Cyber Security (CSE 4003)

Review 1

Title: Secure storage and data-flow in cloud computing and IoT using Bifid cipher.

Team members:

1. Madhav Bahl – 16BCE2311

2. Spreeha Dutta – 16BCE2123

Research Paper: MATLAB-Based Software Tool for Implementation of Bifid Ciphers

Reference:

1.http://delivery.acm.org/10.1145/3140000/3134333/p326Borodzhieva.pdf?
ip=157.50.8.164&id=3134333&acc=ACTIVE
%20SERVICE&key=4D4702B0C3E38B35%2E4D4702B0
C3E38B
35%2EA39F3C0F9899D125%2E4D4702B0C3E38B35&C
FID=84
3021782&CFTOKEN=79037734&__acm__=1513919919
_f78148 95baf5683f3b7fa56565d0b461

2.https://www.researchgate.net/profile/Drdinesh_Goyal/publication/273260684_GPH_Algorithm_Improved_CBC_improved_BIFID_cipher_Symmetric_Key_Algorithm/links/55507d1908ae12808b3810d6/GPH-Algorithm-Improved-CBC-improved-BIFID-cipher-Symmetric-Key-Algorithm.pdf

Description of Bifid algorithm:

The bifid cipher is a cipher which combines the Polybius square with transposition, and uses fractionation to achieve diffusion. First, the letters of the message are converted into numbers (the number of the row and the number of the column) using the Polybius square created on the basis of a keyword. The numbers are written vertically below the message. Then the numbers are read off horizontally and grouped into pairs. The Polybius square is used again to convert the numbers back into letters which is the cipher-text. The bifid ciphers encrypt a message in a way that makes it fairly difficult to decipher without knowing the secret. This is because each letter in the cipher-text message is dependent upon two letters from the plain-text message. As a result, frequency analysis of letters becomes much more difficult.

The key consists of a square table, henceforth called a key-table, composed by the characters of the alphabet, normally a 5X5 square with characters i and j identified, also called a Polybius key, and a small integer ‘, the block size or period, normally greater than 6. The text is divided in blocks of size ‘, padded if necessary with some nulls at the end, and the coordinates of each letter are then written underneath it. The cipher text is now obtained by recoding each block, using the same table, by reading pairs of coordinates horizontally, from left to the right.

