GPH Algorithm: Improved CBC improved BIFID cipher Symmetric Key Algorithm

[1]Dinesh Goyal, [2]Naveen Hemrajani, [3]Kritika Paliwal

[1,2,3]Department of Computer Science,Suresh Gyan Vihar University,

Received: 05-02-2013, **Revised:** 24-03-2013, **Accepted:** 09-05-2013, **Published online:** 21-06-2013

ABSTRACT: Cryptography is art of illusion within which the sender encodes the message employing a key and sends it over the line. The receiver on the opposite facet of the channel decodes the message back and victimization the key tries to get back the initial message. In case the key throughout the communication is same on each side then it's referred to as radial key cryptography and if is termed as uneven key cryptography. There have been completely different secret writing techniques used for the plain text called as block & stream cipher. The modes for encryption are ECB, CBC, OFB & CFB. In this paper we propose a symmetric key algorithm using CBC mode of encryption with high complexity.

***Keywords*: CBC, Symmetric Key, Bifid, Transposition.**

I. INTRODUCTION

Cryptography: - cryptography is a science of knowledge security. Cryptography divided in to 2 Greek words "Crypto's" means that "hidden" and "Graphos" means that "word". It will outline a way to send encrypted or decrypted message. With the assistance of encrypted and decrypted message 2 individuals communicate one another firmly.[3]

Cryptography is the art and science of non-public info protection from dangers of attacks, to convert it into a non-identifiable type their attacks. Primarily information encrypted content information, like text, images, audio, video, etc., to form information illegible, not visible or cannot be referred to as throughout scrambled transmission or storage of encrypted. Cryptography's main objective is to keep the info secure from unauthorized offender. [3]

1.1 There are 5 objective of cryptography[3]

- Authentication
- Secrecy or Confidentiality
- Integrity
- Non-Repudiation
- Service Reliability and Availability

1.2 Modes of operation

This section explains the four most common modes of operations in Block Cipher encryption-ECB and CBC, CFB, OFB with a quick visit to other modes.

- **Electronic Codebook (ECB) mode**

The simplest of the encryption mode is the electronic codebook (ECB) mode. The message is divided in to block and each blocks is encrypted separately. Electronic Codebook is DES native mode "direct application of the DES algorithm to encrypt and decrypt data. In this mode, each plaintext block is independently, to the corresponding cipher text block encryption. This is done through the Feistel password; it creates the basis of the 16 sub keys Symmetric key encryption transformation of plaintext through 16. The same process is used (symmetric key) back into plaintext into cipher text. Duplicate data blocks give same result in duplicate cipher text block.[5].

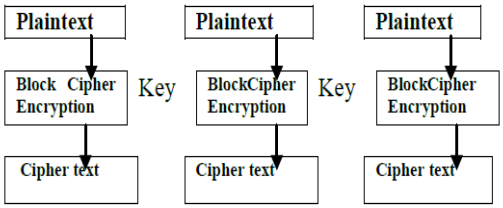

Fig.1 ECB (Encryption encoding)

- **Cipher Block Chaining (CBC) mode**

CBC mode of operation was invented by IBM In 1976. In cipher block chaining (CBC) mode each blocks has plaintext Cipher Block Chaining mode is a block cipher, XOR (exclusive OR) for each new Plaintext block with the previous cipher text block (they are "linked" together). This means that repeating plaintext block does not lead to duplication of cipher text blocks. CBC also uses an initialization vector, which is the initial use of a random function blocks, in order to ensure The results of two identical plaintext cipher text in different (due to different initialization Vectors).[2]

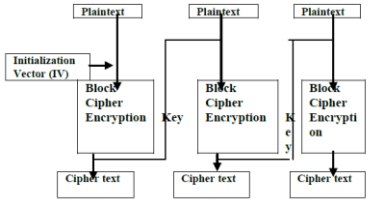

Fig.2 CBC(Cipher Block chaining)

- **Cipher Feedback (CFB) mode**

Cipher feedback mode is a stream cipher to encrypt the plaintext into units X-bit (from 1-64). This allows the bit or byte level of encryption. CFB mode uses a random initialization vector, and the previous cipher text unit XOR plaintext (the password is "feedback" plaintext) follow-up unit.

