Ransomware Attack using AES Encryption on ECB, CBC and CFB Mode

Feillyan Alfreda Antariksa, Is Mardianto

Informatic Engineering, Trisakti University
Jakarta, Indonesia
feillyan064001400012@std.trisakti.ac.id
mardianto@trisakti.ac.id

Abstract

With the help of internet, users are faster getting data that they needed. It's possible that villain insert an evil program (malware) without user knowing it. One of the malwares that spread like a plague right now is ransomware. The infected computer system will encrypt all files on the computer and blackmail the users to pay some money if you want to access back your files. For this experiment it's using 2 approach, first is using online attack and second is offline attack. Ransomware in this experiment is using AES 256 for encrypting the files and using ECB, CBC and CFB mode for comparing time. As the result ECB is 39.5% faster than CBC and 7,17% faster than CFB. For CFB is 34,83% faster than CBC.

Keywords: *Ransomware, Malware, AES 256, ECB, CBC, CFB*

1. Introduction

One of malware function is it can remotely control others computer to send data without user knowing it. It can use to encrypt user data an extorting for money for example [1]. In 2005 – 2006 was the first ransomware attack appear when the culprit tries to blackmail the victim with US$300. Just in 10 year on 2016, Trend Micro found 247 newly ransomware while a year ago on 2015 only 29 ransomwares can be found. Its increased 752% just in one year [2]. There are 2 types of ransomware, first one is locker ransomware that locked your computer from the user. Its objective is to limit your resources on your computer so the user only can use keyboard at numerical type so user can't do anything except for paying them via bitcoin. Second one is the Crypto ransomware, its encrypt all the user files so the files can't be opened anymore. When it involved precious or sensitive data, user will do anything to get that back including paying the culprit to get the decrypt key. Even more, the ransomware gave users the warning with the "time left" or "don't turn off the internet otherwise key is disabled" something similar like those [3].

2. Reseach Methods

2.1 Online Attack

When the downloadable file is executed, the program will generate key to encrypt all the files at victim hard drive. The encrypted file cannot be open or access before the victim paying some money in cryptocurrency like Bitcoin, Redcoin, Ethereum, Litecoin etc. After the payment done, then the key to decrypt will be given as shown on **Figure 1.**

2.2 Offline Attack

In offline attack, malware is inserted in flash drive. When the malware in the flash drive executed, file automatically open and the key for decrypting is created in the flash drive. File in computer will be encrypted in a specified time as shown on **Figure 2.**

p-ISSN: 1979-5661
e-ISSN: 2622-321X

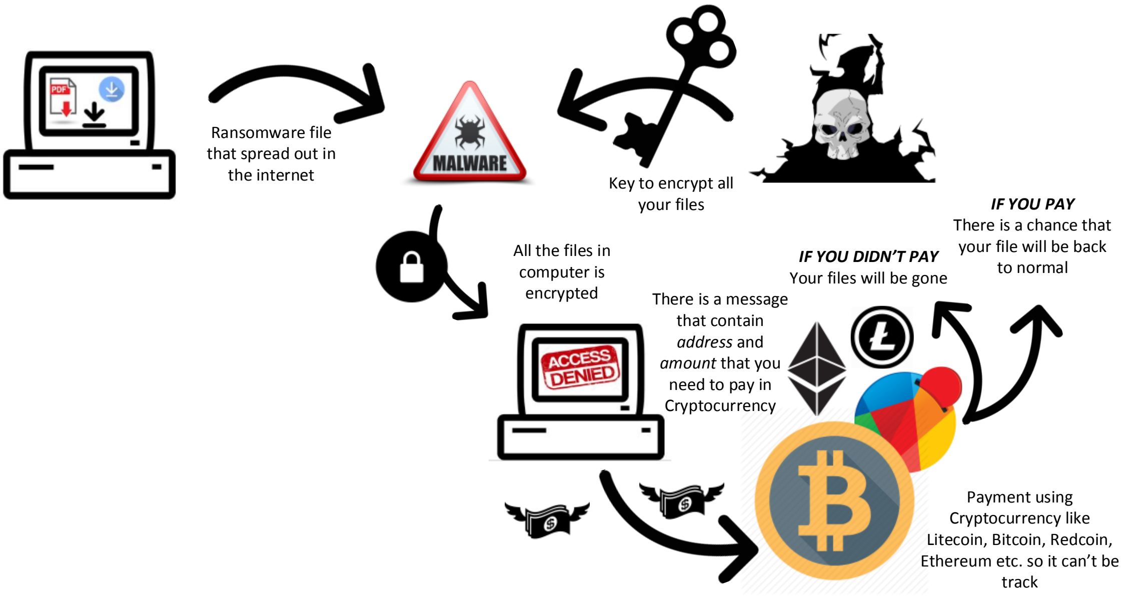

Ransomware file that spread out in the internet
MALWARE
Key to encrypt all your files
All the files in computer is encrypted
ACCESS DENIED
There is a message that contain *address* and *amount* that you need to pay in Cryptocurrency
IF YOU DIDN'T PAY
Your files will be gone
IF YOU PAY
There is a chance that your file will be back to normal
Payment using Cryptocurrency like Litecoin, Bitcoin, Redcoin, Ethereum etc. so it can't be track

Figure 1. Online Attack Ransomware Scheme

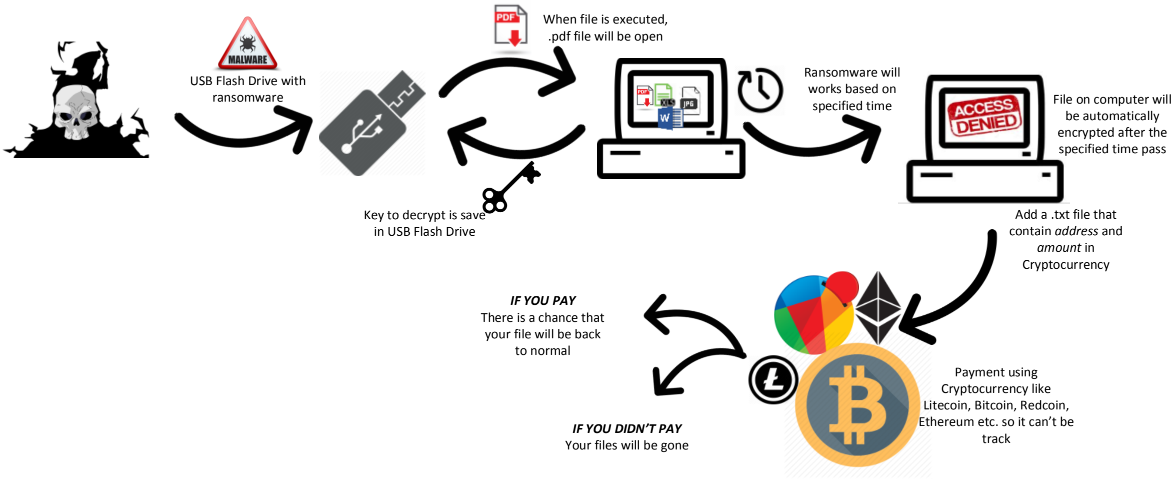

MALWARE
USB Flash Drive with ransomware
When file is executed, .pdf file will be open
Key to decrypt is save in USB Flash Drive
Ransomware will works based on specified time
ACCESS DENIED
File on computer will be automatically encrypted after the specified time pass
Add a .txt file that contain *address* and *amount* in Cryptocurrency
IF YOU PAY
There is a chance that your file will be back to normal
IF YOU DIDN'T PAY
Your files will be gone
Payment using Cryptocurrency like Litecoin, Bitcoin, Redcoin, Ethereum etc. so it can't be track

Figure 2. Offline Attack Ransomware Scheme

2.3 AES Mode

Developed by Joan Daemen and Vincent Rijmen, Advanced Encrypted Standard (AES) use a 128 bits of data block and 128, 192 or 256 bits of cipher key.[4 FIPS]. Encryption process is shown on **Figure 3.**

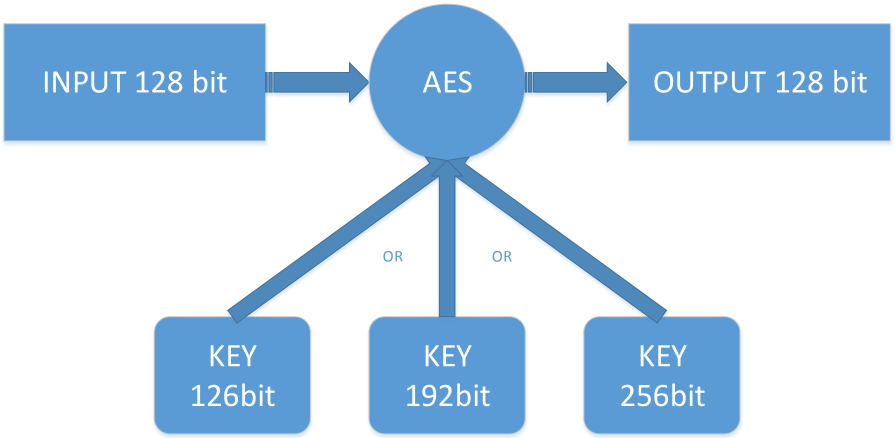


Figure 3. AES Process

AES algorithm work by repeating the same step in a certain rounds (10 round for 128 bit, 12 round for 192 bit, 14 round on 256 bit)[5 IJETT]. In this paper, AES that going to be use is AES 256 bits.

The first mode that will be used is AES ECB (Electronic Codebook). It's most simple encryption from the other mode because each block is encrypted using the same key shown on **Figure 4.** The formula used is as follow [6]:

Encryption : $C_j = CIPH_K(P_j)$ *for j = 1 … n.*

Decryption : $P_1 = CIPH^{-1}_K(C_j)$ *for j = 1 … n.*

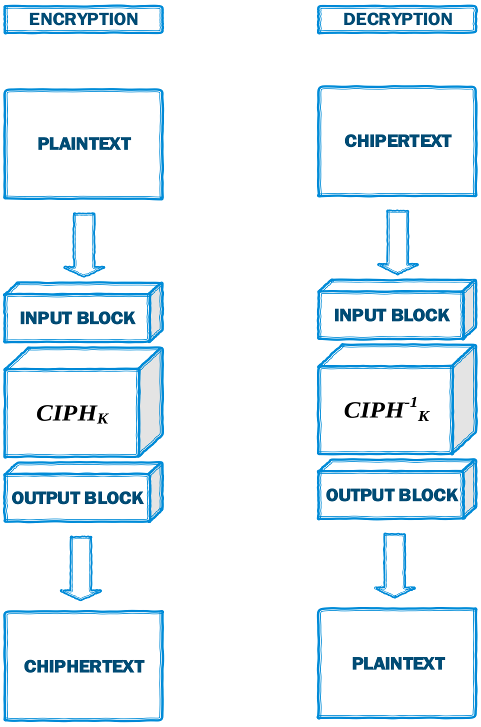


Figure 4. AES ECB mode

Second mode is the CBC (Cipher Block Chaining). On CBC block plaintext is combining with the previous block ciphertext. For the first block plaintext, is combining with Initialization Vector (IV) shown on **Figure 5.** The formula used is as follows [6]:

Encryption : $C_1 = CIPH_K(P_1 \oplus IV);$

$C_j = CIPH_K(P_j \oplus C_{j-1})$ *for j = 2 … n.*

Decryption : $P_1 = CIPH^{-1}{}_K(C_1) \oplus IV);$

$P_1 = CIPH^{-1}{}_K(C_j) \oplus Cj\text{-}1);$ *for j = 2 … n.*

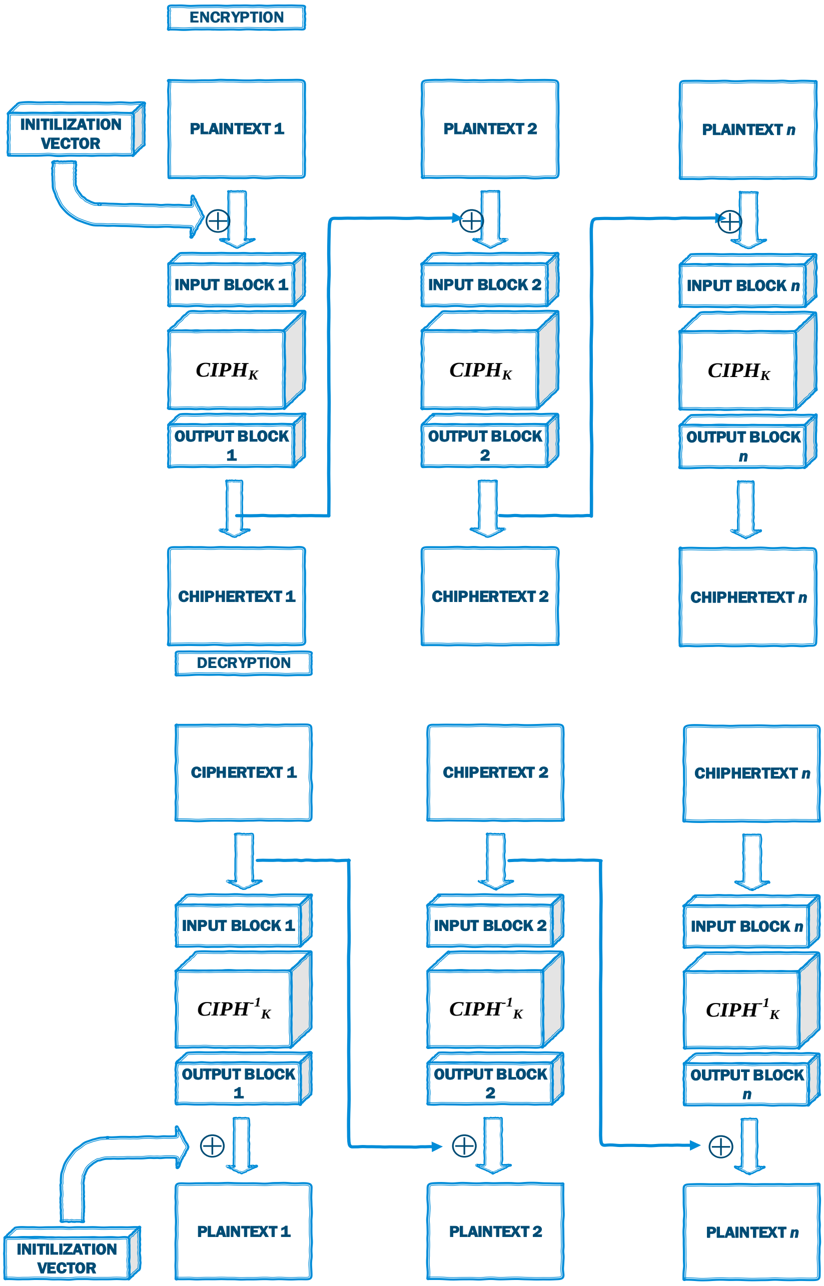


Figure 5. AES CBC

p-ISSN: 1979-5661
e-ISSN: 2622-321X

On CFB (Cipher Feedback Mode), IV is used to get an output block. Then the plaintext block is XOR with the output block but only using s most significant bit from the output block where s is an integer parameter. The remaining bit will be discarded shown on **Figure 6.** The formula used is as follows [6]:

Encryption : $I_1 = IV;$
$I_j = LSBb\text{-}s(Ij\text{-}1) \mid C^{\#}_{j-1}$ *for j = 2 … n.*
$O_j = CIPHK(I_j)$ *for j = 1, 2 … n.*
$C^{\#}_j = P^{\#}_j \oplus MSB_s(O_j)$ *for j = 1, 2 … n.*

Decryption : $I_1 = IV;$
$I_j = LSB_{b\text{-}s}(I_{j\text{-}1}) \mid C^{\#}_{j-1}$ *for j = 2 … n.*
$O_j = CIPH_K(I_j)$ *for j = 1, 2 … n.*
$P^{\#}_j = C^{\#}_j \oplus MSB_s(O_j)$ *for j = 1, 2 … n.*