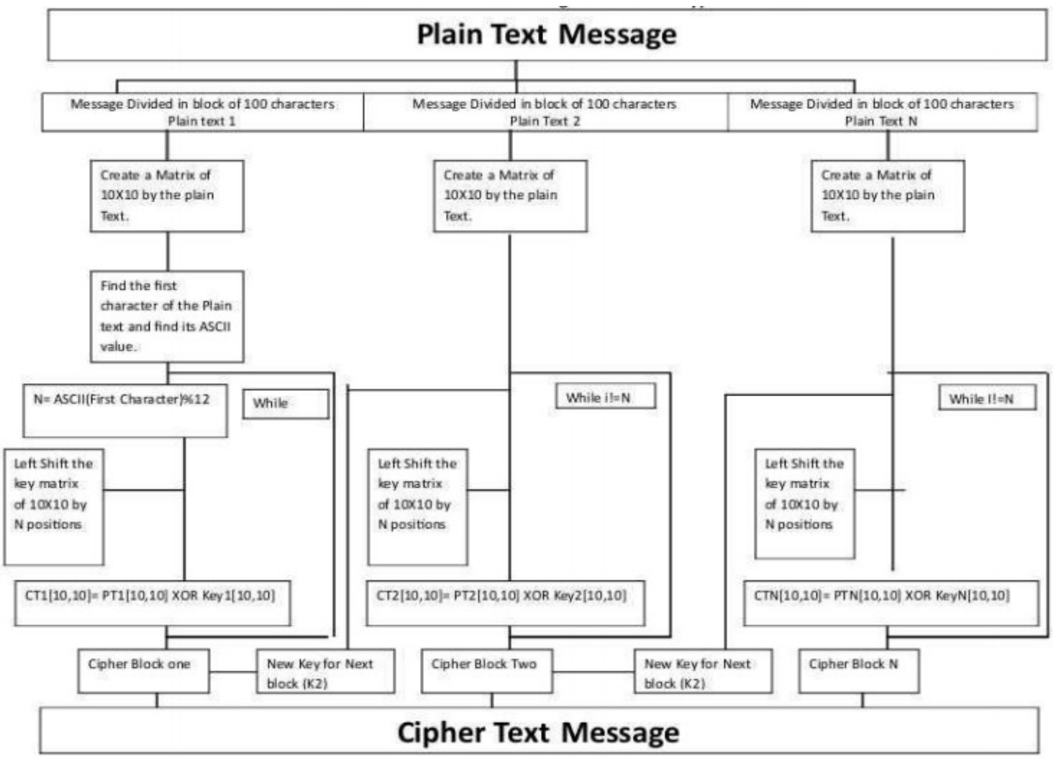

Plain Text Message
Message Divided in block of 100 characters Plain text 1
Message Divided in block of 100 characters Plain Text 2
Message Divided in block of 100 characters Plain Text N
Create a Matrix of 10X10 by the plain Text.
Create a Matrix of 10X10 by the plain Text.
Create a Matrix of 10X10 by the plain Text.
Find the first character of the Plain text and find its ASCII value.
N= ASCII(First Character)%12
While
While i!=N
While I!=N
Left Shift the key matrix of 10X10 by N positions
Left Shift the key matrix of 10X10 by N positions
Left Shift the key matrix of 10X10 by N positions
CT1[10,10]= PT1[10,10] XOR Key1[10,10]
CT2[10,10]= PT2[10,10] XOR Key2[10,10]
CTN[10,10]= PTN[10,10] XOR KeyN[10,10]
Cipher Block one
New Key for Next block (K2)
Cipher Block Two
New Key for Next block (K2)
Cipher Block N
Cipher Text Message

