Volume 5, Issue 7, July 2015

ISSN: 2277 128X



# International Journal of Advanced Research in Computer Science and Software Engineering

**Research Paper** 

Available online at: <u>www.ijarcsse.com</u>

# Implementation of B2G & G2B Cipher, Bit Flip Cipher and Comparative Analysis of Both in Respect of Key Space and Time

Taken to Encrypt a Message

Sandeep Sharma, Jawad Ahmad Dar Department of Computer Science & Engineering

Kurukshetra University, Kurukshetra, Haryana, India

Abstract— Bit Flip Cipher and B2G & G2B Cipher; both are Symmetric & Substitution type of Ciphers for Encryption in Cryptography. Bit Flip Cipher<sup>[1]</sup> is introduced and designed by the Author in February 2015, to overcome some of the limitations of B2G & G2B Cipher<sup>[2]</sup>. In this paper Author implements the both Ciphers and compares them in respect of Key Space and Time taken to encrypt a message by them.

Keywords—Cryptography, Symmetric Cryptography, Bit Flip Cipher, B2G & G2B Cipher, Implementation of Bit Flip and B2G & G2B Cipher.

# I. INTRODUCTION

Before going to study Bit Flip and B2G & G2B Cipher, and their implementation there is need to understand Cryptography and its various terminologies. So below is some valuable explanation about cryptography and its terminologies used.

Cryptography is the domain or field of study of techniques those are used to represent a message by changing it according to some pattern or method. Cryptography has some basic terminology which is necessary to understand for better understanding of techniques or Ciphers belong to it, which are –

Plaintext:	is the message a sender wishes to transmit to a receiver.
Cipher text:	is the form of Plaintext readable to only receiver for whom it is intended.
Key:	is the particular value by implementing which Plaintext is converted to Cipher text.
Encryption:	is the technique used to convert Plain text into Cipher text.
Decryption:	is the technique used to convert Cipher text into Plain text.
Algorithm:	are the steps used in Encryption or Decryption.
Cipher:	is the combined algorithm of both Encryption and Decryption.

As above defined, Cryptography is the field of study belongs to all the ciphers. Cryptography Ciphers are further classified into following categories –

# II. SYMMETRIC & ASYMMETRIC

In Symmetric Ciphers only one key is used for encryption and decryption of message which is kept secret between sender and receiver of message.



Fig. 1 Symmetric Cryptography

In Asymmetric Cipher a pair of two keys e.g. Public Key and Private Key is used for encryption and decryption of message where only Private Key is kept secret between sender and receiver of message and Public key is available to all. In this type of Cipher message is Encrypted using Public Key of receiver and Decrypted using the Private Key of receiver.



Fig. 2 Asymmetric Cryptography

# A. Substitution & Transposition –

In Substitution Ciphers, each character of message is replaced by other character (which may or may not in message) by using some Key rule.

AB	С	D	E	F	G	н	Ι	J	к	L	М
1 1	\$	\$	\$	\$	\$	\$	\$	\$	\$	\$	\$
NO	Р	Q	R	s	Т	U	۷	w	Х	Y	z

Fig. 3 Substitution Cryptography

In Transposition Ciphers, each character of message is shuffled (position of character in message is changed) using some Key rule.

Message: JAMESBONDNEEDSBACKUP Code: JEONDAUASNESCPMBDEBK

J	E	0	N	D	A	U
A	S	N	E	S	С	Р
M	в	D	Е	в	к	

Fig. 4 Transposition Cryptography

# B. B2G & G2B Cipher –

B2G & G2B (Binary to Gray & Gray to Binary) Cipher represents a message by implementing Binary to Gray conversion steps in Encryption and vice versa for Decryption as described in below steps.

# 1) For Encryption :

- 1. Generate the ASCII value of the letter in message.
- 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.
- 5. Repeat step 1 to 4 until last letter in message.

