Semiconductor Optoelectronics
ISSN: 1001-5868

DEVELOPING A MULTI-LEVEL ALGORITHM FOR ENCRYPTION AND DECRYPTION

Mr. Hirdesh Sharma[1], Dr. Gaurav Aggarwal[2]
[1]Research Scholar, **Jagannath University**, Bahadurgarh (Jhajjar), Haryana, India
ORCID iD: **0000-0002-1278-4135,** EmailID:- hirdesharma@gmail.com
[2]Professor & Dean, Dept. of CSE, Jagannath University, Bahadurgarh (Jhajjar), Haryana, India
ORCID iD: 0000-0002-6836-9352, EmailId:- gauravaggarw@gmail.com

ABSTRACT: The field of cryptography combines ideas, strategies, and methods for data transformation in order to obfuscate the factual content of data, prohibit its undiscovered modification, and/or forbid its unauthorized use. In the field of cryptography, encryption describes the use of an algorithm to change data, also referred to as plaintext (referred to as a cypher) to render it indecipherable to all save those with specialized expertise, also referred to as a key. Symmetric algorithms are appealing because they are 1000 times quicker than asymmetric ones and simple to use. Two authorised parties can only share the key using symmetric algorithms or secret key algorithms. Although a multidimensional scheme was in place in the current system, it did not provide security for small data. Work here by is improvement to existing system it is removing the problems of previous one. The problem is solved by giving seven rounds. Round one will operate on bits and last round is also on bits. Encryption go strong by strong as rounds followed means as number of rounds processed get increased encryption get more strong. Even a single word will be 3 times encrypted. Even a single line will be encrypted five times. The large text will have good security.
KEYWORDS: *Multidimensional Encryption, Cryptography, Encryption, symmetric algorithms.*

1. INTRODUCTION: The field that incorporates guidelines, tools, and techniques for transforming data to conceal its informational content, thwart unlawful usage, and/or prevent undetected alteration. Secret writing --- the most effective weapon for defending against various security risks. I will begin this chapter by introducing what is encryption how it works and encryption methods.

Let S-- Sender, R-- Recipient, O-- Intruder, K-- Key, Ke--- Encryption Key, Kd--- Decryption Key.

Encryption [1]

In the field of cryptography, encryption describes the use of an algorithm to change data, also referred to as plaintext (referred to as a cypher) to render it indecipherable to all save those with specialized expertise, also referred to as a key. A process used in cryptography to change plaintext into cypher text so that only the intended recipient may read the data. Data encryption

comes in a variety of forms, and it forms the backbone of network security. Public-key encryption and the Data Encryption Standard are examples of common forms. By encoding a message in a way that obscures its meaning, encryption is the process.

Decryption [1]

Is an encrypted communication transformed back into its original/null form during the reverse process?

Cryptosystem

A cryptosystem, which is a system for encrypting data and decrypting it

PT (plain text):- Plain text refers to a message's original format.

CT (cipher text):- The encrypted form of plain text is known as cipher text.

Cryptanalysts: - chore is to break an encryption.

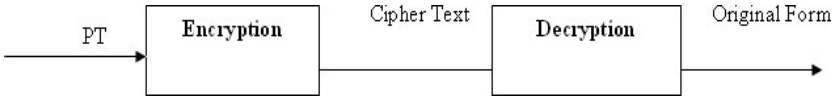


Figure 1.1 Cryptosystem

Symmetric Algorithms

when the keys for encryption and decryption are same.

$$P=D(K, (E(K, P)).$$

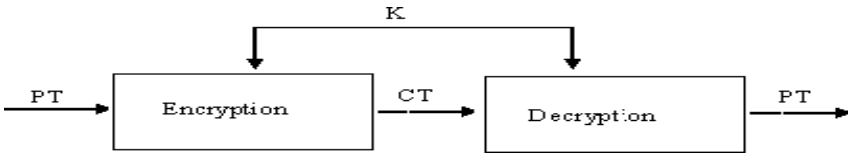


Figure 1.2 Symmetric Encryption

Asymmetric Algorithms

When keys are not same.

$$P=D(Kd, (E(Ke, P)).$$

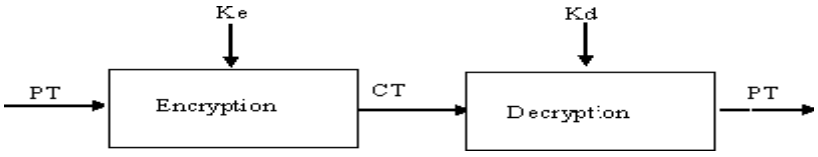


Figure 1.3 Asymmetric Encryption

There are essentially three categories of cryptographic techniques used to encrypt and decrypt data: Secret Key schemes, which employ the same key (also known as a shared key), for both operations (i.e. RSA algorithm), DES algorithm-based public key schemes and hash functions, wherein one-way processes are employed to guarantee the authenticity and integrity of messages, are both examples of public key encryption and decryption techniques (Shamir, 1997; Brenton and Cameron, 2003).

The purpose of this essay is to provide a new security paradigm that stops threats from

attackers (internal and external threats) of immediately attaining their objectives and limits the amount of time until the value and privacy of the protected data cease to be significant. This study proposes a multi-level method that can both encrypt and decrypt plain text messages. The algorithm has four security levels, the first three of which are dependent on block cypher and the fourth of which is predicated on stream cypher. Depending on the significance of the message's contents, the appropriate security level will be chosen and applied. While adopting the fourth level of encryption is designed to provide strategic security, levels (1-3) are intended to provide tactical security. The problem is solved by giving seven rounds. Round one will operate on bits and last round is also on bits. Encryption go strong by strong as rounds followed means as number of rounds processed get increased encryption get more strong. Even a single word will be 3 times encrypted. Even a single line will be encrypted fivetimes. The large text will have good security.

2. MULTI-LEVEL ENCRYPTION

Multi-level Encryption[2] objectives are to create a new protection model in a manner that prevents attacker threats (including internal and external threats) from achieving their immediate goals and handicaps them in terms of how long until the importance and privacy of the sensitive information no longer matter. It is suggested to use a multi-level technique to both encrypt and decrypt plain text messages. The technique is built upon a four-level security structure, utilising block cypher for the first three different levels and stream cypher for the fourth level. Depending on the significance of the message's contents, the appropriate security level will be chosen and applied.

While adopting the fourth level of encryption is designed to provide strategic security, levels (1-3) are intended to provide tactical security. Any communication (i.e., text file) can be separated into groups of eight lines, groups of eight words, groups of eight characters, and if possible, groups of eight characters per word. Each character is also converted to an encoded 8-binary value that differs from its true ASCII value. Of course, there are a variety of options available for Lines, Words, Characters, and Binary. The selection of eight, however, saves time (i.e. a good trade-off is between time and speed of execution of the algorithm). A robust cybersecurity level will be chosen in accordance with the significance of the communication or any individual components thereof. To choose the amount of security needed to encrypt the communication, there are four options:

I. Low level security
II. Moderate level security
III. High level security
IV. Critically high level security

The four dimensions of the algorithm—line, word, character, and binary (ASCII)—are represented by these levels of security in the following ways:

I. Only the line encryption dimension can be used to implement low levels of security.
II.Using just the word encryption dimension, moderate security levels can be implemented.
III. Character encryption alone can provide a high level of security.