Fig.7 Encryption Flow chart

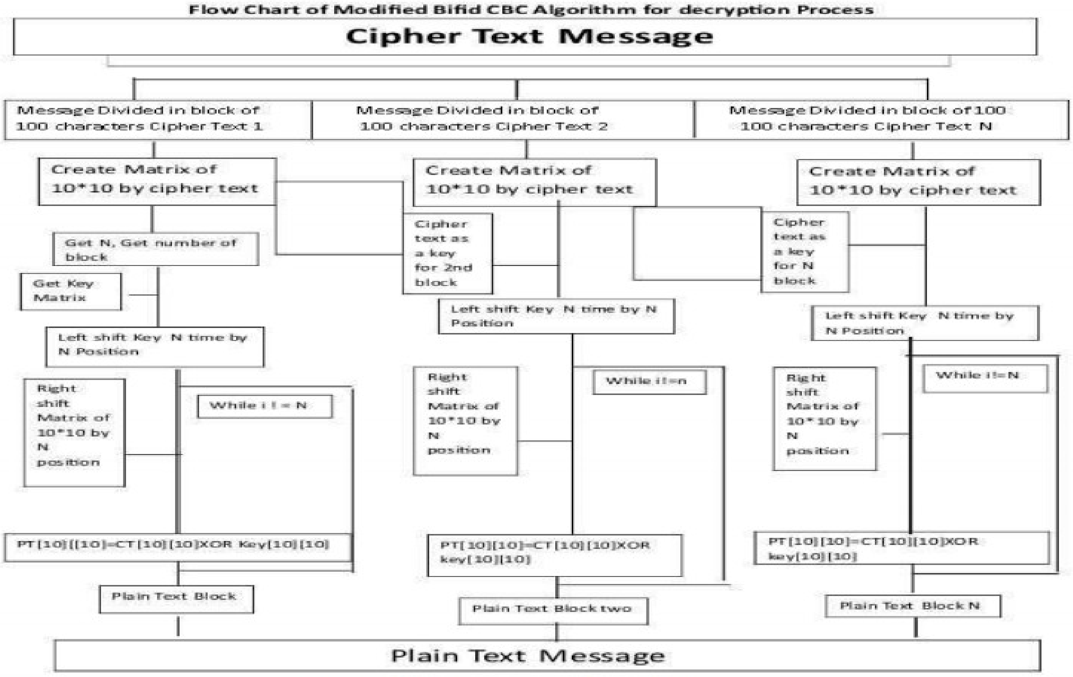

Flow Chart of Modified Bifid CBC Algorithm for decryption Process
Cipher Text Message
Message Divided in block of 100 characters Cipher Text 1
Message Divided in block of 100 characters Cipher Text 2
Message Divided in block of 100 100 characters Cipher Text N
Create Matrix of 10*10 by cipher text
Create Matrix of 10*10 by cipher text
Create Matrix of 10*10 by cipher text
Get N, Get number of block
Get Key Matrix
Cipher text as a key for 2nd block
Cipher text as a key for N block
Left shift Key N time by N Position
Left shift Key N time by N Position
Left shift Key N time by N Position
Right shift Matrix of 10*10 by N position
Right shift Matrix of 10*10 by N position
Right shift Matrix of 10* 10 by N position
While i ! = N
While i!=n
While i!=N
PT[10][[10]=CT[10][10]XOR Key[10][10]
PT[10][10]=CT[10][10]XOR key[10][10]
PT[10][10]=CT[10][10]XOR key[10][10]
Plain Text Block
Plain Text Block two
Plain Text Block N
Plain Text Message

Fig.8 Decryption Flow chart

Example:

First, a mixed alphabet Polybius square is drawn up, where the I and the J share their position:

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

The message is converted to its coordinates in the usual manner, but they are written vertically beneath:

F L E E A T O N C E

4 4 3 3 3 5 3 2 4 3

1 3 5 5 3 1 2 3 2 5

They are then read out in rows:

4 4 3 3 3 5 3 2 4 3 1 3 5 5 3 1 2 3 2 5

Then divided up into pairs again, and the pairs turned back into letters using the square Worked example:

44 33 35 32 43 13 55 31 23 25

U A E O L W R I N S

Objective:

Cloud Storage is a service where data is remotely maintained, managed, and backed up. The service allows the users to store files online, so that they can access them from any location via the Internet. In recent days, almost everyone is moving towards cloud storage and cloud computing, According to a recent survey conducted with more than 800 business decision makers and users worldwide, the number of organizations gaining competitive advantage through high cloud adoption has almost doubled in the last few years and by 2017, the public cloud services market is predicted to exceed $244 billion. People in their daily life use cloud storage for saving their private data. Hence, need for the data to be secured is much more than the same in case of local storage. There are concerns with the safety and privacy of important data stored remotely. Any compromise in data will automatically destroy the privacy, which is the fundamental right for human beings.