#### 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 2<sup>nd</sup> bit of Gray code perform X-OR between 1<sup>st</sup>& 2<sup>nd</sup> bit of binary value.



# 2) 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.
- 5. Repeat step 1 to 4 until last letter in message.

#### Sharma et al., International Journal of Advanced Research in Computer Science and Software Engineering 5(7), July- 2015, pp. 936-940

Gray to Binary Conversion

- 1. Write the MSB (Most Significant Bit) same as the MSB in Gray value.
- 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 2<sup>nd</sup> bit of Binary value perform X-OR between 1<sup>st</sup> bit of binary value & 2<sup>nd</sup> bit of Gray value.



# C. Bit Flip Cipher –

In Bit Flip Cipher the message is encrypted or decrypted by changing the bit value of binary number of the respective character in message. Following are the steps that describe the Bit Flip Cipher.

- 1) Encryption/Decryption steps:-
  - 1. Generate the ASCII value of the letter in message.
  - 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.
  - 5. Repeat step 1 to 4 until the last letter in message.



Fig. 7 Bit Flip Cipher Bock Diagram

D. Implementation of B2G & G2B Cipher to Encrypt the Message "cryptography"



Final Cipher text produced is - "RKEHNXTKQHE"

E. Implementation of Bit Flip Cipher to Encrypt the Message "cryptography"



Final Cipher text produced by using Key '1' is – "bsxqunfs'qix" If we replace key '1' with other keys among key space then final Cipher text produced will be as – Cipher text produced by using Key '2' is – "ap{rvmepcrj{" Cipher text produced by using Key '3' is – "gv}tpkcvetl}" Cipher text produced by using Key '4' is – "kzqx|gozix'q" Cipher text produced by using Key '5' is – "sbi'd wbq'xi"

# F. Comparative Analysis of B2G & G2B and Bit Flip Cipher

TABLE I

C M	a i		D'EFE C'1
Sr. No.	Comparative	B2G & G2B Cipher	Bit Flip Cipher
	Attributes		
1	Key Space	It has only one key in its key space,	It has 5 keys in its key space, meaning every
		meaning every message will be	message can be encrypted to 5 Cipher texts.
		encrypted every time to only one	
		cipher text.	
2	Time Taken	As in this Cipher, the every adjacent	As in this Cipher, value of only one bit, that
	To Encrypt	bits of binary number of character in	is the key positioned, is changed, the time
	Message	message, are compared to generate	taken to encrypt message can be generated by
		gray code or vice versa, the time taken	$f(x)=x^*n^*y$ , where $n = no.$ of characters in
		to encrypt message can be generated by	message, $y = time$ taken to convert each
		$f(x) = 7x^*n^*y$ , where $n = no.$ of	character to its ASCII value then to Binary
		characters in message, $y = time taken$	number and from changed binary number to
		to convert each character to its ASCII	ASCII value and then back to character, $x =$
		value then to Binary number and from	the time taken to generate new binary number
		Gray number to ASCII value and then	after changing the value of key positioned
		back to character, $7x =$ the time taken	bit. Hence Encryption speed of this Cipher is
		to convert binary number of character	7 times faster than B2G & G2B Cipher.
		to gray number.	

G. Graphical Representation of Comparative Analysis of B2G & G2B and Bit Flip Cipher



# **III. CONCLUSION**

Conclusion of this comparative analysis is that the Bit Flip Cipher is better than B2G & G2B Cipher, in respect of Key Space and time taken to encrypt a message.

#### REFERENCES

- [1] SANDEEP SHARMA and AMIT VERMA, *Bit Flip Cipher: An approach to enhance B2G & G2B Cipher*, Volume 4, Issue 2, February 2015, ISSN 2319 7064.
- [2] Er. REEME GUPTA, Dr. SUKHVIR SINGH and PARDEEP MAAN, *Efficient Encryption Techniques In Cryptography Better Security Enhancement*, Volume 4, Issue 5, May 2014, ISSN: 2277 128X.