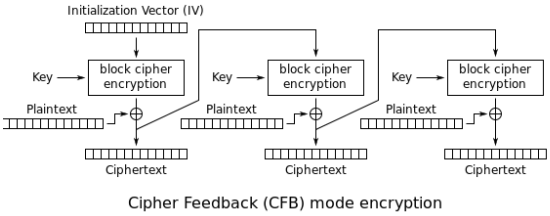

Fig.3 CFB (Cipher Feedback mode)

- **Output Feedback (OFB) mode**

Like CFB mode output feedback mode, uses a random initialization vector encryption Plaintext encryption unit into a stream of X (from 1-64) bit Plaintext. OFB mode differs from the CFB mode, by creating a pseudo-random bit stream (referred to as "Output"), which is XORed with the plaintext (XOR) operation, at each step ("Output", "feedback" Plaintext). Because the output (cipher text) is XORed with plaintext, the error does not transmission.[2]

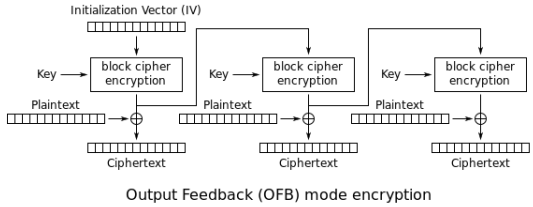

Fig.4 OFB (Output Feedback mode)

- **Counter (CTR) Mode**

Counter mode is a stream cipher, such as OFB mode key difference is the addition of Counter module. The counter can be added or connected in series to a random number (a random value, Used once) and then increments the plaintext encryption of each unit. The first counter block acts as an initialization vector. In each round, the counter module is XORed with plaintext.[2]

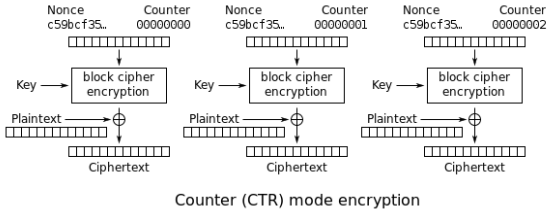

Fig.5 CTR (Counter mode)

II. BIFID CIPHER

Invented by Felix Blessed Virgin Delastelle (1840 - 1902), though divided microorganism word [Ame05 Kah67] has never been used for any "serious" applications, it's become among the foremost widespread passwords "Amateur" cryptographers.[4]

The BIFID Cipher is a type of matrix, or columnar transposition, cipher. Start by creating a 5 by 5 matrix of letters, with the rows and columns labeled 1 to 5

	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	I	J
3	K		M	N	O
4	P	Q	R	S	T
5	U	V	W	X	YZ

Fig.6 Example of BIFID CIPHER

To start, find the value of each letter by reading the row and the column values. The two numbers are then written vertically on a piece of paper below the plain letter. All the plain letters within the secret message are written next to one another as seen below:[4]

Plain Message: S E N D R E I N F O R C E M E N T
Row Value: 4 1 3 1 4 1 4 3 2 3 4 1 1 3 1 3 4
Column Value: 4 5 4 4 3 5 4 4 1 5 3 3 5 3 5 4 5

Notice how the letter "S" has the value of 44. "E" is 15 since it is found in row 1, column 5. Y and Z share the position of (5,5) in the matrix above. After the message has been written out, with row and column values written as shown above, you rewrite the message from left to right, combing numbers into groups of 2.

