Linear Congruential Generator and Caesar Cipher

Karuna Pandit

***Abstract**: With the massive development in the technology, this era is witnessing tremendous use of Internet . Huge amount of confidential data trasfer is taking place through Internet. The consequence of this growth is the great demand for data security. Privacy is the most sorted topic in Information Security. The protection of privacy of data can be achieved by the application of cryptography. In this paper a new encryption algorithm is proposed using the simplest classical Caesar Cipher with Linear Congruential Generator for shift size followed by permutation of the words of the message. The strength of the algorithm is ease of use and large key space making Brute force cryptanalysis impossible.*

Keywords : Encryption, Decryption, Linear Congruential Generator, Security,Caesar Cipher, Cryptanalysis.

I. INTRODUCTION

Due to the advances in the technology, there is incredible growth in the use of internet. Enormous amount of confidential data like bank details, credit card details are tranfered through communication channels. Maintaining the secrecy of these details is the most need of the day. Most widely used means of secure communication is encryption. Several encryption algorithms have been developed to offer data security.

A. Cryptography

Cryptography is the art of covert writing .It is the study of various schemes used for encryption[1][2][3]. The message to be communicated, plain text is scrambled using encryption algorithm into cipher text. At the destination cipher text is unscrambled using decryption algorithm to get the original plain text.

The plain text 'P' converted in to cipher text 'C' using the algorithm 'E' and secret key 'k'

$$C = E_k(P)$$

The plain text is extracted from the cipher text using the decryption algorithm 'D' and the key 'k'[1][3].

$$P = D_k(C)$$

Revised Manuscript Received on October 15, 2019.

Karuna Pandit, Department of Master of Computer Applications, N.M.A.M. Institute of Technology,(Visvesaraya Technological University, Belagavi),Nitte, 574110, Udupi District, Karnataka, India

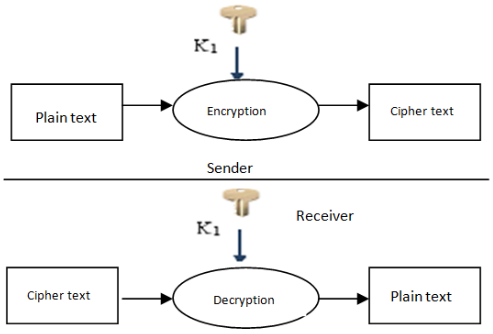

Fig. 1. Encryption and Decryption

Cryptographic algorithms are classified in to two types depending on the number of keys used for encryption and decryption.Secret key cryptosystem ,uses a same key for both encryption and decryption while public key cryptosystem uses different keys for encryption and decryption[3].

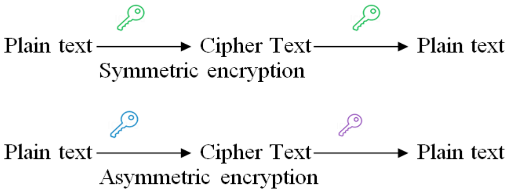

Fig. 2. Symmetric and Asymmetric Encryption

B. Caesar Cipher

Caesar Cipher is one of the oldest and the easiest substitution cipher. The encryption is, replacing each letter of the alphabet with the letter three places to the right of it.[1]. The Brute force technique can be performed very easily due to the smaller key size.

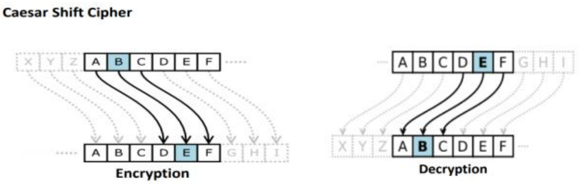

Fig.3. Ceasar Cipher

C. Linear Congruential Generator

The linear congruential generator ia an algorithm that generates a random sequence of integers between 0 and m-1. This technique is one of the simple and widely used random number generator. The generator is defined by the recurrence relation

$X_{i+1} = (a X_i + c) \bmod m$, for i = 0,1,2,3…….. m-1

$m > 0$ and $a < m$, $c < m$, $X_0 < m$

where the initial value X_0 is the seed, ‘a’ is the constant multiplier, ‘c’ is the increment and ‘m’ is the modulus.With suitable selection of a, c, m and X_0, sequence of full length ‘m’ can be generated[4].