Block cyphers fall under Levels I, II, and III. The character encryption dimension, however, can also be thought of as a stream cypher (Anderson,2001).

IV. Binary (ASCII) encryption alone can provide extremely high levels of security. It is thought that this portion is a stream cypher. Even while it is technically feasible to choose the security levels in a non-consecutive order, this is not advised because it adds no value and has no real-world implications.

3. PROPOSED ALGORITHM

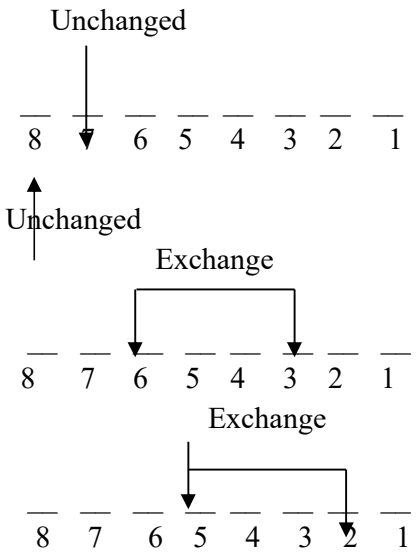
The process of this algorithm has seven rounds. The process start from Round 1.each round has its own description and owns working criteria means to say on which (bit, character. line…) round will operate.

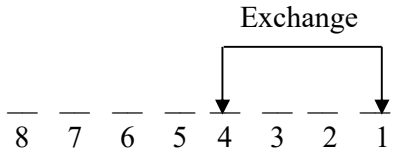
- Round 1 on bits.
- Round 2 on character.
- Round 3 on paragraph.
- Round 4 on lines.
- Round 5 on words.
- Round 6 on character.
- Round 7 on bits.

Round 1 will do permutation of bits. Bits that were representing the character of PT. The permutation will be done in such a manner that new combination of bits will in turn give a new character. That will be character of CT. So first Round has given first level encrypted PT.

Steps

Step 1: Pick the character.
Step 2: Convert into bits.
Step 3: Per mutate as follows
Step 4: Convert the new bit combination into character.
Step 5: Put this character in the place of original character.

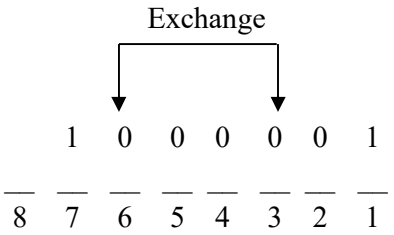


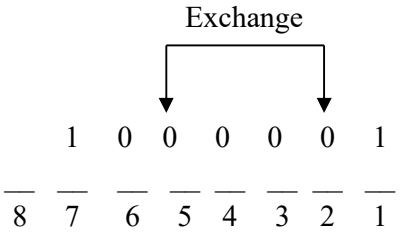


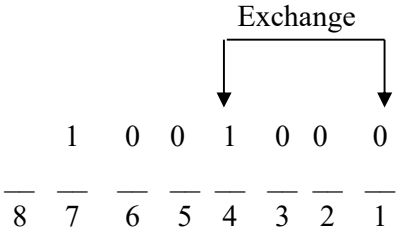
8→unchanged
7→unchanged
6↔3 exchange
5↔2exchange
4↔1 exchange

Example: 65 is ASCII code for A

Bit representation 1 0 0 0 0 0 1







The bit representation is now for 80
Which is in turn representation for P?

3.2.2 Description of Round 2

Round 2 operate on characters First of All blocks of eight characters are constructed and each block of eight characters is permuted by left shifting of one character. If the last block is not of eight characters then padding will done to make block of eight.

Step 1: Make the block of eight characters.
Step 2: If necessary do the padding.

Step 3: Rotate the character by left shifting one.

1←2
2←3
3←4
4←5
5←6
6←7
7←8
8←1

For example
Take the word 'REPLACED'

Then after the implementation of 2nd round the word will become 'EPLACEDR'
(SINGLE QUOTS ARE HERE FOR JUST HIGHLIGHTING)

3.2.3 Description of Round 3

Round 3 starts processing on paragraph .it say if your text is having n paragraph where range of n start from one then n paragraphs will be shuffled Rotate the paragraph in circular by one movement means Nth paragraph will be replaced by $(N-1)^{th}$ means to say

1←2
2←3
N-1←N…….
N←1

3.2.4 Description of Round 4

Round 4 operate on lines. Lines will be shuffled by directed shuffling. Don't worry if you are having two lines, Lines will be shuffled in circular

1←2
2←3
N-1←N…….
N←1

3.2.5 Description of Round 5

This level work on blocks. The blocks of 8 characters each will be shuffled in a line. Blocks will be rotated in circular manner by 1 position left means to say

1←2
2←3
N-1←N…….
N←1

3.2.6 Description of Round 6

Round 6 again operate on characters. Again blocks of eight characters are constructed. Each

block of eight characters is permuted by left shifting of one character. If the last block is not of eight characters, then padding will done to make last block of eight characters.

Step 1

Make the block of eight characters.

Step 2

If necessary do the padding.

Step 3

Rotate the character by left shifting one.

1←2
2←3
3←4
4←5
5←6
6←7
7←8
8←1

For example

Take the word ‘EPLACEDR’

Then after the implementation of 2nd round the word will become ‘PLACEDRE’

(SINGLE QUOTS ARE HERE FOR JUST HIGHLIGHTING)

3.2.7 Description of Round 7

Round 7 will again do permutation of bits. Bits that were representing the character of CT(up to 6 rounds).The permutation will be done in such a manner that new combination of bits will in turn give a new character. That will be character of final CT.

Steps

Step1

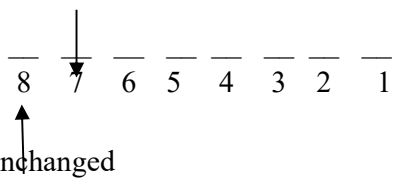
Pick the character.

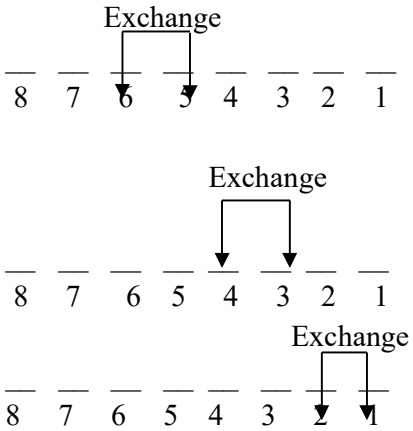
Step 2

Convert into bits.

Step 3

Per mutate as follows





8→unchanged
7→unchanged
6↔5exchange
4↔3exchange
2↔1exchange

Step 4

Convert the new bit combination into character.