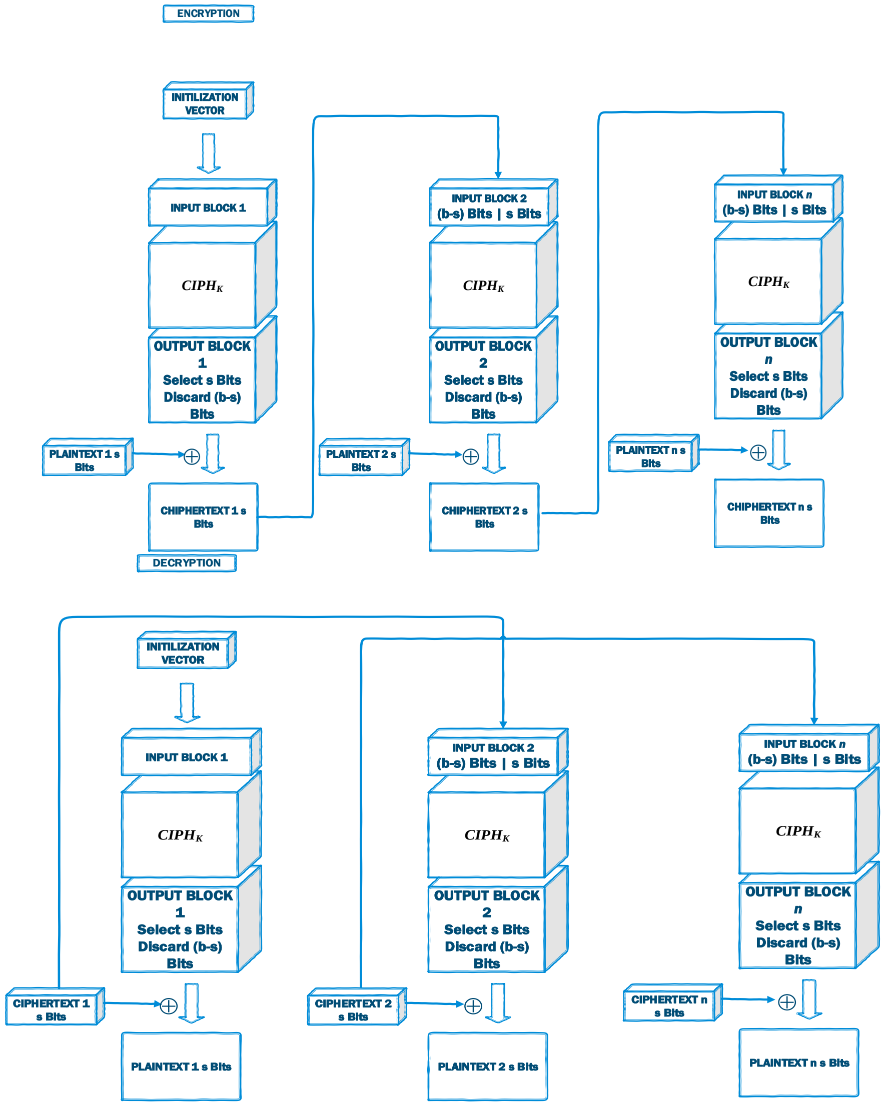

ENCRYPTION
INITILIZATION VECTOR
INPUT BLOCK 1
CIPHK
OUTPUT BLOCK 1 Select s Bits Discard (b-s) Bits
PLAINTEXT 1 s Bits
CHIPHERTEXT 1 s Bits
INPUT BLOCK 2 (b-s) Bits | s Bits
CIPHK
OUTPUT BLOCK 2 Select s Bits Discard (b-s) Bits
PLAINTEXT 2 s Bits
CHIPHERTEXT 2 s Bits
INPUT BLOCK n (b-s) Bits | s Bits
CIPHK
OUTPUT BLOCK n Select s Bits Discard (b-s) Bits
PLAINTEXT n s Bits
CHIPHERTEXT n s Bits
DECRYPTION
INITILIZATION VECTOR
INPUT BLOCK 1
CIPHK
OUTPUT BLOCK 1 Select s Bits Discard (b-s) Bits
CIPHERTEXT 1 s Bits
PLAINTEXT 1 s Bits
INPUT BLOCK 2 (b-s) Bits | s Bits
CIPHK
OUTPUT BLOCK 2 Select s Bits Discard (b-s) Bits
CIPHERTEXT 2 s Bits
PLAINTEXT 2 s Bits
INPUT BLOCK n (b-s) Bits | s Bits
CIPHK
OUTPUT BLOCK n Select s Bits Discard (b-s) Bits
CIPHERTEXT n s Bits
PLAINTEXT n s Bits

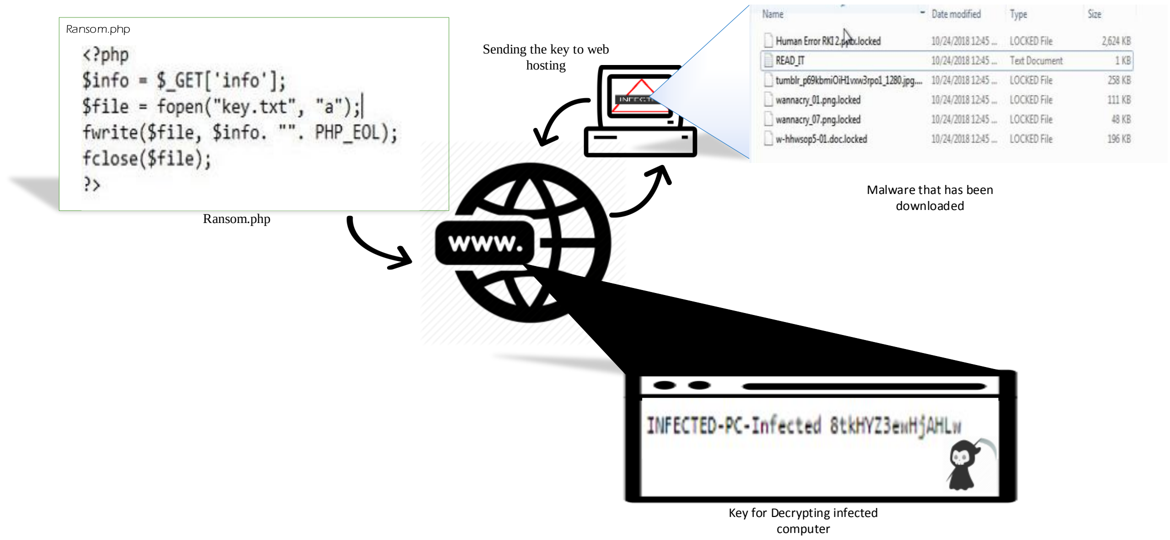
Figure 6. AES CFB

p-ISSN: 1979-5661
e-ISSN: 2622-321X

3. Result and Discussion

3.1. Online Mode

This web hosting will be used to receiving the encryption password from the victim using the php script in **Figure 7**.



Ransom.php

```
<?php
$info = $_GET['info'];
$file = fopen("key.txt", "a");
fwrite($file, $info. "". PHP_EOL);
fclose($file);
?>
```

Name	Date modified	Type	Size
Human Error RKI 2.pptx.locked	10/24/2018 12:45 ...	LOCKED File	2,624 KB
READ_IT	10/24/2018 12:45 ...	Text Document	1 KB
tumblr_p69kbmiOiH1vxw3rpo1_1280.jpg....	10/24/2018 12:45 ...	LOCKED File	258 KB
wannacry_01.png.locked	10/24/2018 12:45 ...	LOCKED File	111 KB
wannacry_07.png.locked	10/24/2018 12:45 ...	LOCKED File	48 KB
w-hhwsop5-01.doc.locked	10/24/2018 12:45 ...	LOCKED File	196 KB

