differential attack.

3.3. Integral Cryptanalysis

In cryptography, integral cryptanalysis is a cryptanalytic attack that is particularly applicable to block ciphers based on substitution-permutation networks. In integral cryptanalysis [8], n will represent the number of words in the plaintext and ciphertexts and m denotes the number of plaintexts and ciphertexts considered.

In an attack one tries to predict the values in the integrals after a certain number of rounds of encryption. For this purpose it is advantageous to distinguish between the three cases. Where all the i^{th} words are equal are all different or sum to a certain value predicted in advance. In an attack with our algorithm we take n = 3 and m = 4.

Table.1: Encrypted text in this algorithm for different plain text

Plain text	cipher text
akbar and birbal	áßR p0àdÚ=ÆÁ‡ õ
capital of agra	/F‰Ž'×V ýÞð'•
begum and birbal	âl÷ph`NÛfT÷h]œ'
akbar great ruler	`Ivh` §ú.Ób©NS¤ b

Let us consider i as 4 and analyze the above example. All the characters are different and unpredicted. One word can take m different values. We cannot guess the plain (or) cipher text with the help of integral analysis in our GKSBC algorithm.

3.4. Linear Cryptanalysis

In cryptography, linear cryptanalysis [17,18] is a general form of cryptanalysis based on finding affine approximations to the action of a cipher. There are two phases in linear cryptanalysis. The first is to construct linear equations relating plaintext, ciphertext and key bits that have a high bias that is whose probabilities of holding are as close as possible to 0 or 1. The second is to use these linear equations in conjunction with plaintext-ciphertext pairs to derive key bits.

In our algorithm the function F takes an input(x) and key(k) as input and produces an output(y). We can write this as y = (x, k) mod 2. As the key bits are random in our algorithm and consequently so are the cipher bits to the last round. It is impossible to access the decrypted plaintext and the key with linear cryptanalysis.

3.5. Rectangle attack

The rectangle attack[19] is as follow

i. choose n plaintext pairs(p_a, $p_b = p_a \oplus \alpha$) at random and ask for the encryption of p_α under k_a and p_b under k_b. Denote the set of these pairs by S.
   a. $S = (p_a, p_{b)} = (c,e)$ and $\alpha = 2$
   b. $p_a = c = 1100$ and $\alpha = 2 = 0010$
   c. $p_b = p_a \oplus \alpha = 1100 \oplus 0010 = 1110 = e$

ii. choose n plaintext pairs(p_c, $p_d = p_c \oplus \alpha$) at random and ask for the encryption of p_c under k_c and p_d under k_d. Denote the set of these pairs by T.
   a. $T = (p_c, p_{d)} = (d,f)$ and $\alpha = 2$
   b. $P_c = D = 1101$ and $\alpha = 2 = 0010$
   c. $P_d = p_c \oplus \alpha = 1101 \oplus 0010 = 1111 = f$

iii. Search a pair of plaintexts(p_a, $p_{b)} \in S$ and a pair ofplaintexts(p_c, $p_{d)} \in T$ and their corresponding ciphertexts (c_a,$c_{b)}$ and (c_c,c_d) respectively, satisfying
   a. $p_a \oplus p_b = p_c \oplus p_d = \alpha$
   b. $p_a \oplus p_b = 1100 \oplus 1110 = 0010 = 2 = \alpha$
   c. $p_c \oplus p_d = 1101 \oplus 1111 = 0010 = 2 = \alpha$
   d. $c_a \oplus c_c = c_b \oplus c_d = \delta$
   e. $c_a \oplus c_c = 1000 \oplus 0101 = d \neq \delta$
   f. $c_b \oplus c_d = 1010 \oplus 1011 = 1 \neq \delta$

But in our algorithm second case is not true, since our key is random the ciphertext changes irrationally. So we cannot predict the plaintext with the help of this attack.

3.6. Frequency Analysis

In cryptanalysis, Frequency analysis is the study of the frequency of letters or groups of letters in a ciphertext. It is basically the process of examining the occurrence of characters but when combined with other skills it becomes an essential tool for cryptanalysis.

The other weakness is an inability to disguise the rules of language. The English language has only a few letters that are commonly found in pairs(ee, tt, ff, ll, ss) a few words with two letters(an, at, in, if, is, wl, of, on, to, so, go) and even fewer with one (i, a). This can be a good starting point for breaking into a cipher if the spacing is in tact. Sometimes cipher messages are broken down into groups of five, making the cryptanalyst's task slightly trickier. By attacking the small words with the aid of frequency analysis we would start to see parts of the plaintext come through.

Now with the help of our GKSBC algorithm, we encrypt a text file, given below is the input plain text and its encrypted ciphertext.

Plaintext	Cipher text
The evolution leading to RC6 has provided a simple cipher yielding numerous evaluations and adequate security in a small package. After describing the structure of the algorithm, the prominent goal that stands out is simplicity.	ÿ3Û³I¢™7 [«ËøkN):› ö÷Phç?¸@µóÚÿq/"£bÁbû`y1* w -‡«š#ægåPœÃ$2R ÓñbKO =qç`'àHËùr7M*ƒäƒ¾ÁOðÖH¼' Ç-Â\#†ÓñÔø^D 8 çqéQ ž Ž¹ò€H&gv¨u+F'Aƒí 2Ú¾•— ÿ«{‡òƒwµ@« ½N È *q35 °·Â´TÉ†üò- ûÎ<x@ñõm~uSFR„Êæå}{)nå); bO'Dß

Letter frequencies corresponding to plain text.

