**Secret Key Encryption**

**A REPORT**

***Submitted by***

**Beni Iyaka**

***In fulfillment of requirement***

***Of***

**Bachelor of Science (BSc.)**

**IN**

**COMPUTER SCIENCE**

**MACS**

**HERIOT WATT UNIVERSITY**

**F20CN**

**OCTOBER 2015**

**Acknowledgement**

Many people have contributed to the accomplishment of this. Even though single phrases are hardly sufficient, I would like to thank the almighty God for his grace, I extend my sincere and hart felt thanks to **Dr. Hani, Computer Network Security Professor,** for providing us with the knowledge for carrying out the work.

I express my gratefulness to all the professors and staff of the Department of Computer Science of the Dubai campus for their support.

Beni Iyaka

Table of Contents

Introduction\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_1

Task1\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_2-13

Task2\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_14-15

Task3\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_16-18

Task4\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_19

Task5\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_19-21

Bibliography\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_22

**Introduction**

In cryptography, a secret key algorithm is also known as symmetric algorithm, in this algorithm, the encryption and decryption key is only known by the person/people exchanging secret messages over the network. In the secret key algorithm, the key would be shared by people communicating so that they may be able to encrypt and decrypt message. This algorithm doesn’t guarantee security because if the person loses their key, the system will be broken. In this report, I will be demonstrating how to use different mode, ciphers and hashes to ensure that the system becomes much safer.

**Goal**

The goal of the Coursework is to allow the students to share their knowledge on the symmetric cryptography and also implement their knowledge by developing an application.

**Assumptions**

* An encrypted file cannot be edited regardless of the circumstances.
* A password cannot be generated from the plaintext.
* After changing the header of the encrypted file, nothing will happen.

**Environment implementation**

Cryptography is mostly used in a shared network, usually work place whereby more nodes are connected to a switch and therefore when communicating over the network, confidential information will need to be encrypted so as to prevent other people on the network to view them.

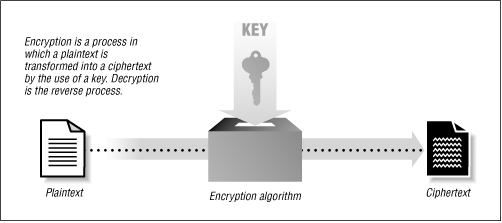
This can also be used in the online transaction system. While buying a certain item online, to prevent people to have access to the information which was input during the transaction, encryption will then be used to hide those information.

**Coursework Tasks**

**Task 1: Encryption using different ciphers and modes**

Encryption is a process of enhancing the security of a file or message by scrambling the contents so that it can be read only by the person who has the right encryption key to unscramble the message or file. For example: While purchasing somethings from a website, the details of the transaction such as address, credit card number an telephone number will be kept safe by encrypting it.

**Figure 1.1: An example of encryption**

 (Anon., 2012)

In figure 1.1, a message which is called **plaintext** is gone through a certain mathematical function of which a special encryption password called **key** is used so as to produce an encrypted message called **ciphertext.** (Mihir & Rogaway , 2005)

Encryption is used to protect the confidentiality of data stored on computer systems or transmitted via the internet or other computer networks. Encryption plays a vital role in assuring security of computer systems and communications as they provide:

Authentication: the origin of the message can be verified.

Integrity: proof that the message was not modified since it was sent.

Non-Repudiation: the person who sent the file cannot deny sending the message.

In cryptography, there are many algorithm for performing encryption and decryption of which Cipher is one of them. (James, 2006)

**Ciphers**

These are algorithms used for performing encryption and decryption which involves the transformation of the plaintext (Stallings, n.d.). In this report, I will be discussing 3 different types of ciphers which are Data Encryption standards, Advance Encryption Standards and RC5.

**Data Encryption Standards (DES)**

This is a symmetric key block cipher used in computer security cryptography of which block cipher is an algorithm that operate on a fixed length of group bits. (Springer, 2009)

Data encryption standard makes use of 3 different operations to successfully encrypt a file or text; namely: Confusion, Diffusion and Block cipher.

This is the operation whereby the statistics of the ciphertext should be dependent on the plaintext statistic so as to become too complicated that enemy is not able to crack it.

**Diffusion**

This is the operation whereby each digit of the plaintext influences many digits of the ciphertext. This just means if a bit of the plaintext is changed; many bit of the ciphertext is also changed.

**Block cipher**

This is the repetition of confusion and diffusion process until it reaches the 16th block.

When using the data encryption standards, the size of data encryption standard key is 64 bits of which 56 bits are randomly generated and used by the DES algorithm and 8 bits are used for error detection.