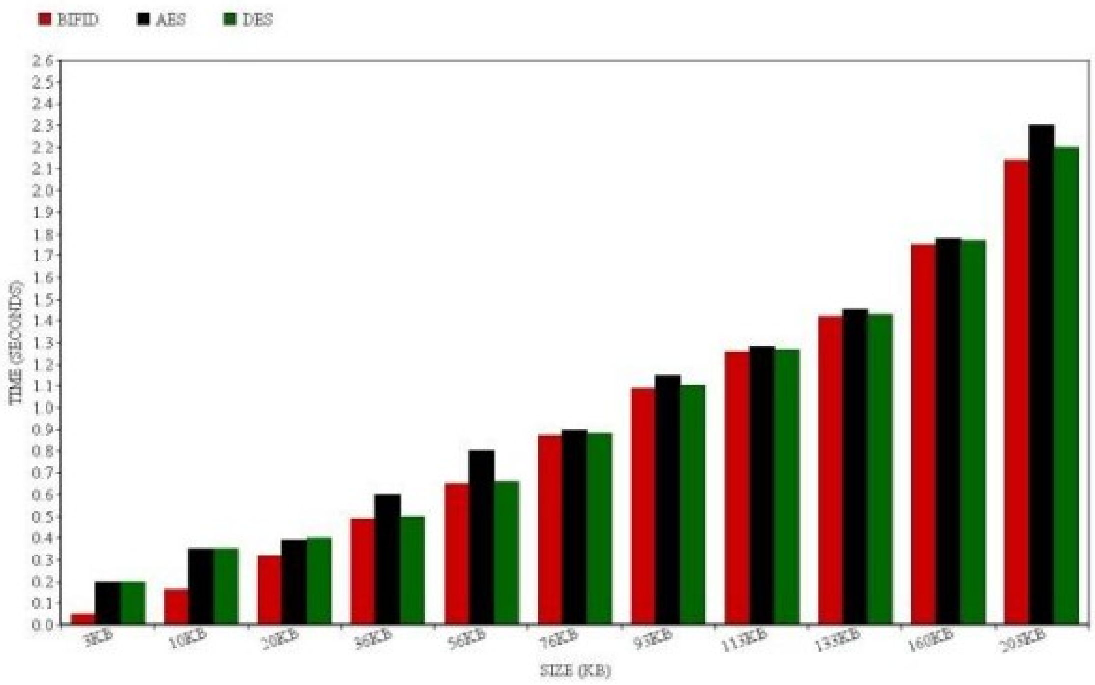
Invented by Felix Blessed Virgin Delastelle (1840 - 1902), though divided microorganism word [Ame05 Kah67] has never been used for any "serious applications, it's become among the foremost widespread passwords "Amateur" cryptographers.

Why This Algorithm?

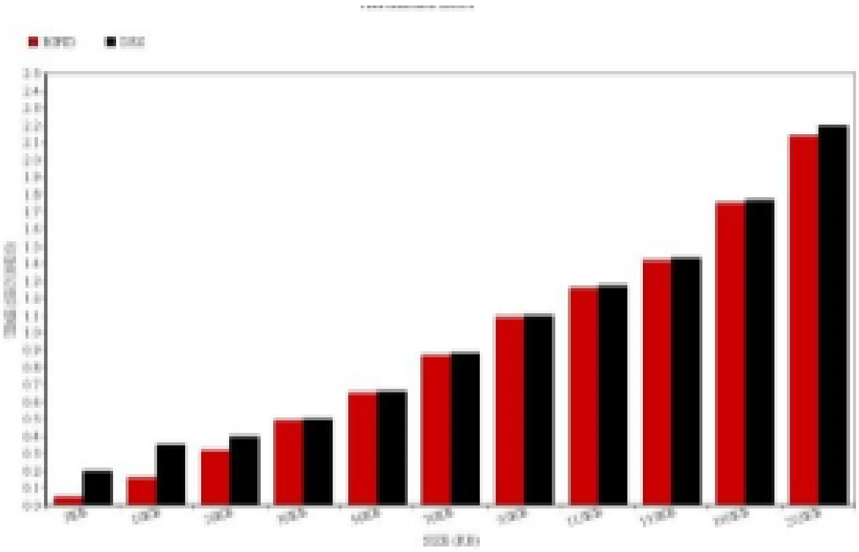
Bifid is a Lightweight Encryption Algorithm for Secure data transfer and storage. The shortcomings of the cloud and IoT in terms of constrained devices are highlighted. There in fact exist some lightweight cryptography algorithms that does not always exploit security-efficiency trade-offs.

Therefore, we chose our topic to be security in storage and dataflow in cloud storage and cloud computing using this Algorithm.

Time Phaze Analysis



Comparison between DES and BIFID:



Comparison between AES and BIFID: