A Novel Approach to Generate a Key for Cryptographic Algorithm

Kiran Bala B*

Department of Computer Science and Engineering, K. Ramakrishnan College of Engineering, Trichy, Tamil Nadu, India

***Corresponding author: Email: kiranit2010@gmail.com**

ABSTRACT

In this study encryption and decryption techniques are same, but generation of key is new concept to generate the key, however the key is purely depends on plain text to generate key for encryption part but key size is not static, however the key is purely depends on plain text to generate key, then decryption side cipher text along with header will be send with the help of header cipher text can be converted into plain text here header consists of two things in decryption part key as well as plain text draft like total count of number of letters, number of words, repetition of words and repetition of letters in unknown form to strengthen the key for encryption and decryption part in present technology and integrity of the message can also be check with the help of header.

KEY WORDS: Encryption, Decryption, Key, Cipher Text, Plain text, Header.

1. INTRODUCTION

Sending message is still now issue in present technology, however cryptographic place a major role in sending and receiving the messages. Fortunately, in both encryption side as well as decryption side one important and major part is key generation with the help of the key only encryption and decryption can be made safe and secure in transactions.

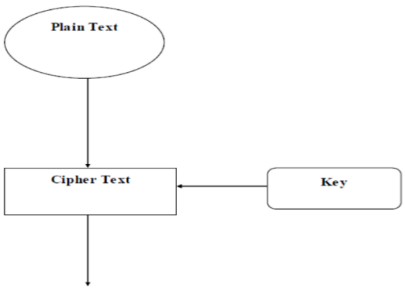

Figure.1. Basic Diagram for Encryption

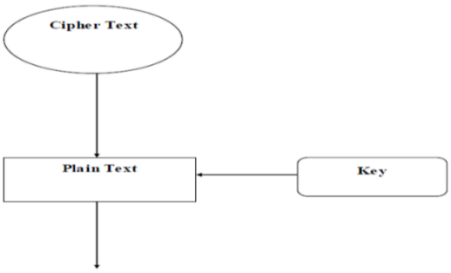

Figure.2. Basic Diagram for Decryption

Proposed System: From the introduction the basic principles of encryption and decryption can be easily understood coming to the proposed system mainly concentrates on key generation only in both sides.

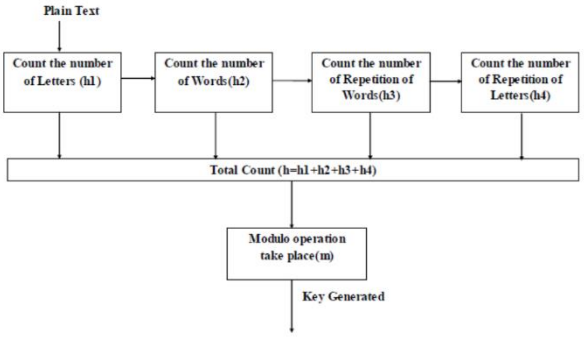

Figure.3. System Architecture for key generation in Encryption side

The Figure.3, shows the system architecture for the key generation in encryption part. Initially the plain text will be enter into our system then plain text will be consider as a=1, b=2,.....z=26 and A=27, B=28,....Z=52 in our system then each letter(h1), word(h2), repetition of words(h3) and repetition of letters(h4) will be totally counted(h) is shown in the equation 1. Then, as early mentioned in the figure 3 total count (h) will be made mod operation (m) is shown in the equation 2. Finally key will be generated for the encryption side.

$$h=h1+h2+h3+h4 \quad (1)$$

$$m=0,\ h \bmod 52;\ 0<= h<=52 \quad (2)$$

$$m=h \bmod 52;\ h>52$$

Now with the help of key the system can convert plain text into cipher text along with the header as shown in the figure.5, which represent the header frame format. It consist of count of letter (h1), word (h2), repetition of words (h3) and repetition of letters (h4) and made mod 52 for each segment separately as mentioned in the figure.4.

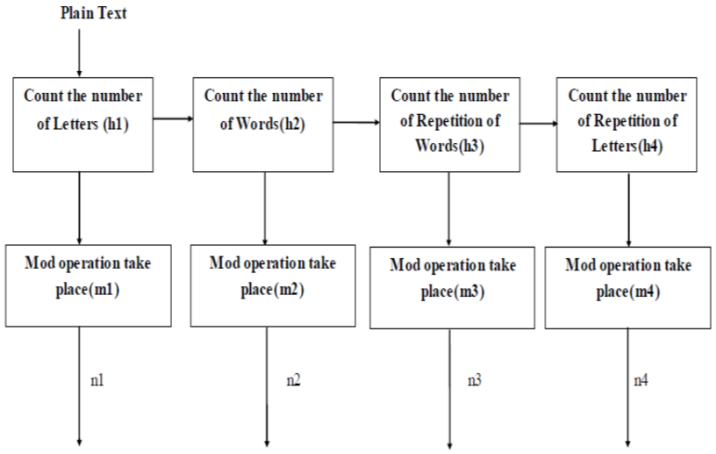

Figure.4.Header segment generation

After the key has been generated now apply the key to plain text as shown in the figure 1 and convert plain text into cipher text. In that case for generation of key the system takes the total count of number of letters, number of words, repetition of words and repetition of letters in that make the mod operation that final value will the key for encryption side as shown in the equation.3.