41 31 41 43 23 41 13 13 44 54 43 54 41 53 35 35 45

The last step is to take each group of numbers, such as 41 and 31 in the beginning of the line above, and find the corresponding cipher values in the same matrix above. 41 is row 4, [4]

Column 1, the letter "P."
41 31 41 43 23 41 13 13 44 54 43 54 41 53 35 35 45
P K P R H P C C S X R X P W O O T

III. PROPOSED METHODOLOGY

Here we propose an improved BIFID Cipher model. In this Model we use 10X10 matrixes for plain text instead of old 5X5 model, and we also use 10X10 matrix key for encryption and decryption. In this model we use 800 bit key and also use 800 bit block size. 100 characters convert into 800 bit using ASCII value than we use for encryption and decryption. We use symmetric block Cipher & CBC mode encryption. Flowcharts for Encryption and Decryption for proposed model are given below:

3.1 Encryption

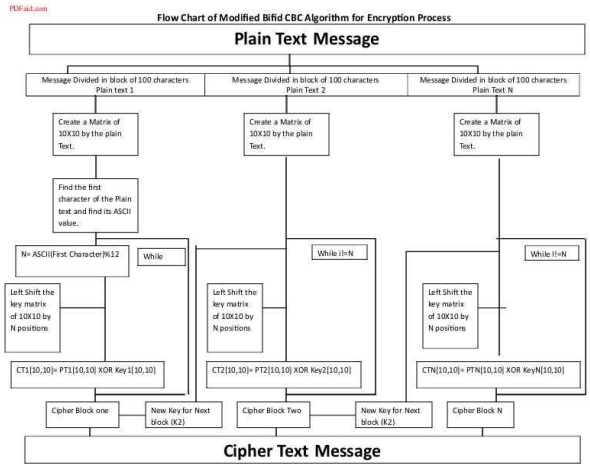

Fig.7 Encryption Flow chart

3.2 Decryption:-

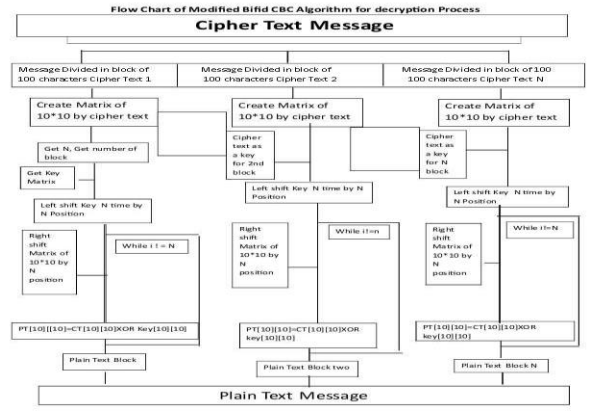

Fig.8 Decryption Flow chart

Various Algorithms for GPH model are as follows:

3.3 Encryption

1. Function Get Key
2. Function Get Plain Text File Location
3. Calculate N; i.e. Mod of ASCII Value of First Character in File by 10
4. Calculate B; i.e. Total No of Blocks in File with size 100 characters in each block
5. Matrix Creation of by blocks of 100 characters from File
6. XOR Matrix with Key and Left Shift Key by N position; N times repeat process
7. Save Cipher Text as Key for next block Encryption
8. Save Cipher Text to a File
9. Repeat Step 5-8 for total No of Blocks

3.4 Decryption

1. Function Get Key
2. Read N and B from File
3. Matrix Creation of by blocks of 100 characters from Cipher Text File
4. Left Shift Key by N Position
5. Right Shift Key by 1 Position
6. Save Cipher Text Block in Temporary Variable
7. XOR Matrix with Key and Right Shift Key by N position; N times repeat process
8. Get Next Block Key from Temporary Variable
9. Save Decrypted Text to a File
10. Repeat Step 3-9 for total No of Blocks

IV. COMPARATIVE ANALYSIS

After the experiment we conducted both theoretical and feature based analysis of the proposed GPH Algorithm. The results for the same are given below.