Step 5

Put this character in the place of original character.

4. OUTPUTS:

In this the encryption is done in seven different steps, which makes the data more secure. The different steps of encryption is shown below

4.1. TEXT DATA

Here we are taking text data in notepad shown below in Figure 4.1 as a snapshot. This is a plain text data. We apply first level of encryption on this plaintext data.

```
Checking file system on C:
The type of the file system is FAT32.


One of your disks needs to be checked for consistency. You
may cancel the disk check, but it is strongly recommended
that you continue.
Windows will now check the disk.
Volume Serial Number is 188D-7DF2
      7255192 KB total disk space.
       675284 KB in 838 hidden files.
         6896 KB in 1185 folders.
      3295268 KB in 23955 files.
      3277740 KB are available.

         4096 bytes in each allocation unit.
      1813798 total allocation units on disk.
       819435 allocation units available on disk.
Checking file system on C:
The type of the file system is FAT32.


One of your disks needs to be checked for consistency. You
may cancel the disk check, but it is strongly recommended
that you continue.
Windows will now check the disk.
Volume Serial Number is 188D-7DF2
\Documents and Settings\AMIT CHUGH\Application Data\Vidalia\vidalia.pid  first allocation
unit is not valid. The entry will be truncated.
Convert lost chains to files (Y/N? Yes
4 KB in 1 recovered files.
Windows has made corrections to the file system.
```

Figure 4.1 Text Data for Encryption

4.2. FIRST LEVEL ENCRYPTION

The Figure 4.2 below shows the change that take place when we implement first level encryption on the text data that we have taken for encryption. In this level encryption is done on bits only.

```
XEl\]Mu| tMel ^O^flm }u X□
bEl fOFl }t fEl tMel ^O^flm M^ pHb□□5


yul }t O}nV dM^]^ ulld^ f} Tl \El\]ld t}V \}u^M^flu\O5 K}n
mLO \Lu\le fEl dM^] \El\]% Tnf Mf M^ ^fV}u|eO Vl\}mmludld
fELf O}n \}ufMunl5
zMud}~^ ~Mee u}~ \El\] fEl dM^]5
r}enml ZlVMLe qnmTlV M^ □□□`->`p□
      >□..□□□ YP f}fLe dM^] ^FL\l5
       6>.□□& YP Mu □□□ EMddlu tMel^5
         6□□6 YP Mu □□□. t}edlV^5
      □□□.□6□ YP Mu □□□.. tMel^5
      □□>>>&□ YP LVl LvLMeLTel5

         &□□6 TOfl^ Mu lL\E Lee}\LfM}u nuMf5
      □□□□>□□ f}fLe Lee}\LfM}u nuMf^ }u dM^]5
       □□□&□. Lee}\LfM}u nuMf^ LvLMeLTel }u dM^]5
XEl\]Mu| tMel ^O^flm }u X□
bEl fOFl }t fEl tMel ^O^flm M^ pHb□□5


yul }t O}nV dM^]^ ulld^ f} Tl \El\]ld t}V \}u^M^flu\O5 K}n
mLO \Lu\le fEl dM^] \El\]% Tnf Mf M^ ^fV}u|eO Vl\}mmludld
fELf O}n \}ufMunl5
zMud}~^ ~Mee u}~ \El\] fEl dM^]5
r}enml ZlVMLe qnmTlV M^ □□□`->`p□
c`}\nmluf^ Lud ZlffMu|^cHiIb XAjxAcHFFeM\LfM}u `LfLcrMdLeMLcvMdLeML5FMd  tMV^f Lee}\LfM}u
nuMf M^ u}f vLeMd5 bEl lufVO ~Mee Tl fVnu\Lfld5
X}uvlVf e}^f \ELMu^ f} tMel^ □K=q□? Kl^
& YP Mu □ Vl\}vlVld tMel^5
zMud}~^ EL^ mLdl \}VVl\fM}u^ f} fEl tMel ^O^flm5
```

Figure 4.2 Data after First Level Encryption

4.3. SECOND LEVEL ENCRYPTION

Here in second level the data after first level encryption is further encrypted as shown in Figure 4.3. In this level the encryption is done on characters. Each character is further encrypted in this level.

```
El\]Mu|XtMel ^O flm }u ^□X
El fOFlb}t fEl  Mel ^O^tlm M^ pfb□□5H


ul }t OynV dM^]} ulld^ ^} Tl \Ef\]ld t}l \}u^M^Vlu\O5 Kfn}
LO \Lu\me fEl dl^] \El\M% Tnf M] M^ ^fVfu|eO Vl}}mmludl\d
ELf O}nf\}ufMun 5l
Mud}~^ zMee u}~~\El\] f l dM^]5E
}enml ZrVMLe qnlTlV M^ m□□`->`p□□
     >□ .□□□ YP.f}fLe d ^] ^FL\M5l
      6 .□□& YP>Mu □□□  Mddlu tEel^5M
        6□□6 YP Mu □□□. t}edlV^ 5
     □□ .□6□ YP□Mu □□□.  tMel^5.
     □□ >>&□ YP>LVl LvL eLTel5M

        &□□6 TO l^ Mu lf\E Lee}LLfM}u n\Mf5u
     □□ □>□□ f}□Le Lee}fLfM}u n\Mf^ }u uM^]5d
      □ □&□. Le□}\LfM}uenuMf^ L LMeLTelv}u dM^] 5
El\]Mu|XtMel ^O flm }u ^□X
El fOFlb}t fEl  Mel ^O^tlm M^ pfb□□5H


ul }t OynV dM^]} ulld^ ^} Tl \Ef\]ld t}l \}u^M^Vlu\O5 Kfn}
LO \Lu\me fEl dl^] \El\M% Tnf M] M^ ^fVfu|eO Vl}}mmludl\d
ELf O}nf\}ufMun 5l
Mud}~^ zMee u}~~\El\] f l dM^]5E
}enml ZrVMLe qnlTlV M^ m□□`->`p□□
`}\nmluc^ Lud ZfffMu|^cliIb XAjHAcHFFeMxLfM}u `\fLcrMdLLMLcvMdLeML5FMd etMV^f L e}\LfM}e
nuMf Mu u}f vL^Md5 bElelufVO ~ ee Tl fMnu\LfldV5
}uvlVf X}^f \ELeu^ f} tMel^ □K=M? Kl^q
 YP Mu & Vl\}vl□ld tMelV5^
Mud}~^ zL^ mLdlE\}VVl\f }u^ f} MEl tMelf^O^flm5
```