**Encrypting using Data Encryption Standard**

When doing encryption using DES, the user input a message “P” which is initially 64 bit; the message then goes through the “Initial Permutation (IP).”the is a table that specifies the input permutation on a 64 bit block of which, information are presented inform of a table. Then the permutated information is then divided in two “Left 0 (L0)” and “Right 0 (R0)” of which each of them contain 32 bit. The L0 is then XOR with the function of the key scheduling of which on its own it contains 56 bit so as to get an encrypted L0. Once the XOR is done, the output which is L1 will then be on the right side and the right side will then be on the left side as shown in figure 1.3. This process is done 16 times before having a R16 and L16; then these two will enter the Final permutation so as to get a Ciphertext. (James, 2006)

**Figure 1.2: Structure of DES**

Key Scheduling

Round function

**P**

**K**

**IP**

**f**

**FP**

**PC-2**

**C**

**16 Round**

**PC-1**

**Rot**

**Rot**

**R0 (32)**

**L0 (32)**

**R16**

**L16**

**PC-2**

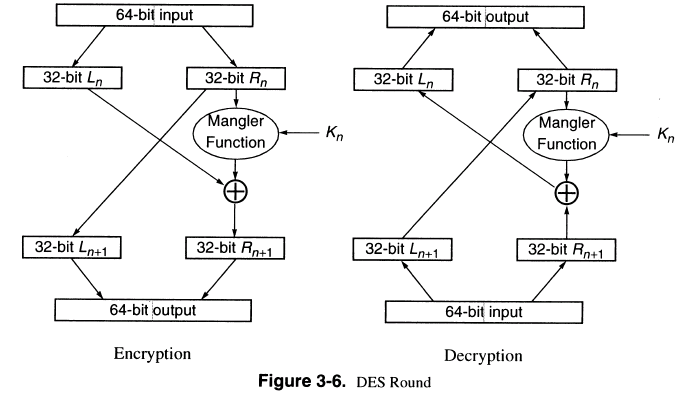
**64**

**56**

**64**

(Springer, 2009)

**Figure1.3 Encryption using DES**



(James, 2006)**Advance Encryption Standard (AES)**

This is a symmetric key block cipher used in computer security cryptography. AES is an approved encryption standard of the National of Standards and Technology (NIST). This was built to replace the Data Encryption Standard. AES is based on a principle known as Substitution-Permutation network; which means combining both substitution and permutation. (ITBusinessEdge, 2014). This is known to be generally fast in software and hardware.

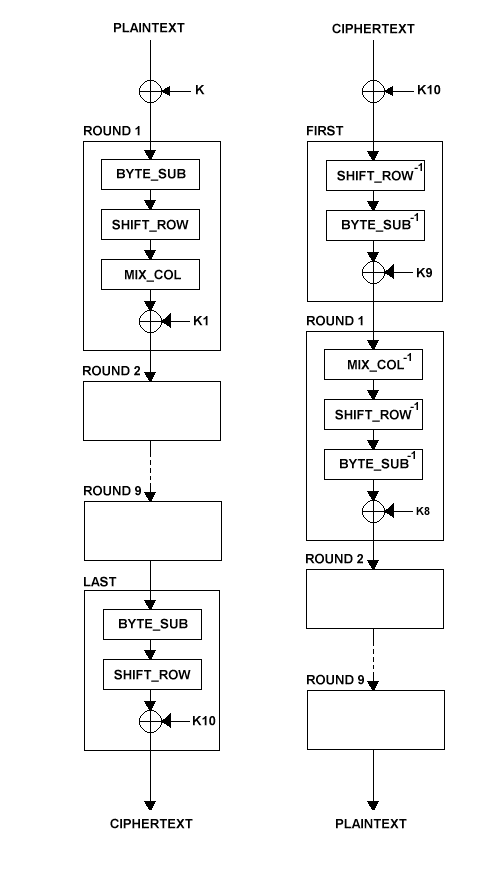
**Figure2.1 AES encryption**



(Corporation, 2015)

AES algorithm consists of three block ciphers name: AES-128, AES-192, and AES-256 because they are a combination of key sizes of 128, 192 and 256 bits of which each of them has a fixed block size of 128 bit data.

AES block cipher operates on an array of 16 bytes (128 bits) arranged as 4 rows and 4 columns. This array is called the state and it is denoted by s. AES applies byte-oriented transformation to encrypt state array. These transformations happen for a certain number of rounds depending on the key size. (ITBusinessEdge, 2014). A key size of 128 bits will have 10 rounds, 192 bits will have 12 rounds and 256 bits will have 14 rounds.

**Figure 2.2 AES encryption**

(ITBusinessEdge, 2014)

Encrypting data of 128 bits using Advanced Encryption Standard

The user input a message of 128 bits long and a key size of 128 bits. The key then goes through the key-scheduling process where it is transformed.

In the first block, the transformed key is then mixed with the plaintext using the XOR method. The output is sent to the second round. From the second round until the ninth round, the output of each round will go through the process of bytes substitution, rows shifting, column mixing and XOR with the key. In the final round, the output of the ninth round will go through a bytes substitution, rows shifting and XOR so as to get the encrypted file which is the ciphertext.

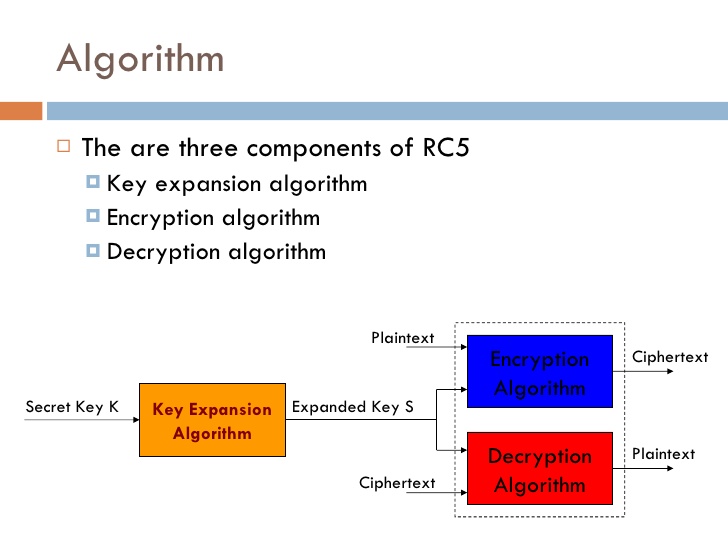
**CR5**

This is a symmetric block cipher where by the plaintext and ciphertext are fixed length bit sequence also known as blocks. This is a parametrized algorithm that contains blocks algorithms with variable block size, variable key size and a variable number of rounds.

RC5 is designated as RC5/W/R/S of which: W represents the “word size” in bits. The standard value is 32 bits with allowable values 16, 32 and 64. This algorithm encrypts two words per block so that the plaintext and ciphertext blocks are 2W bits long each. T represents the number of rounds. This has allowable values of 0 to 255. B represents the number of bytes in the secret key.

This is a symmetric key block cipher used in computer security cryptography. This is known for its simplicity. RC5 consists of 3 algorithm components namely: key encryption algorithm, encryption algorithm and decryption algorithm of which each algorithm uses 3 primitive operations namely: mod, XOR and rotation.

**Figure3.1 CR encryption**



**Doing encryption using CR5**

The key expansion algorithm expands the key inputted by the user so as to fill the expanded table so that the table should resemble the array of random binary words which then becomes the expanded key. This new key is then sent to the encryption algorithm where it will be combined with the plaintext in the encryption algorithm by going through the Mod, XOR and Rotation operation so as to get a ciphertext.

**Modes**

This is an algorithm that uses a block cipher algorithm to provide confidentiality or authentication because, a block cipher itself is only suitable for the secure encryption or decryption of a block. Modes describes how to apply a cipher’s single-block operation repeatedly so as to securely transform information that re bigger than the block. In this report, I will be discussing 3 different types of modes namely: Electronic Code Book, Cipher Block Channing and Cipher feedback mode.

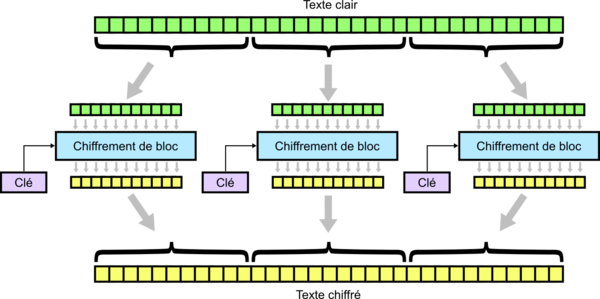
* **Electronic Code Block (ECB)**

This is a mode operation block cipher which divides the message into blocks of which each block is encrypted separately and also known to be simple. ECB has the ability to support a separate encryption key for each block type. This is one of the mode operation used by Advanced Encryption Standard block cipher to encrypt.

* **Doing encryption using ECB**

While encrypting a message using ECB mode, the user inputs the message which is then broken into blocks and each block goes through the advanced encryption standard where it will be combined with the key so as to produce an output which is the ciphertext.

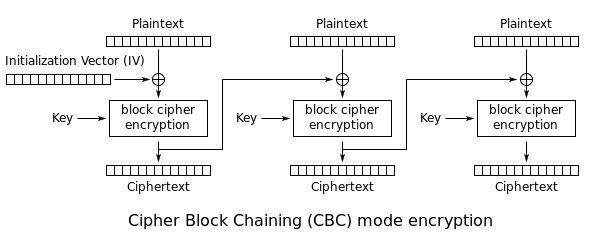
**Figure 4.1 Encryption using ECB**



* **Cipher Block Channing (CBC)**

This is one of mode operation block cipher which breaks the message into blocks and each block of the message is XOR with the ciphertext of the previous block before encrypting the block. (Mihir & Rogaway , 2005). In this mode operation, the first block is XOR with an initialization vector so as to make each message unique.

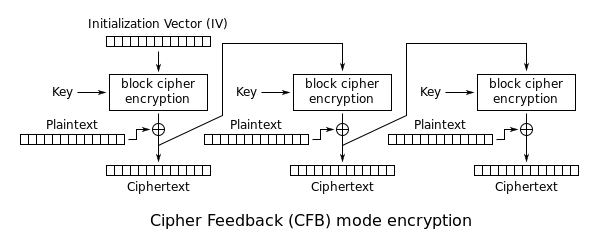
**Figure 4.2 CBC mode**



* **CFB**

This is one of the mode operation block cipher which breaks the message into blocks and each block of the message is XOR with the ciphertext of the previous block before it should be encrypted. Cipher feedback works and also described similar with CBC except that the initialization vector and the key goes through the block cipher encryption and then XOR with the plaintext.

**Figure 4.3 CFB mode**

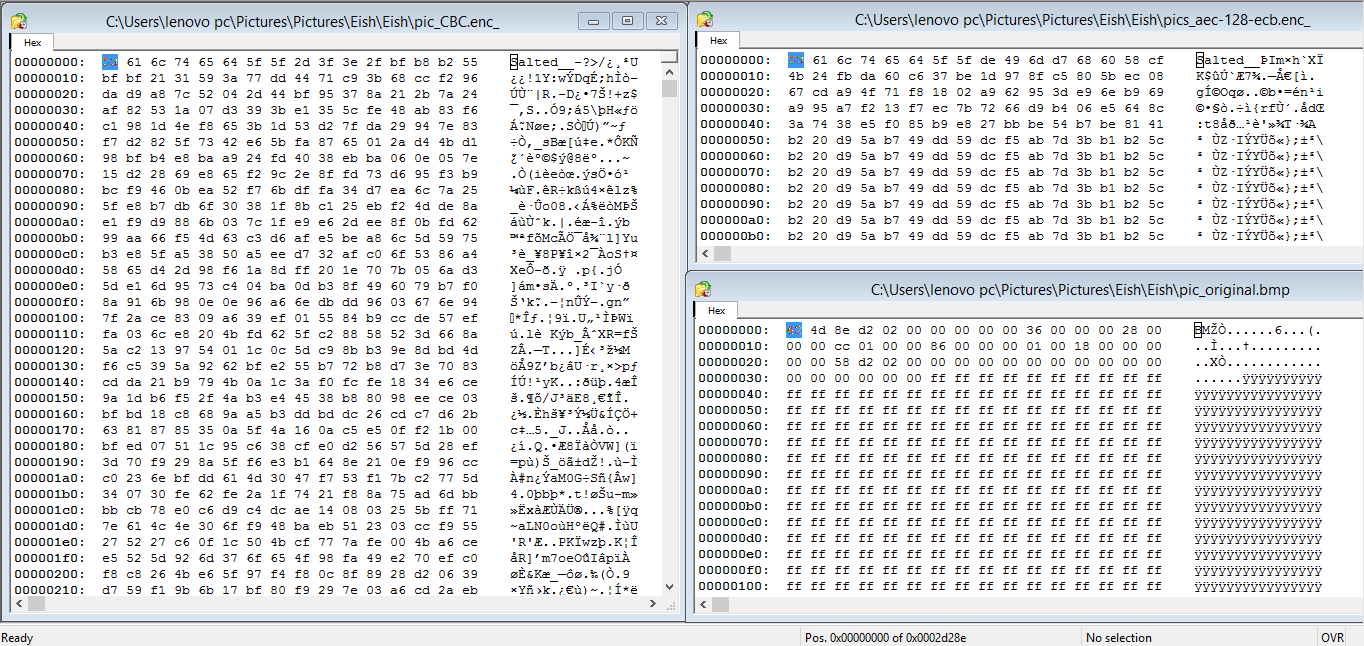


**Task 2**

1. **ECB vs CBC**

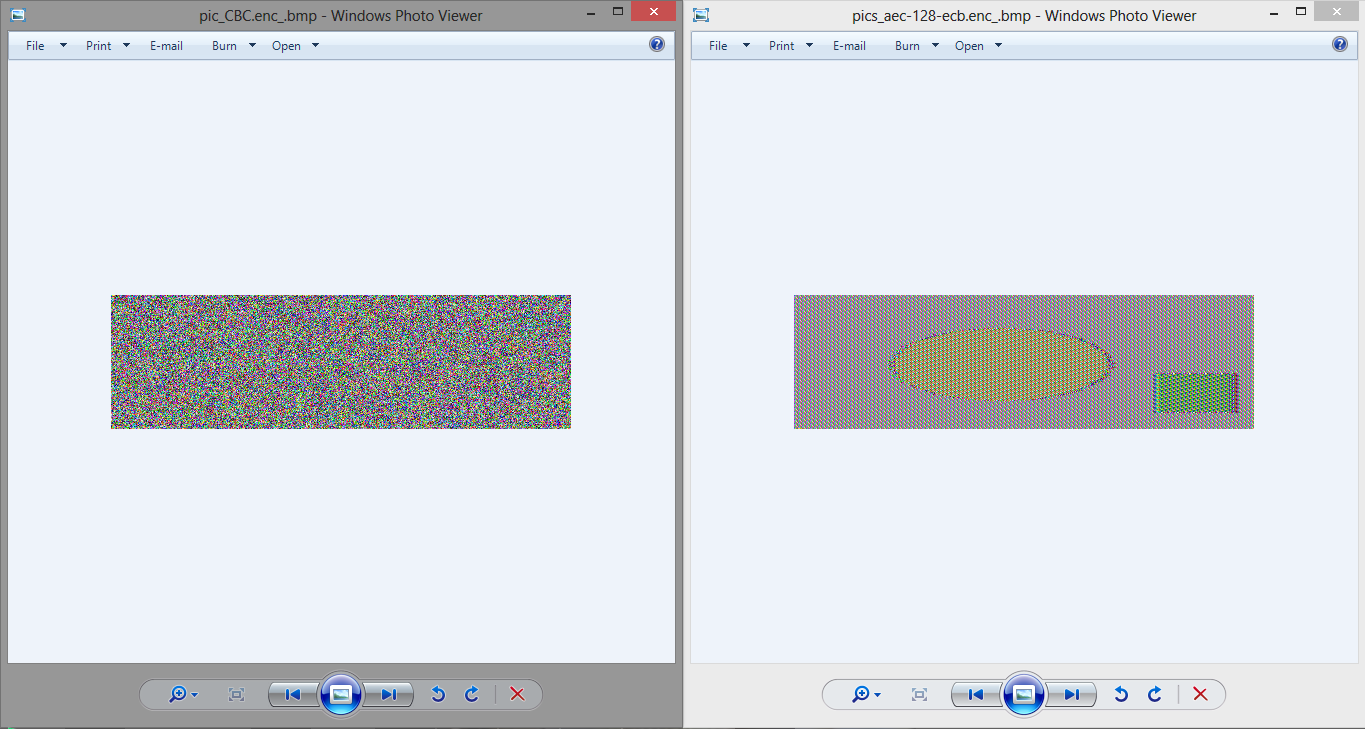
* After encrypting the picture, I cannot open or view the picture.
* So I used HHD Hex software to edit the header file which was copied from the original file.

**Figure 5.1 ECB & CBC encryption**



* And this was the output.

**Figure 5.2 ECB & CBC after encryption**

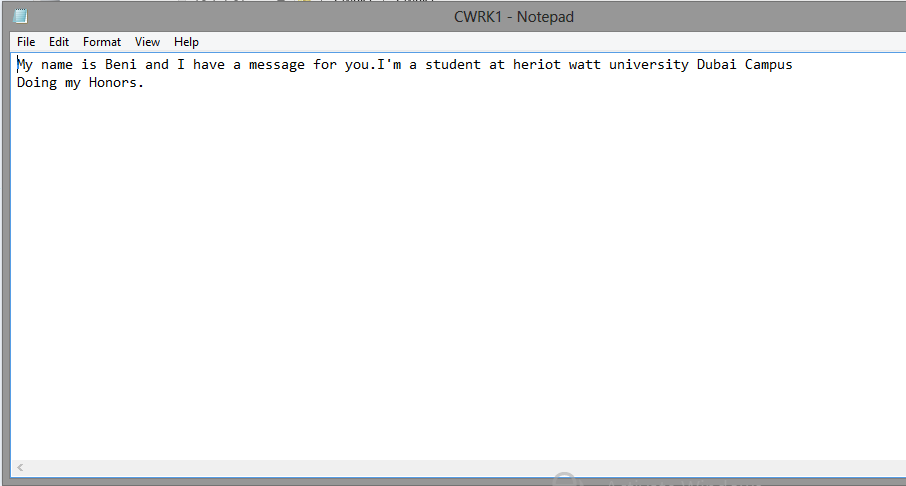


Looking at the two images, CBC encryption mode is more confidential therefor, even after changing the header of the file, the encrypted file still hides the full plaintext comparing to the ECB encryption mode which after changing the header, we have a glimpse of what the plaintext looks like.

**Task 3**

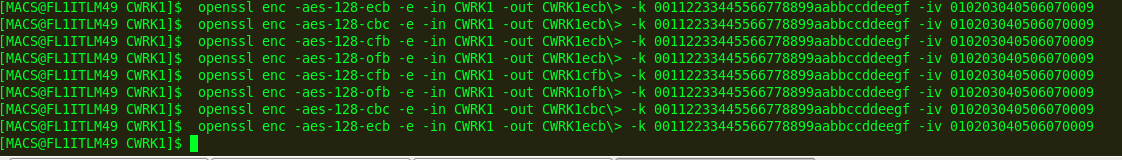
1. File created named CWRK1

**Figure 6.1 CWRK1 file**



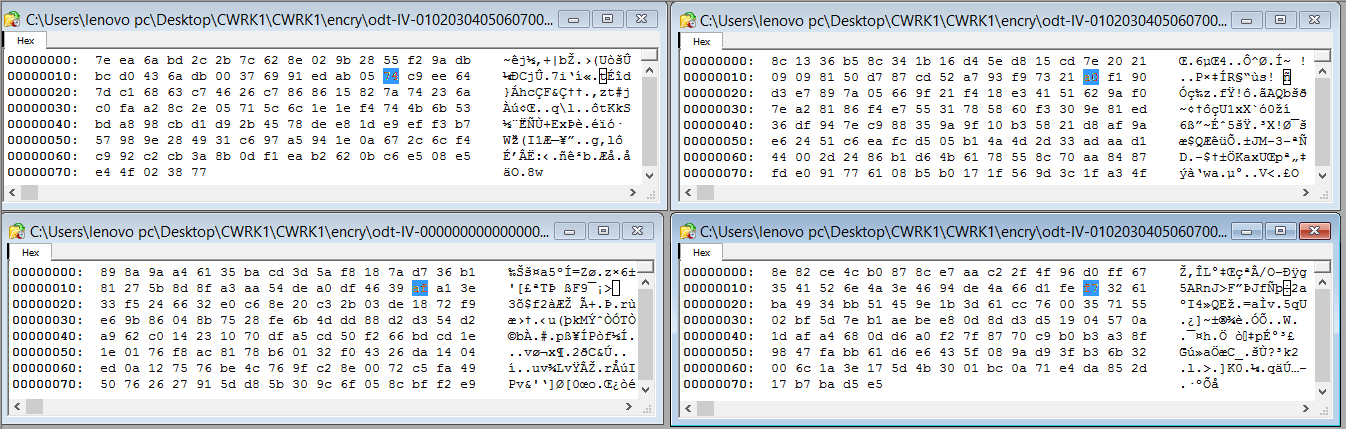
1. Doing the encryption of the CWRK1 file

**Figure 6.2 Encrypting CWRK1**



1. Changing the 30th bits of each mode.

**Figure 6.3 Editing Header**



1. Decryption

In the decryption of the message, in ECB, I don’t expect to recover much of the message because this mode encrypt and decrypt each block separately.

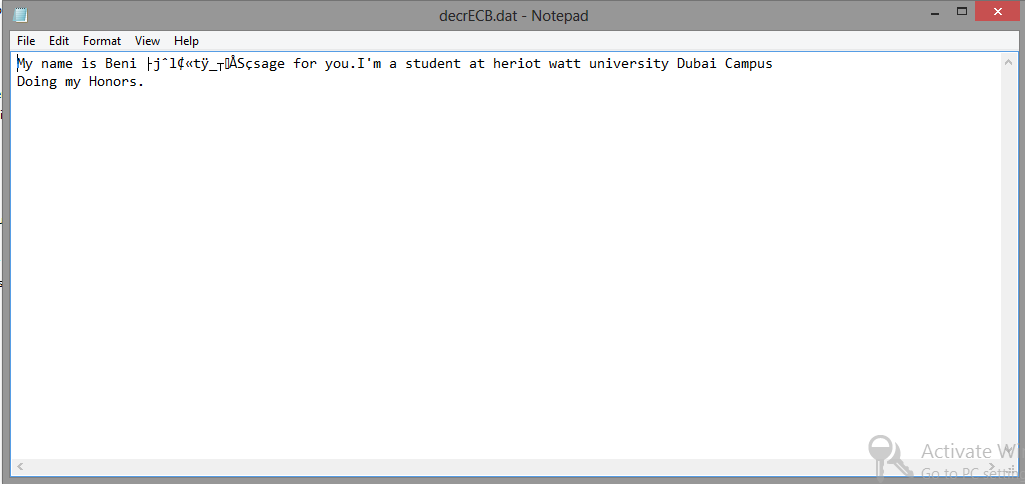
In the decryption of the message in CBC, due to the fact that encryption is using the ciphertext from the previous output, more block will be affected compared to the ECB.

In the decryption of the message in CFB, more blocks should be affected because encryption is done by XOR the output of the key and IV. Comparing to other modes, more blocks will be affected.

In the decryption of the message in OFB, I expect only a single bit to be corrupted because it is a key-generator mode. So most if not all of the message will be recovered.

ECB

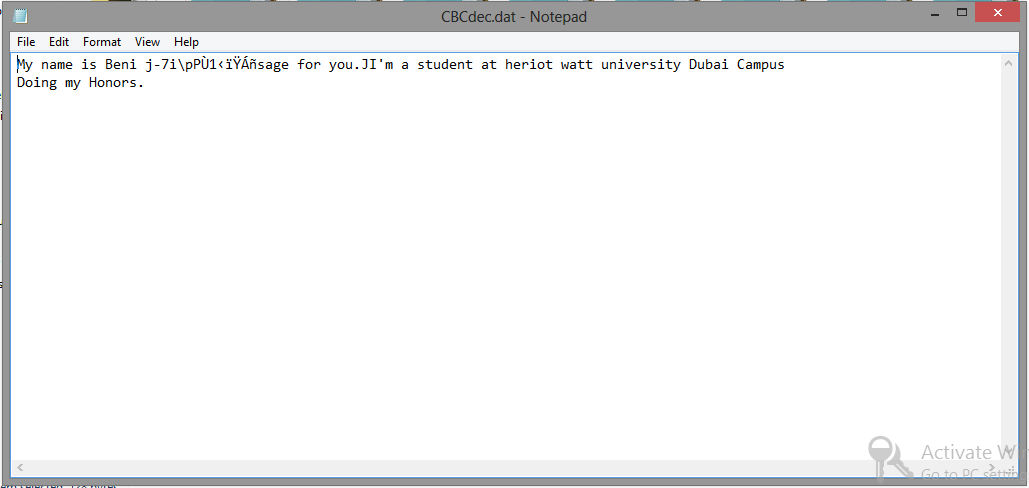
**Figure 6.4 ECB output**



With this mode, only one block which is affected with the change of bits but the rests are readable.

CBC

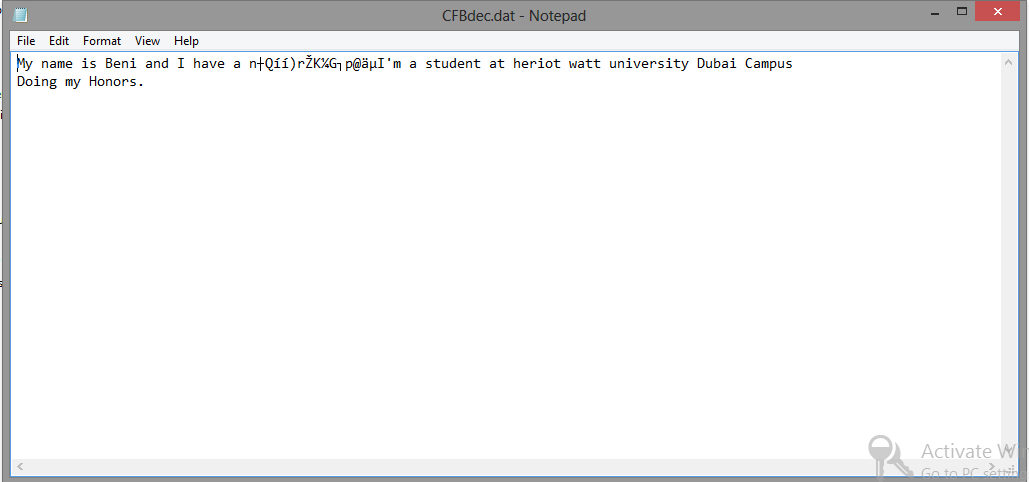
**Figure 6.5 CBC output**



With this mode, two blocks are affected by the change of bits.