One letter sequences

e	t	i	a	s	n	r	o	l	u	d	h	c	p	m	g	v	y	f	k	b	q
20	19	18	17	12	11	11	11	10	9	8	8	7	6	6	6	3	3	2	1	1	1

Two letter sequences

th	in	he	al
6	5	5	4

Three letter sequences

the
4

With the help of the frequencies given above, we cannot predict similar patterns between the plaintext and ciphertext. So it is not possible to find the plaintext with the help of frequency cryptanalysis.

IV. CONCLUSION

In the process of continuous advancement of new encryption systems, necessitated by the advancement in security and efficiency requirements, recently developed Generalized Key Scheme Block Cipher (GKSBC) algorithm proved to outperform popular encryption schemes in terms of stability, execution time and encryption quality. This paper evaluated capability of GKSBC in the face of various cryptanalytic attacks viz., Brute – Force Attack, Differential Cryptanalysis, Integral Cryptanalysis, Linear Cryptanalysis Rectangle attack and Frequency Analysis. The study found that none of the traditional attacks are designed to decrypt GKSBC encryption as the use of key scheme is different in it and therefore robust to the conventional cryptanalytic attacks.

REFERENCES

[1] S. Aruljothi and M.Venkatesulu, "Encryption Quality and Performance Analysis of GKSBC Algorithm", Journal of information engineering and applications, Vol. 2, No.10, 2012.
[2] Zeghid M et al. A Modified AES Based Algorithm for Image Encryption. World Academy of Science. Engineering and Technology 27; 2007.
[3] Alex Biryukov et al. Block Ciphers and Systems of Quadratic Equations. Fast Software Encryption. Vol.2887. Springer pp. 274-289; 2003.
[4] Nicolas et al. Efficient Algorithms for Solving Overdefined Systems of Multivariate Polynomial Equations. Advances in Cryptology - EUROCRYPT 2000. International Conference on the Theory and Application of Cryptographic Techniques. Bruges. Belgium. May 14-18. pp. 392-407; 2000.
[5] Bellare M et al. Pseudo-Random Number Generation within Cryptographic Algorithms: the DSS Case. Advances in Cryptology - Crypto 97; 1997.
[6] N.T. Courtois and J. Pieprzyk. Cryptanalysis of Block Ciphers with Overdefined Systems of Quadratic Equations. Advances in Cryptology. Asiacrypt'02. Springer- Verlag p. 267–287; 2002.
[7] J. Zhou, Z. Liang, Y. Chen, and O. C. Au, "Security analysis of multimedia encryption schemes based on multiple Huffman table", IEEE Signal Processing Letters, Vol. 14, No. 3, pp. 201– 204, 2007.
[8] Priya Dhawan. Performance Comparison: Security Design Choices. Microsoft Developer Network; October 2002.
[9] E. Biham and A. Shamir. Differential Cryptanalysis of DES-like Cryptosystems Lecture Notes in Computer Science: Advances in Cryptology- Proceedings of CRYPTO '90. Springer-Verlag pp. 2-21; 1990.
[10] U. Blocher and M. Dichtl. Problems with the Linear Cryptanalysis of DES using More than One Active S-box per Round. Fast Software Encryption Workshop Springer- Verlag pp. 256–274. 1994.
[11] J.J. Amador and R.W.Green. Symmetric-Key Block Cipher for Image and Text Cryptography. International Journal of Imaging Systems and Technology. pp. 178-188; 2005.
[12] S.S. Maniccama and N.G. Bourbakis. Image and video encryption using Scan patterns., Pattern Recognition. pp. 725 – 737; 2004.
[13] Socek D et al. Digital video encryption algorithms based on correlation- preserving permutations. EURASIP J Inform Security; 2007.
[14] Ch.Rupa and P.S.Avadhani. Performance Evaluation of Message Encryption Scheme Using Cheating Text. Global Journal of Computer Science and Technology. Vol 9. 2009.
[15] Chengqing Li and Guanrong Chen. On the security of a class of image encryption schemes. IEEE International Symposium on Circuits and Systems. ISCAS 2008.
[16] Wen J et al. A format compliant configurable encryption framework for access control of video. IEEE Trans. Circuits and Systems for Video Technology. Vol. 12. pp. 545–557; 2002.
[17] Mohamed Abdelraheem et al. Differential Cryptanalysis of Round-Reduced PRINT cipher: Computing Roots of Permutations. proceedings of Fast Software Encryption. 2011.
[18] Kenji Ohkuma et al. Weak Keys of Reduced-Round PRESENT for Linear Cryptanalysis. proceedings of

SAC 2009. LNCS vol. 5867. Springer pp. 249- 265; 2009.

[19] Biham E et al. Related-key boomerang and rectangle Attacks. Advances in Cryptology - EUROCRYPT'05. Volume 3494 of Lecture Notes in Computer Science. Springer-Verlag pp. 507–525; 2005.