Figure 4.3 Data after Second Level Encryption

4.4. THIRD LEVEL ENCRYPTION

After encrypting the data character wise, the data obtained is further moved for another level of encryption in third level. In this level the data is arranged in paragraph and each paragraph is encrypted further for getting secure data as shown in Figure 4.4.

```
El fOFlb}t fEl  Mel ^O^tlm M^ pfb□□5H


ul }t OynV dM^]} ulld^ ^} Tl \Ef\]ld t}l \}u^M^Vlu\O5 Kfn}
LO \Lu\me fEl dl^] \El\M% Tnf M] M^ ^fVfu|eO Vl}}mmludl\d
ELf O}nf\}ufMun 5l
Mud}~^ zMee u}~~\El\] f l dM^]5E

El\]Mu|XtMel ^O flm }u ^□X
     >□ .□□□ YP.f}fLe d ^] ^FL\M5l
      6 .□□& YP>Mu □□□  Mddlu tEel^5M
        6□□6 YP Mu □□□. t}edlV^ 5
     □□ .□6□ YP□Mu □□□.  tMel^5.
     □□ >>&□ YP>LVl LvL eLTel5M

        &□□6 TO l^ Mu lf\E Lee}LLfM}u n\Mf5u

}enml ZrVMLe qnlTlV M^ m□□`->`p□□
      □ □&□. Le□}\LfM}uenuMf^ L LMeLTelv}u dM^] 5
El\]Mu|XtMel ^O flm }u ^□X
El fOFlb}t fEl  Mel ^O^tlm M^ pfb□□5H


ul }t OynV dM^]} ulld^ ^} Tl \Ef\]ld t}l \}u^M^Vlu\O5 Kfn}
LO \Lu\me fEl dl^] \El\M% Tnf M] M^ ^fVfu|eO Vl}}mmludl\d

     □□ □>□□ f}□Le Lee}fLfM}u n\Mf^ }u uM^]5d
Mud}~^ zMee u}~~\El\] f l dM^]5E
}enml ZrVMLe qnlTlV M^ m□□`->`p□□
`}\nmluc^ Lud ZfffMu|^cliIb XAjHAcHFFeMxLfM}u `\fLcrMdLLMLcvMdLeML5FMd etMV^f L e}\LfM}e
nuMf Mu u}f vL^Md5 bElelufVO ~ ee Tl fMnu\LfldV5
}uvlVf X}^f \ELeu^ f} tMel^ □K=M? Kl^q
```

Figure 4.4 Data after Third Level Encryption

4.5. FORTH LEVEL ENCRYPTION

Here in the forth level the data after third level in further encrypted. In this level the encryption is done on lines of eight words. Each line is shuffled by direct shuffling shown as in Figure 4.5.

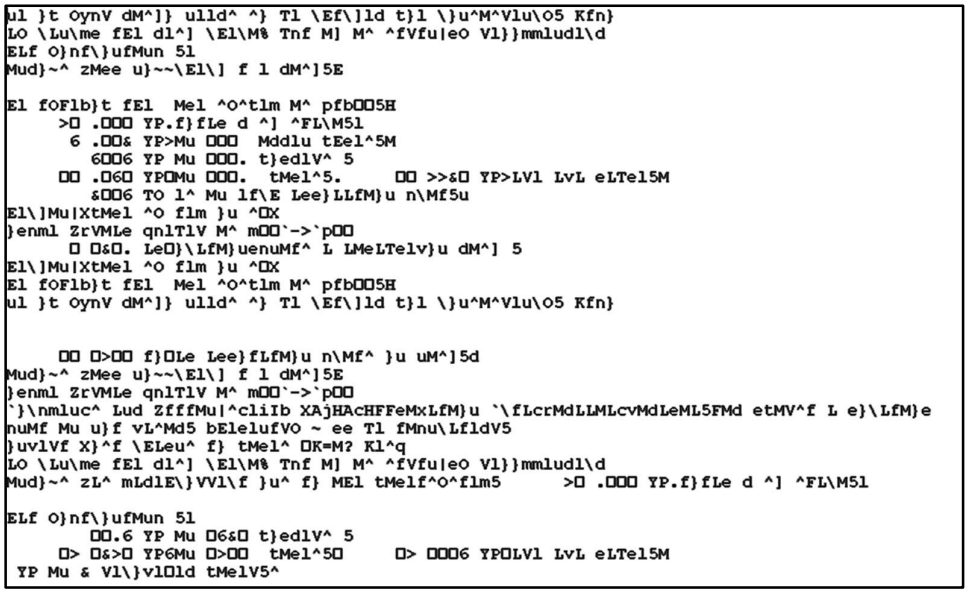


Figure 4.5 Data after Forth Level Encryption

4.6. FIFTH LEVEL ENCRYPTION

After encrypting the data line wise, the data obtained is further moved for another level of encryption in fifth level. In this level the data is arranged in block of 8 characters and each block is shuffled in a line for getting secure data as shown in Figure 4.6.

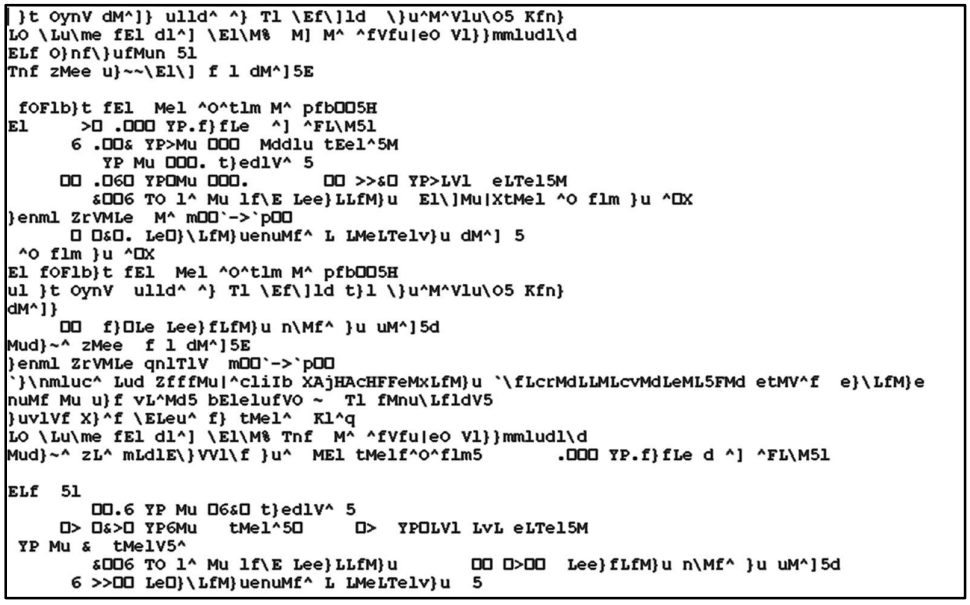


Figure 4.6 Data after Fifth Level Encryption

4.7. SIXTH LEVEL ENCRYPTION

Here in sixth level the data after fifth level encryption is further encrypted. In this level the blocks of eight characters are constructed. In the block each character is permuted by left shifting of one character as shown in Figure 4.7.