$$CT=0,k \bmod 52;\ 0<= k<=52 \qquad (3)$$
$$CT=k \bmod 52;\ k>52$$

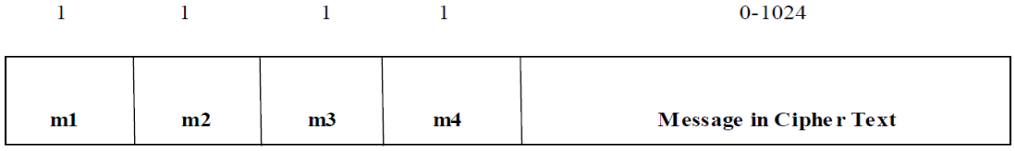

Figure.5. Header Frame Format in Encryption

Now the encryption part is completed. Then, decryption part has the same header frame format as shown in figure.5. The system will check the frame format m1, m2, m3, m4 which help us to generate the key for decryption. The first step in decryption part is modular multiplicative inverse shortly known as MMI is used to extract the original value of h1, h2, h3 and h4 then, in second step add all the values and once again use the MMI to generate the value of key to decrypt the cipher text. Finally, apply the key to cipher text and convert into plain text as shown in the figure.6 & figure.7.

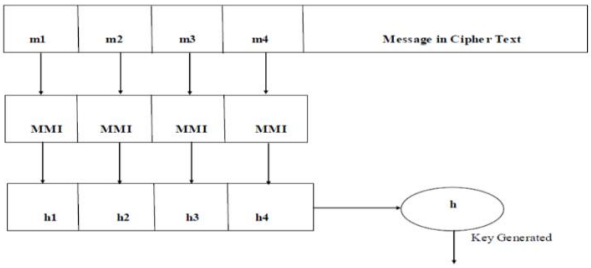

Figure.6. Key Generation in Decryption part

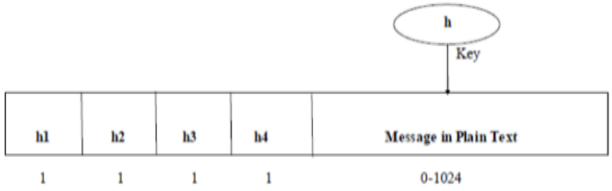

Figure.7. Header Frame format in Decryption

Implementation: The novel approach algorithm implemented in c language by using gcc compiler the key generation algorithm for both encryption as well as decryption implemented initially plain text must be given as How are you then it will count letter by letters, word by words, repetition of words and repetition of letters. For the given plain text how are you the system generate total count of number of letters (h1) are 9, number of words (h2) are 3, repetition of word (h3) is 0 and repetition of letter (h4) is 1.

Figure.8. Implementation in Encryption part

Figure.9. Implementation in Decryption part

Then, make mod operation as given in equation 1 and equation 2. And store those values in header as m1, m2, m3 & m4. Now sum all the values that sum will be made mod operation that final value is known as encryption key. Now with the help of the key system can convert plain text into cipher text and transfer the cipher text along with the header which consists of m1, m2, m3 & m4.

In the receiver side by using MMI system generate the h1, h2, h3 & h4 from m1, m2, m3 and m4. Now sum of those values once again the system apply the MMI operation to extract the original key is named as h that is the decryption part key has been generated now. Here two things to be notify one is key help us to convert cipher text into plain text another one is h1, h2, h3 & h4 is used to verify whether converted plain text is matching with those value to give more integrity for the message.

2. CONCLUSION

Security is the major issues in present technology in this system security is achievable by proposed system along with less complex process in order to reduce the execution time as well as to strengthen the cipher text as shown in the figure 8 & figure.9. The generation of key in both side like encryption and decryption is purely based on the plain text however the key is always depends on plain text so the intruder may not aware of the plain so cipher text is very confidential and integrity is also possible because in final execution of program header along with plain text available so system can check the original message is also possible.

Future Enhancement: The system likes to be implementing in steganography and biometrics to give more security to those kind of technology in upcoming days for that purpose database is very important especially size of the database and processing time should be consider in that kind of approach which leads to very high challenge in those areas.

REFERENCES

Bala B.K, Audithan S, Wavelet and curvelet analysis for the classification of micro calcification using mammogram images, 2 nd International Conference on Current Trends in Engineering and Technology, 2014.

Kiran Bala B, Audithan S, Kannan G and Raja K, Frequency Domain Approaches for Breast Cancer Diagnosis, Australian Journal of Basic and Applied Sciences, 10 (2), 2016, 93-96.

Kiran Bala B, Lourdu Joanna J, Multi-Modal Biometrics using Cryptographic Algorithm, European Journal of Academic Essays, 1 (1), 2014, 6-10.

William Stallings, Cryptography and Network Security Principles and Practice, Sixth Edition, Pearson Education Limited, England, 2013.