4. 1 Theoretical Analysis

Factor	AES	DES	GPH
Key size(bits)	128	56	800
Block Size(bits)	128	64	800
Cipher Type	Symmetric Cipher	Symmetric Cipher	symmetric Cipher
Possible Key	2^{128}	2^{56}	2^{800}
Developed	2000	1977	2013

Possible ASCII printable character	95^{16}	95^{7}	95^{100}

Fig.9 Table 1 Comparative Analysis with AES & DES [1]

4.2 Experiment Analysis

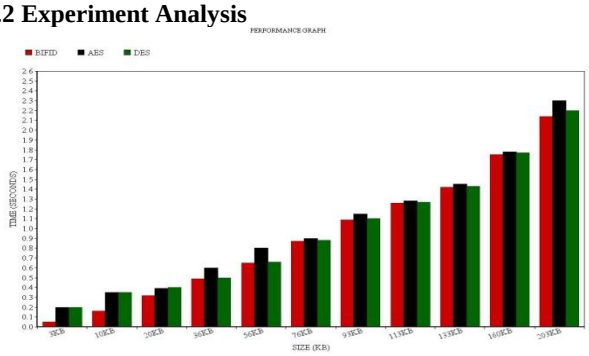

Fig.10 Comparisons between GPH, AES, DES

This graph shows the comparative Analysis between GPH, AES, and DES. Its show execution time of these Algorithms. In these Algorithms even though GPH has high complexity since it uses heavy key size still time required to execute the task is quite low. That's why GPH is much secure than all and even faster too.

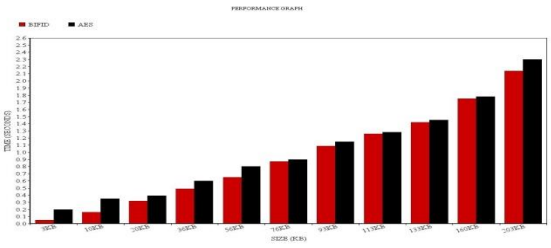

Fig.11 Comparison between GPH & AES

This graph shows the comparison between GPH and AES and proves that GPH is better than AES.

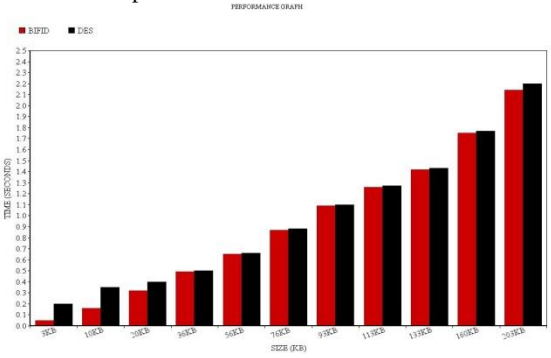

Fig.12 Comparison Improved GPH & DES

This graph shows comparison improved GPH and DES and proves that GPH is better than DES

V. CONCLUSION

In this paper a new comparative study between DES, GPH and AES were presented in to factors, Which are key length, cipher type, block size, developed, Security, possibility key, possible ACSII printable character keys these eligible's proved that in some factor AES is better than improved GPH but in many factors GPH is better than AES. GPH provides high security because it change key in every time or it use 800 bits key.

VI. FUTURE WORK

In GPH we are using binary conversion but in future work one may work on hexadecimal number. The algorithm can also be modified for work on Image processing. In GPH we uses file as a input but in future we may use other data formats for input too. More complexity can be provided by using other modes of encryption and other permutation and combinations too.

VII. REFERENCES

Journal Papers:

[1] Shraddha soni, himani agrawal, dr. (mrs.) monisha sharma, "Analysis and comparison between AES and DES cryptographic algorithm", *International journal of engineering and innovative technology, ISSN:2277-3754 ISO 9001:2008* .

[2] Jawahar thakur1, nagesh kumar2," DES, AES and Blowfish: Symmetric key cryptography algorithms simulation based performance analysis",

[3] Dinesh goyal,vishal srivastava "RDA algortihm: symmetric key algorithm" international journal of information and communication technology research, volume 2 no. 4, april 2012.

[4] António Machiavelo, Rogério Reis "Automated ciphertext-only cryptanalysis of the bifid cipher" *Reis technical report series: dcc-2006-1.*

Books:

[5] Stallings, William; "*cryptography and network security principles and practices*"; (fourth edition; Pearson education; prentice hall; 2009)