CFB

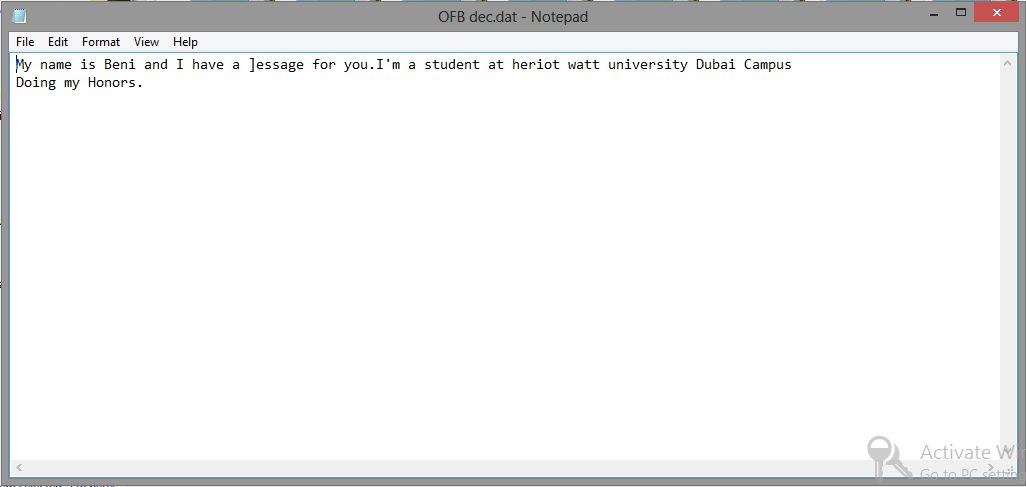
**Figure 6.6 CFB output**



In this mode, many blocks are affected by changing the 30th byte

OFB

**Figure 6.7 OFB output**



In this mode, most of the message is showing regardless of in the change of the 30th byte change.

**Task 4**

Looking at all the modes, CFB mode hides most of the information.

In ECB mode, the encryption and decryption of a message is achieved by breaking the message in blocks and each block encrypted or decrypted separately.

In CBC mode, the encryption is done by using the ciphertext from the previous output, which result to more blocks being affected if a single byte is changed.

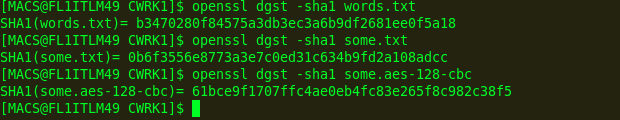
In CFB mode, the encryption of a message is done by XOR the output of the key and IV of which it results to having more blocks being affected after the change of byte when decrypting the message.

In OFB mode, the key is generated by the system, so even after editing the byte, only a single byte will be corrupted.

**Task 5**

1. Looking at the checksum result, for the first file “word.txt” the downloaded file has not been tampered because their checksums are identical. For the second file “some.txt” the downloaded file was not tampered because their checksums are identical. For the third file, “some.aes-128-cbc”, thee downloaded has been tampered because the checksum given in the scenario and the one I downloaded are not the same.
2. Checksum covers the concept of integrity control which means checking if the file was changed or not.

**Figure 7.1 Checksum**



1. Yes because after downloading a certain fie, you can compute the checksum of the installed file to compare with the checksum provided on the downloading page. By doing this, it guarantees that the integrity of the downloaded file.

# Bibliography

Anon., 2012. *The process of encryption and decryption.* [Online]   
Available at: www.daiblotin.com the process of encryption and decryption  
[Accessed 22 10 2015].

Corporation, L.-O. T., 2015. *M6M.* [Online]   
Available at: http://goplextor.com/asia/index.php/sata3-ssd/msata-ssd/m6m  
[Accessed 16 10 2015].

ITBusinessEdge, 2014. *ITBusinessEdge.* [Online]   
Available at: http://www.webopedia.com/TERM/A/AES.html  
[Accessed 20 10 2015].

James, 2006. *Symmetric Cryptography,* s.l.: James.

Konheim, n.d. Computer Security and Cryptography. In: *Computer Security and Cryptography.* s.l.:s.n., p. 301.

Mihir, B. & Rogaway , P., 2005. Introduction to modern cryptography. In: *Introduction.* s.l.:Pearson, p. 10.

Springer, 2009. *The Data Encryption Standard(DES) and Alternatives.* s.l.:s.n.

Stallings, W., n.d. *Cryptography and Network Security: principles and practices.* s.l.:s.n.