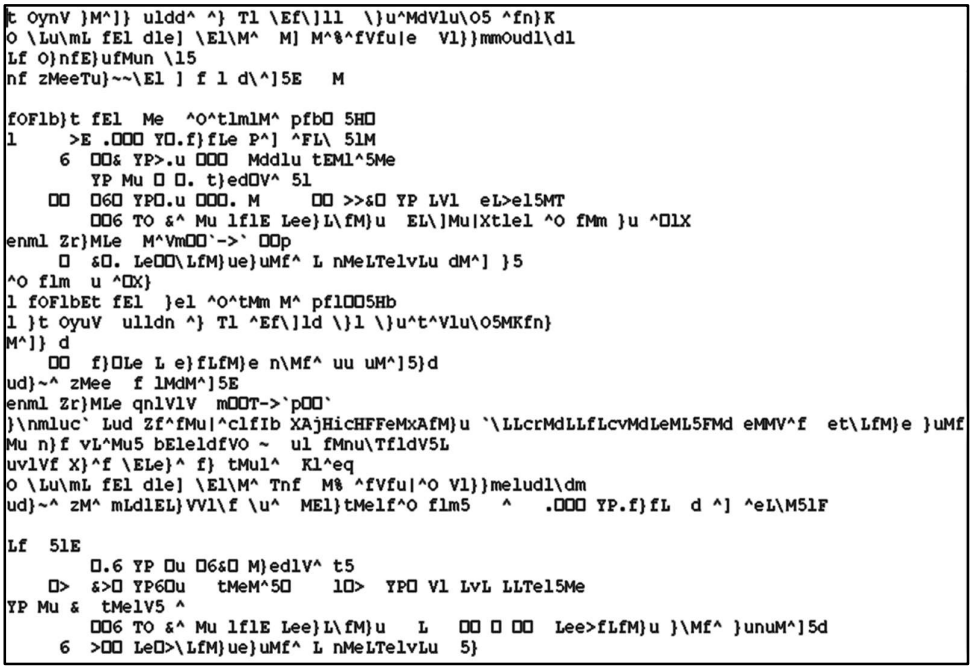


Figure 4.7 Data after Sixth Level Encryption

4.8. SEVENTH LEVEL ENCRYPTION

Here in seventh level the data after sixth level encryption is further encrypted. In this level the encryption is done on bits. Each bit is permutated in this level. The following Figure 4.8 shows the final cipher text obtained after applying all seven level of encryption.

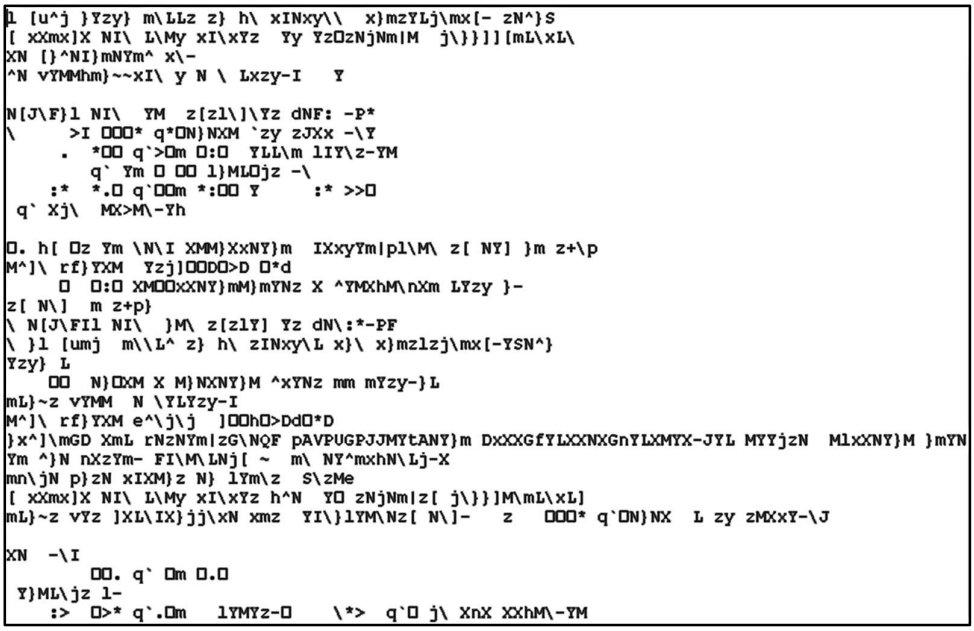


Figure 4.8 Data after Seventh Level Encryption

5.1. CIPHER TEXT

We are taking the data obtained after applying all the seven level of encryption. The Figure 5.1 below shows the data for decryption. This data is the input for first level of decryption.

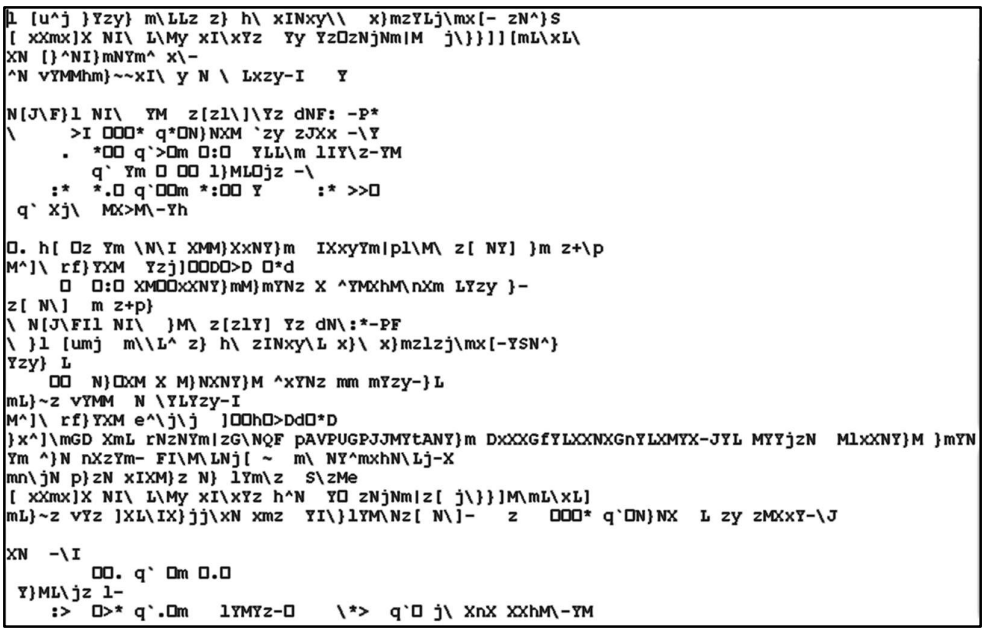


Figure 5.1 Data for Decryption

5.2. FIRST LEVEL DECRYPTION

The Figure 5.2 below shows the change that take place when we implement first level decryption on the cipher text data that we have taken for decryption. In this level decryption is done on bits only.