For example,

a=41 X_0=29 b=2 m=100

The generated sequence is

42, 45, 68, 11, 74, 57, 60, 83, 26, 89, 72, 75, 98, 41, 4, 87, 90, 13, 56, 19, 2, 5, 28, 71, 34, 17, 20, 43, 86, 49, 32, 35, 58, 1, 64, 47, 50, 73, 16, 79, 62, 65, 88, 31, 94, 77, 80, 3, 46, 9, 92, 95, 18, 61, 24, 7, 10, 33, 76, 39, 22, 25, 48, 91, 54, 37, 40, 63, 6, 69, 52, 55, 78, 21, 84, 67, 70, 93, 36, 99, 82, 85, 8, 51, 14, 97, 0, 23, 66, 29

II . PROPOSED ALGORITHM

A. Encryption

1. Count the number of words, say k , in the plain text
2. Generate as many keys as number of words using Linear Congruential Generator. Key =(ax+b) mod 26 choosing suitable values for a, c and initial seed x_0.
3. Apply Caesar Cipher to each word in the plain text using the keys generated in step2 taking separate keys for individual words. Repeat till all k words are encrypted.
4. Generate permutation of 1 to k numbers and arrange the encrypted words in the order of permutation to obtain the final Cipher text.
5. Transmit the Cipher text.

B. Decryption

1. Re-permute the received Cipher text.
2. Generate as many keys as number of words using Linear Congruential Generator.
3. Decrypt each word in the Cipher text using keys generated in the step 2 , taking one key and one word at a time. Repeat till all k words are decrypted.

Example1:

Plain text:

The world is in greater peril from those who tolerate or encourage evil than from those who actually commit it.

Generated keys:

24,5,12,19, 0,7, 14,21,2,9,16,23,4,11,18,25,6, 13,20,1

Cipher Text:

rfc btwqi ue bg greater wlyps tfca ocjnz yjq cxunajcn eh bkzlroxdb izmp esly xjge sgnrd enu npghnyyl wiggcn ju

Permutation:

3, 2,5,1,4,10,8,7,6,9,15,11,12,14,13,19,17,20,16,18

Final Cipher Text:

ue btwqi greater rfc bg cxujajcn objnz tfca wlfps yjq tfca eh bazlroxdb bazlroxdb idmp wiggcn yjq ju Objnz npghnyyl

Example2:

Plain text:

The use of internet and network is growing rapidly. So there are more requirements to secure the data transmitted over different networks using different services

Generated keys

24,5,12,19,0,7,14,21,2,9,16,23,4,11,18,25,6,13,20,1,8,15,22,3,10

Cipher Text

rfc zxj ar bgmxkgxm and uladvyr wg bmjrdib tcrk bx jxuhu xob qsvi cpbftcpxpyed lg rdbtqd znk qngn nluhmgcnnyx pwfs lqnnmzmvb ctildgzh qoejc gliihuhqw cobfsmoc

Permutation

20,3,6,9,12,24,13,5,7,16,23,18,21,4,10,15,8,22,17,2,1,19,11,25,14

Final Cipher Text

pwfs ar uladvyr tcrk xob gliihuhqw qsvi and wg rdbtqd qoejc qngn lqnnmzmvb bgmxkgxm bx lg bmjrdib ctildgzh znk zxj rfc nluhmgcnnyx jxuhu cobfsmoc cpbftcpxpyed.

III. CRYPTANALYSIS

Caesar cipher is easily broken. Since the shift is a number between 1 and 25. Brute force technique can be easily deployed to break the cipher[5].The proposed algorithm uses differet Keys for each word. Brute force technique is not as simple as in the case of classic Caesar Cipher. Further, the encrypted words are permutaed. For a ‘n’ word plain text there are n! permutations and Brute force cryptanalysis is impossible.

Frequency analysis is the fundamental cryptanalytic technique besides Brute force technique[2][6]. Each language has certain features and Substitution ciphers preserve these features. So Substitution ciphers are vulnerable to frequency analysis attacks.

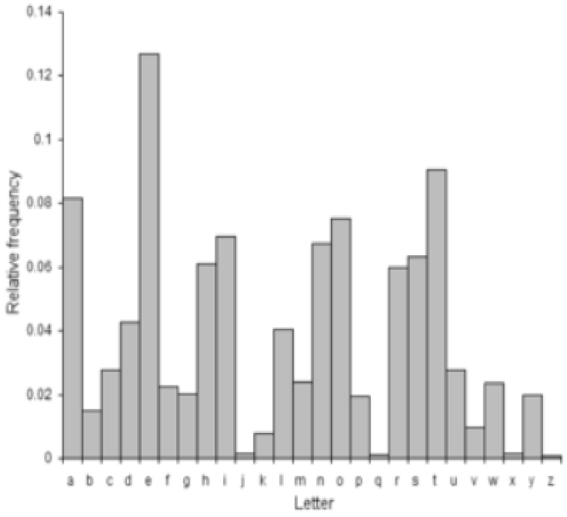

Fig.4. Typical Frequency Distribution of English Alphabets.

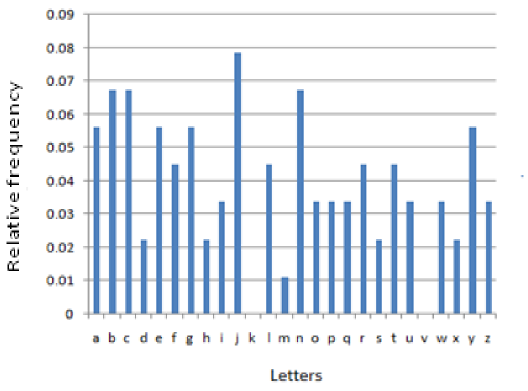

Fig. 5. Frequency Distribution of Characters in Cipher Text(Example1)

Comparing with the frequency distribution of characters in Figure 4 and 5, the shift size is ‘5’ , because, most frquent occuring letter is ‘j’ which is ‘5’positions to the right of ‘e’.

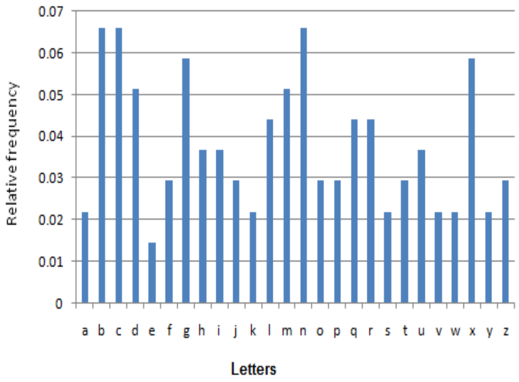

Fig.6. Frequency Distribution of Characters in Cipher Text(Example2)

Once again, comparing with the frequency distribution of characters in Figure4 and 6, the shift size is ‘9’ , because, most frquent ouuring letter is ‘n’ which is ‘9’positions to the right of ‘e’. Thus frequency analysis is also of no much use for cryptanalysts.

III. CONCLUSION

In the propopsed algorithm , shift size is determined by the Linear Congruential Generator and the resulting cipher is permuted to enhance the security of Caesar cipher. For a text with ‘n’ words there are n! possible arrangements. This makes Brute force analysis still difficult. The proposed algorithm definitely strngthen the Caesar cipher.

REFERENCES

1. Stalling, William(2006). “Cryptography and Network Security: Principles and Practice”, 5th Edition, Prentice Hall.
2. Schneier,B. (1996). “Applied Cryptography: Protocols, Algorithms, and SourceCode in C”, 2nd Edition, John Wiley and Sons.
3. G. C. Kessler, "An Overview of Cryptography," published by Auerbach, 1998 (14 August 2019). http://www.garykessler.net/
4. Knuth, D.E.(1998).“The Art of Computer Programming, Volume 2: Seminumerical Algorithms”, 3rd Edition Reading, MA: Addison-Wesley.
5. Singh, S. (2000). “The code book: the science of secrecy from ancient Egypt to quantum cryptography”, New York: Anchor Books.
6. Lewand, R(2000). “Cryptological Mathematics”, Washington, DC: Mathematical Association of America.