International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2013): 4.438

Bit Flip Cipher: An Approach to Enhance B2G & G2B Cipher

Sandeep Sharma, Amit Verma

Abstract: ***There are two types of cryptography algorithms i.e. Symmetric and Asymmetric which are further divided into two types i.e. Substitution and Transposition Algorithms. The Bit Flip cipher is the substitution algorithm which is approached to overcome the limitations of B2G & G2B cipher.***

Keywords: Cryptography,symmetric cryptography, substitution cipher, B2G & G2B cipher, binary cipher, Bit Flip cipher.

1. Introduction

Before discussing the approached algorithm, there is a need to go through some terms which are:-

- **Cipher** is the set or combination of both algorithms used to encrypt and decrypt information.
- **Cryptography** is the domain of techniques used to encrypt (changing information from its original form to other form) and decrypt (changing information to its original form from changed form) the information. Cryptography is used to hide or secure the information and uses key(s) to encrypt & decrypt information. Cryptography is divided further into following categories:

2. Symmetric & Asymmetric

In symmetric category only one key is used to encrypt and decrypt information which is kept private between sender and receiver. In asymmetric category a pair of two keys i.e. public key and private key is used to encrypt and decrypt information where only private key is kept private and public key is available to all.

3. Substitution & Transposition

In Substitution the each letter of information is replaced by the other letter by using some key rule whereas in Transposition each letter of information is shuffled (position of letter is changed) by using some key rule.

4. B2G & G2B (Binary to Gray & Gray to Binary) cipher

4.1 Encryption Algorithm

1. Generate the ASCII value of the letter in information.
2. Generate corresponding binary value of it.
3. Implement Binary to Gray conversion on this binary value.
4. Generate the ASCII value from Gray Code generated after step 3 and convert to letter according to ASCII value.

4.2 Binary to Gray Conversion

1. Write the MSB (Most Significant Bit) same as the MSB in Binary value.
2. The next bit value of Gray Code can be obtained by performing the X-OR operation between the same place bit of binary number and next place bit of binary value, i.e. for 2nd bit of Gray code perform X-OR between 1st& 2nd bit of binary value.

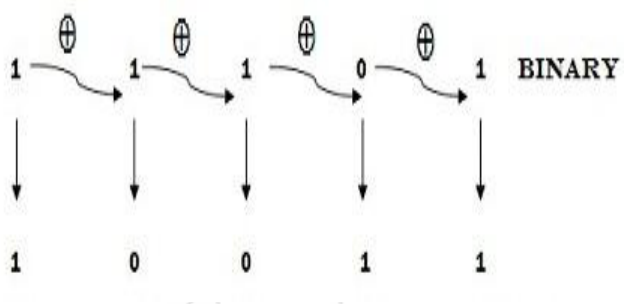

Figure 1: B2G Conversion

4.3 Decryption Algorithm

1. Generate the ASCII value of the letter in encrypted text.
2. Generate the corresponding binary value of it.
3. Implement Gray to Binary conversion on this binary value.
4. Generate the ASCII value from Binary value generated after step 3 and convert to letter according to ASCII value.

4.4 Gray to Binary Conversion

1. Write the MSB (Most Significant Bit) same as the MSB in Gray value.
2. The next bit value of Binary value can be obtained by performing the X-OR operation between the same place bit of binary value and next place bit of Gray value, i.e. for 2nd bit of Binary value perform X-OR between 1st bit of binary value & 2nd bit of Gray value.

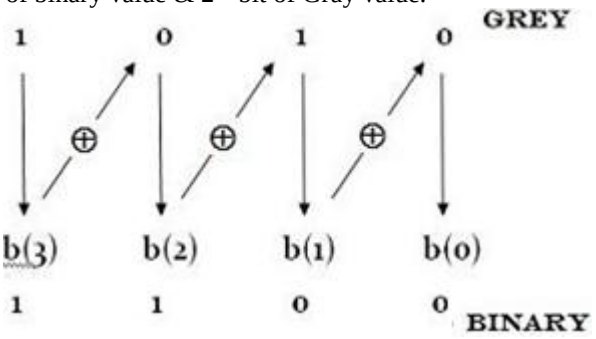

Figure 2: G2B Conversion

4.5 Limitation of B2G & G2B Cipher

As B2G & G2B cipher substitute letters by changing their binary values, it is good cipher, but still has some limitations as:

- It has only one Key, i.e. every letter is substituted with only one letter that is the Gray value of its corresponding binary value.
- It takes more time to encrypt information, i.e. As every adjacent bits are compared and X-OR operation is performed on to convert from binary to gray and vice versa its time taken is directly proportional the number of bits in number.
- It uses two different algorithms, i.e. B2G, G2B, to encrypt and decrypt respectively.

5. Approached Cipher: Bit Flip Cipher

1. Generate the ASCII value of the letter in information.
2. Generate corresponding binary value of it.
3. Change the value of key position bit in binary value i.e. 0 to 1, or 1 to 0.
4. Generate the ASCII value from value generated after step 3 and convert to letter according to ASCII value.

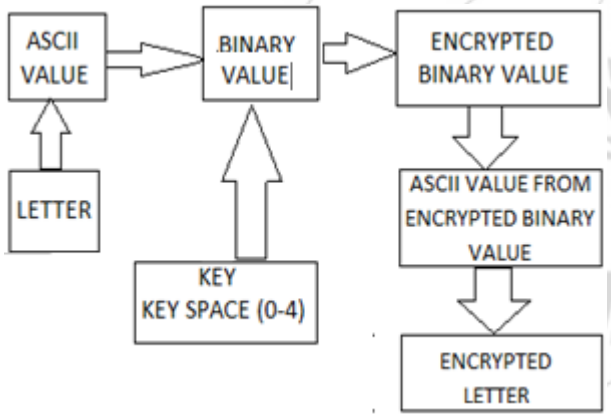

Figure 3: Bit Flip Cipher

6. Advantages of Bit Flip Cipher

As B2G & G2B has some limitations Bit Flip cipher overcomes those limitations as below:-

- It has Key space of 5 Keys, which are more than 1 key as in B2G & G2B cipher.
- It takes less time to encrypt information as only one bit value is selected and changed using keys in key space.
- It uses same algorithm for both encrypt and decrypt information instead of two as in B2G & G2B.

7. Further Scope

Bit Cipher can be used as a standalone Cipher and can also be used as a combination with other Ciphers like Rail Fence, Caesar, Columnar Transposition, Play Fair and more.

References

[1] Everyday Cryptography: Fundamental Principles and Applications by Keith M. Martin.
[2] A Course in Number Theory and Cryptography by NEAL Koblitz.
[3] Cryptography: The Science of Secret Writing by Laurence Dwight Smith.
[4] Efficient Encryption Techniques In Cryptography Better Security Enhancement, Volume 4, Issue 5, May 2014, ISSN 2277-128X.