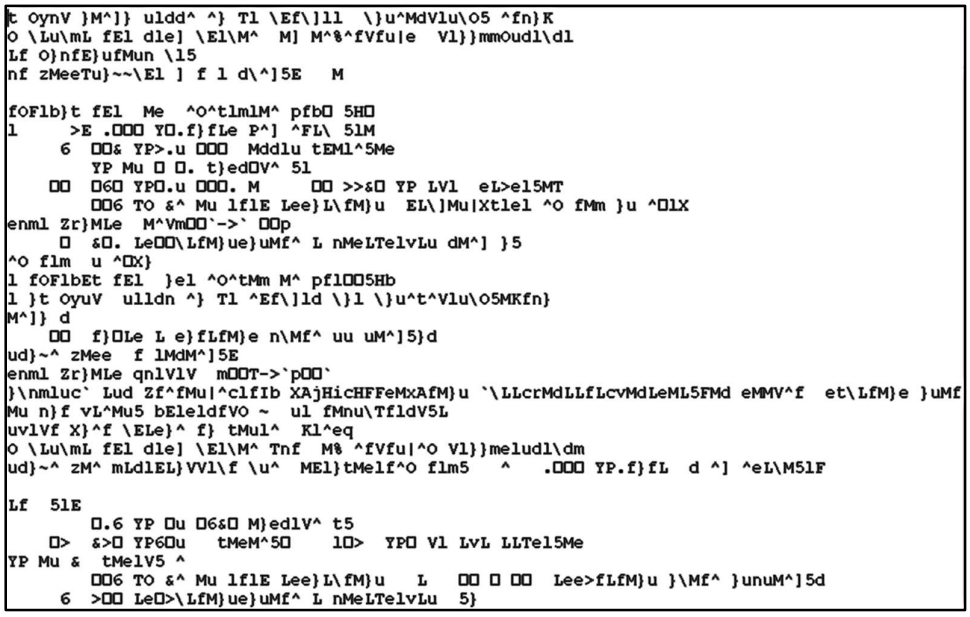


Figure 5.2 Data after First Level Decryption

5.3. SECOND LEVEL DECRYPTION

Here in second level the data after first level decryption is further decrypted. In this level the

blocks of eight characters are constructed. In the block each character is permuted by left shifting of one character, result of which is shown in Figure 5.3.

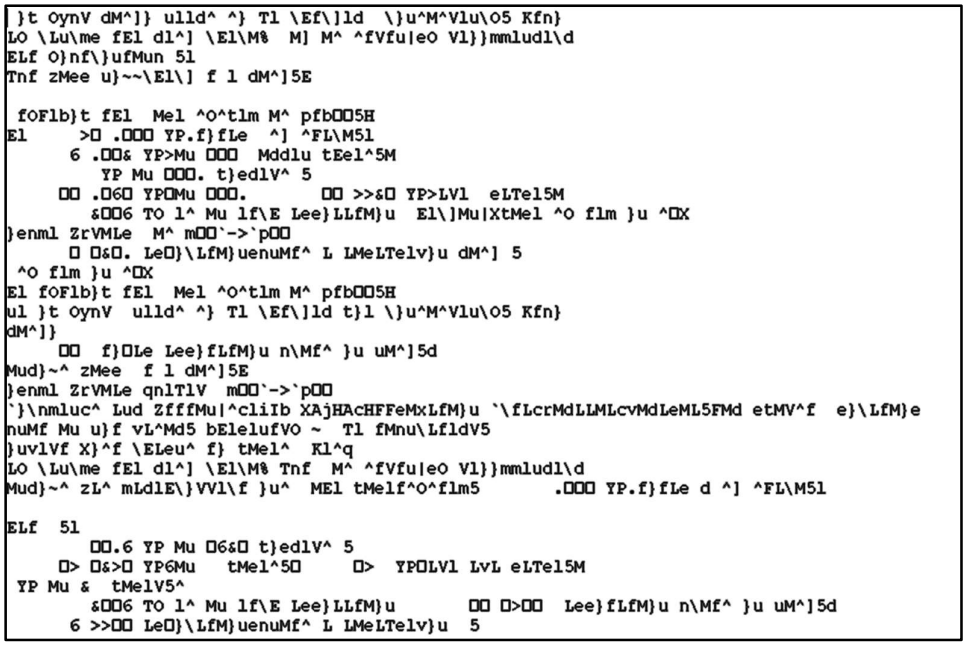


Figure 5.3 Data after Second Level Decryption

5.4. THIRD LEVEL DECRYPTION

After decrypting the data on blocks, the data obtained is further moved for another level of decryption in third level. In this level the data is arranged in block of 8 characters and each block is shuffled in a line for getting secure data as shown in Figure 5.4.

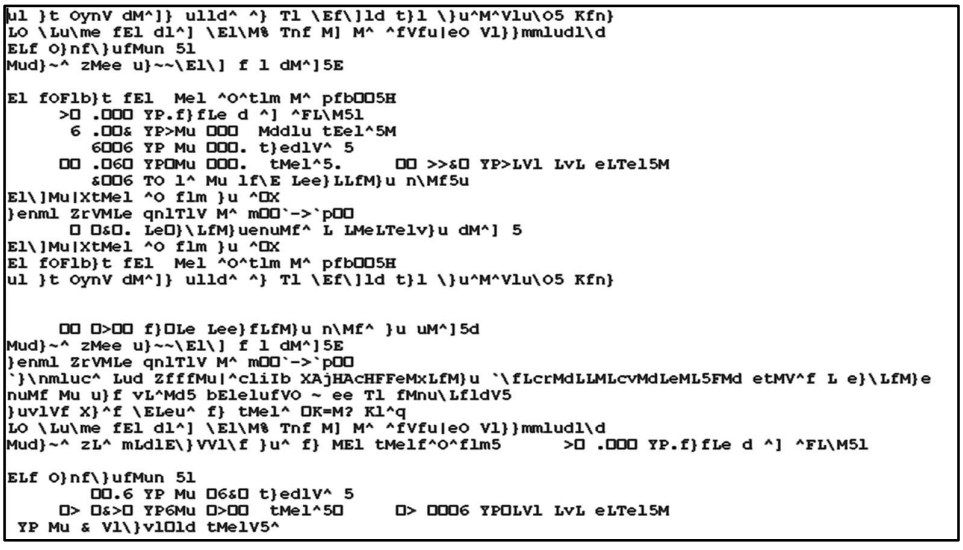


Figure 5.4 Data after Third Level Decryption

5.5. FORTH LEVEL DECRYPTION

Here in the forth level the data after third level in further decrypted. In this level the decryption is done on lines of eight words. Each line is shuffled by direct shuffling in a paragraph, output of which is shown in Figure 5.5.

```
El f0Flb}t fEl  Mel ^0^tlm M^ pfb□□5H


ul }t 0ynV dM^]} ulld^ ^} Tl \Ef\]ld t}l \}u^M^Vlu\05 Kfn}
L0 \Lu\me fEl dl^] \El\M% Tnf M] M^ ^fVfu|e0 Vl}}mmludl\d
ELf 0}nf\}ufMun 5l
Mud}~^ zMee u}~~\El\] f l dM^]5E

El\]Mu|XtMel ^0 flm }u ^□X
     >□ .□□□ YP.f}fLe d ^] ^FL\M5l
      6 .□□& YP>Mu □□□  Mddlu tEel^5M
        6□□6 YP Mu □□□. t}edlV^ 5
     □□ .□6□ YP□Mu □□□.  tMel^5.
     □□ >>&□ YP>LVl LvL eLTel5M

        &□□6 T0 l^ Mu lf\E Lee}LLfM}u n\Mf5u

}enml ZrVMLe qnlTlV M^ m□□`->`p□□
      □ □&□. Le□}\LfM}uenuMf^ L LMeLTelv}u dM^] 5
El\]Mu|XtMel ^0 flm }u ^□X
El f0Flb}t fEl  Mel ^0^tlm M^ pfb□□5H


ul }t 0ynV dM^]} ulld^ ^} Tl \Ef\]ld t}l \}u^M^Vlu\05 Kfn}
L0 \Lu\me fEl dl^] \El\M% Tnf M] M^ ^fVfu|e0 Vl}}mmludl\d

     □□ □>□□ f}□Le Lee}fLfM}u n\Mf^ }u uM^]5d
Mud}~^ zMee u}~~\El\] f l dM^]5E
}enml ZrVMLe qnlTlV M^ m□□`->`p□□
`}\nmluc^ Lud ZfffMu|^cliIb XAjHAcHFFeMxLfM}u `\fLcrMdLLMLcvMdLeML5FMd etMV^f L e}\LfM}e
nuMf Mu u}f vL^Md5 bElelufV0 ~ ee Tl fMnu\LfldV5
}uvlVf X}^f \ELeu^ f} tMel^ □K=M? Kl^q
```

Figure 5.5 Data after Forth Level Decryption

5.6. FIFTH LEVEL DECRYPTION

The data obtained after forth level decryption is further moved for another level of decryption in fifth level. In this level the data is arranged in paragraph and each paragraph is decrypted further for getting plain text data, as shown in Figure 5.6.

```
El\]Mu|XtMel ^0 flm }u ^□X
El f0Flb}t fEl  Mel ^0^tlm M^ pfb□□5H


ul }t 0ynV dM^]} ulld^ ^} Tl \Ef\]ld t}l \}u^M^Vlu\05 Kfn}
L0 \Lu\me fEl dl^] \El\M% Tnf M] M^ ^fVfu|e0 Vl}}mmludl\d
ELf 0}nf\}ufMun 5l
Mud}~^ zMee u}~~\El\] f l dM^]5E
}enml ZrVMLe qnlTlV M^ m□□`->`p□□
     >□ .□□□ YP.f}fLe d ^] ^FL\M5l
      6 .□□& YP>Mu □□□  Mddlu tEel^5M
        6□□6 YP Mu □□□. t}edlV^ 5
     □□ .□6□ YP□Mu □□□.  tMel^5.
     □□ >>&□ YP>LVl LvL eLTel5M

        &□□6 T0 l^ Mu lf\E Lee}LLfM}u n\Mf5u
     □□ □>□□ f}□Le Lee}fLfM}u n\Mf^ }u uM^]5d
      □ □&□. Le□}\LfM}uenuMf^ L LMeLTelv}u dM^] 5
El\]Mu|XtMel ^0 flm }u ^□X
El f0Flb}t fEl  Mel ^0^tlm M^ pfb□□5H


ul }t 0ynV dM^]} ulld^ ^} Tl \Ef\]ld t}l \}u^M^Vlu\05 Kfn}
L0 \Lu\me fEl dl^] \El\M% Tnf M] M^ ^fVfu|e0 Vl}}mmludl\d
ELf 0}nf\}ufMun 5l
Mud}~^ zMee u}~~\El\] f l dM^]5E
}enml ZrVMLe qnlTlV M^ m□□`->`p□□
`}\nmluc^ Lud ZfffMu|^cliIb XAjHAcHFFeMxLfM}u `\fLcrMdLLMLcvMdLeML5FMd etMV^f L e}\LfM}e
nuMf Mu u}f vL^Md5 bElelufV0 ~ ee Tl fMnu\LfldV5
}uvlVf X}^f \ELeu^ f} tMel^ □K=M? Kl^q
 YP Mu & Vl\}vl□ld tMelV5^
Mud}~^ zL^ mLdlE\}VVl\f }u^ f} MEl tMelf^0^flm5
```

Figure 5.6 Data after Fifth Level Decryption

5.7. SIXTH LEVEL DECRYPTION

Here in sixth level the data after fifth level decryption is further decrypted. In this level the

decryption is done on characters. Each character is further decrypted in this level, result of which is shown in Figure 5.7 .

```
XEl\]Mu| tMel ^O^flm }u X□
bEl fOFl }t fEl tMel ^O^flm M^ pHb□□5


yul }t O}nV dM^]^ ulld^ f} Tl \El\]ld t}V \}u^M^flu\O5 K}n
mLO \Lu\le fEl dM^] \El\]% Tnf Mf M^ ^fV}u|eO Vl\}mmludld
fELf O}n \}ufMunl5
zMud}~^ ~Mee u}~ \El\] fEl dM^]5
r}enml ZlVMLe qnmTlV M^ □□□`->`p□
      >□..□□□ YP f}fLe dM^] ^FL\l5
       6>.□□& YP Mu □□□ EMddlu tMel^5
         6□□6 YP Mu □□□. t}edlV^5
      □□□.□6□ YP Mu □□□.. tMel^5
      □□>>>&□ YP LVl LvLMeLTel5

         &□□6 TOfl^ Mu lL\E Lee}\LfM}u nuMf5
      □□□□>□□ f}fLe Lee}\LfM}u nuMf^ }u dM^]5
       □□□&□. Lee}\LfM}u nuMf^ LvLMeLTel }u dM^]5
XEl\]Mu| tMel ^O^flm }u X□
bEl fOFl }t fEl tMel ^O^flm M^ pHb□□5


yul }t O}nV dM^]^ ulld^ f} Tl \El\]ld t}V \}u^M^flu\O5 K}n
mLO \Lu\le fEl dM^] \El\]% Tnf Mf M^ ^fV}u|eO Vl\}mmludld
fELf O}n \}ufMunl5
zMud}~^ ~Mee u}~ \El\] fEl dM^]5
r}enml ZlVMLe qnmTlV M^ □□□`->`p□
c`}\nmluf^ Lud ZlffMu|^cHiIb XAjxAcHFFeM\LfM}u `LfLcrMdLeMLcvMdLeML5FMd  tMV^f Lee}\LfM}u
nuMf M^ u}f vLeMd5 bEl lufVO ~Mee Tl fVnu\Lfld5
X}uvlVf e}^f \ELMu^ f} tMel^ □K=q□? Kl^
& YP Mu □ Vl\}vlVld tMel^5
zMud}~^ EL^ mLdl \}VVl\fM}u^ f} fEl tMel ^O^flm5
```

Figure 5.7 Data after Sixth Level Decryption

5.8. SEVENTH LEVEL DECRYPTION

Here in seventh level the data after sixth level decryption is further decrypted. In this level the decryption is done on bits. Each bit is permutated in this level. The following Figure 5.8 shows the final plain text obtained after applying all seven level of decryption.

```
Checking file system on C:
The type of the file system is FAT32.


One of your disks needs to be checked for consistency. You
may cancel the disk check, but it is strongly recommended
that you continue.
Windows will now check the disk.
Volume Serial Number is 188D-7DF2
      7255192 KB total disk space.
       675284 KB in 838 hidden files.
         6896 KB in 1185 folders.
      3295268 KB in 23955 files.
      3277740 KB are available.

         4096 bytes in each allocation unit.
      1813798 total allocation units on disk.
       819435 allocation units available on disk.
Checking file system on C:
The type of the file system is FAT32.


One of your disks needs to be checked for consistency. You
may cancel the disk check, but it is strongly recommended
that you continue.
Windows will now check the disk.
Volume Serial Number is 188D-7DF2
\Documents and Settings\AMIT CHUGH\Application Data\Vidalia\vidalia.pid  first allocation
unit is not valid. The entry will be truncated.
Convert lost chains to files (Y/N? Yes
4 KB in 1 recovered files.
Windows has made corrections to the file system.
```

Figure 5.8 Data after Seventh Level Decryption

6. CONCLUSION:

Work here by is improvement to existing system it is removing the problems of previous one.The problem is solved by giving seven rounds. Round one will operate on bits and last round is on bits. Encryption go strong by strong as rounds followed means as number of

rounds processed get increased encryption get more strong. Even a single word will be 3 times encrypted. Even a single line will be encrypted five times. The large text will have good security.

7. REFERENCES

1. *N. Sharma, Prabhjot, & H. Kaur. (2017). A Review of Information Security using Cryptography Technique. International Journal of Advanced Research in Computer Science, vol. 8, no. Special Issue, pp. 323-326.*
2. *B. Preneel. (2010). Understanding Cryptography: A Textbook for Students and Practitioners. London: Springer.*
3. *Marshall Ball, Dana Dachman-Soled, & Mukul Kulkarni. (2020). New techniques for zero-knowledge: Leveraging inefficient provers to reduce assumptions, interaction, and trust. Daniele Micciancio and Thomas Ristenpart, editors, CRYPTO2020, PartIII, volume 12172 of LNCS, pages 674–703. Springer, Heidelberg.*
4. *Shohei Egashira, Yuyu Wang, & Keisuke Tanaka. (2019). Fine-grained cryptography revisited. StevenD. Galbraith and Shiho Moriai, editors, ASIACRYPT2019, PartIII, volume 11923 of LNCS, pages 637–666. Springer, Heidelberg.*
5. *Paulo S. L. M. Barreto. (2017). The WHIRLPOOL Hash Function.*
6. *Saarinen, M-J; Aumasson, & J-P. (2015). The BLAKE2 Cryptographic Hash and Message Authentication Code (MAC). IETF. doi:10.17487/RFC7693. RFC 7693. Retrieved 4.*
7. *J. Dittman, P. Wohlmacher and K. Nahrstedt, 2001 "Using Cryptographic and Watermarking Algorithms" IEEE Multimedia, vol. 8, no. 3, PP. 54-65.*
8. *Musbahj. Aqel, A. S.Abdul-Ahad, R. S.Qahwaji, 2009 "Multidimensional encryption algorithm for computer networks " Department of Electronic Image and Media Communication School of Informatics, Bradford University, Richmond Road, Bradford BD7 1DP, U.K.*
9. *Kefa Rabah, 2005 "Theory and Implementation of Data Encryption Standard: A Review" Information Technology Journal 4(4): 307-325.*
10. *http://en.wikipedia.org/wiki/Stream_cipher [accessed 21 June 2012].*
11. *http://en.wikipedia.org/wiki/Block_cipher [accessed 21 June 2012].*
12. *C. Peikari and S. Fogie 2003 "Maximum Wireless Security", SAMS Publishing.*
13. *Charles P. Pfleeger and Shari L. Pfleeger, 2012 "Security in computing" Prentice Hall PTR Upper Saddle River, NJ, USA. [online] available at: http://www.crypto.com/papers/. [accessed 20 August 2012].*
14. *Diaa Salama Abdul. Elminaam, Hatem Mohamed Abdul Kader and Mohie Mohamed Hadhoud, 2010 "Performance Evaluation of Symmetric Encryption Algorithms" International Journal of Network Security, Vol.10, No.3, PP.216–222, May 2010.*
15. *Eli Biham,Helena Handschuh, 2007 "seminar on symmetric cryptography", Dagstuhl seminar 07021*

16. *Federal Information Processing Standards (FIPS), Publication 197, "Advanced Encryption Standard" November 2001, [online] available at: http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf [accessed 17 August 2012].*
17. *Nadeem, Aamer, 2005 "A performance Comparison of Data Encryption Algorithms" IEEE Information and Communication Technologies, 2005. ICICT 2005. First International Conference, 2006-02-27, PP.84-89.*
18. *S.Z.S. Idrus, S.A. Aljunid, S.M.Asi, 2008 "Performance Analysis of Encryption Algorithms Text Length Size on Web Browsers" IJCSNS International Journal of Computer Science and Network Security, VOL.8 No.1, PP-20-25.*
19. *Arpad Incze "The basic of text encryption and decryption".*
20. *Tim Grembowski "Comparative Analysis of the Hardware Implementations of Hash Functions SHA-1 and SHA-512" Electrical and Computer Engineering, George Mason University, 4400 University Drive.*
21. *Federal Information Processing Standards Publication (FIPS) 180-4, "Secure Hash Standard" March 2012, [online] available at: http://csrc.nist.gov/publications/fips/fips180-4/fips-180-4.pdf [accessed 20 August 2012].*
22. *Sean O'Melia and Adam J. Elbirt, 2010 "Enhancing the Performance of Symmetric-Key Cryptography via Instruction Set Extensions" IEEE Transactions On Very Large Scale Integration (Vlsi) Systems, Vol. 18, No. 11, November 2010.*
23. *Li Xiaoming and Yun Zhao, 2011 "Research on Power Information Encryption Algorithm Based on Composite Chaotic System in Wavelet Transform Domain" ELSEVIER, Procedia Engineering 15 (2011) 2118 – 2122.*
24. *Carl Landwehr, Dan Boneh, John C. Mitchell, Steven M. Bellovin, Susan Landau and Michael E. Lesk, 2012. "Privacy and Cyber security: The Next 100 Years" Vol. 100, Proceedings of the IEEE.*
25. *Meikang Qiu, Wenzhong Gao, Min Chen, Jian-Wei Niu and Lei Zhang, 2011 "Energy Efficient Security Algorithm for Power Grid Wide Area Monitoring System" IEEE Transactions On Smart Grid, Vol. 2, No. 4, December 2011.*
26. *J. Ree, V. Centeno, J.Thorp and A. Phadka, 2010 "Synchronized phasor measurement applications in power systems" IEEE Trans. Smart Grid, vol. 1, no. 1, PP. 20-27.*