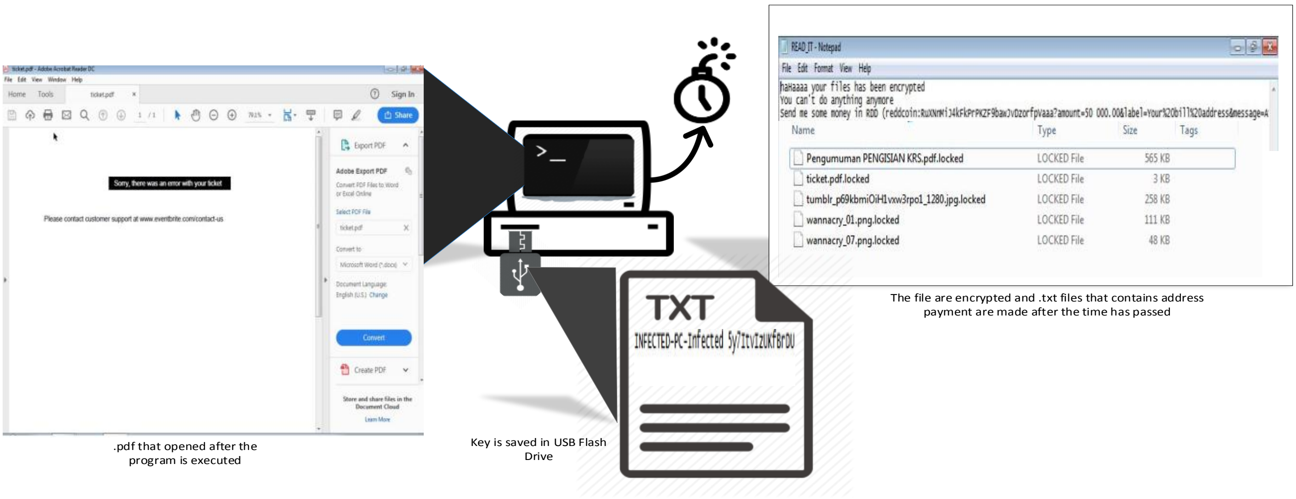
```
INFECTED-PC-Infected 8tkHYZ3ewHjAHLw
```

Ransom.php
Sending the key to web hosting
www.
Malware that has been downloaded
Key for Decrypting infected computer

Figure 7. Online Mode

3.2. Offline Mode

When the program is executed, file will be open by itself and opening its own contain. After file is opened, files on computer are encrypted in the time that has determine before. Then there will be txt file on the desktop that contain information that all your files are encrypted and your payment using address from cryptocurrency. The encryption key is saved in the Flash Drive in txt in **Figure 8.**



Sorry, there was an error with your ticket

Please contact customer support at www.eventbrite.com/contact-us

READ_IT - Notepad

```
haHaaaa your files has been encrypted
You can't do anything anymore
Send me some money in RDD (reddcoin:RuXNmMiJ4kFkPrPKZF9bawJvDzorfpVaaa?amount=50 000.00&label=Your%20bill%20address&message=A
```

Name	Type	Size	Tags
Pengumuman PENGISIAN KRS.pdf.locked	LOCKED File	565 KB	
ticket.pdf.locked	LOCKED File	3 KB	
tumblr_p69kbmiOiH1vxw3rpo1_1280.jpg.locked	LOCKED File	258 KB	
wannacry_01.png.locked	LOCKED File	111 KB	
wannacry_07.png.locked	LOCKED File	48 KB	

```
INFECTED-PC-Infected 5y7ItvIzUKfBrDU
```

ticket.pdf - Adobe Acrobat Reader DC
File Edit View Window Help
Home Tools ticket.pdf
Sign In
Share
Export PDF
Adobe Export PDF
Convert
Create PDF
.pdf that opened after the program is executed
Key is saved in USB Flash Drive
TXT
The file are encrypted and .txt files that contains address payment are made after the time has passed

Figure 8. Offline Mode

p-ISSN: 1979-5661
e-ISSN: 2622-321X

3.3. Comparison Time

In **Table 1.** shows the result of test using AES in ECB, CBC and CFB mode for encryption. Time measurement is on millisecond.

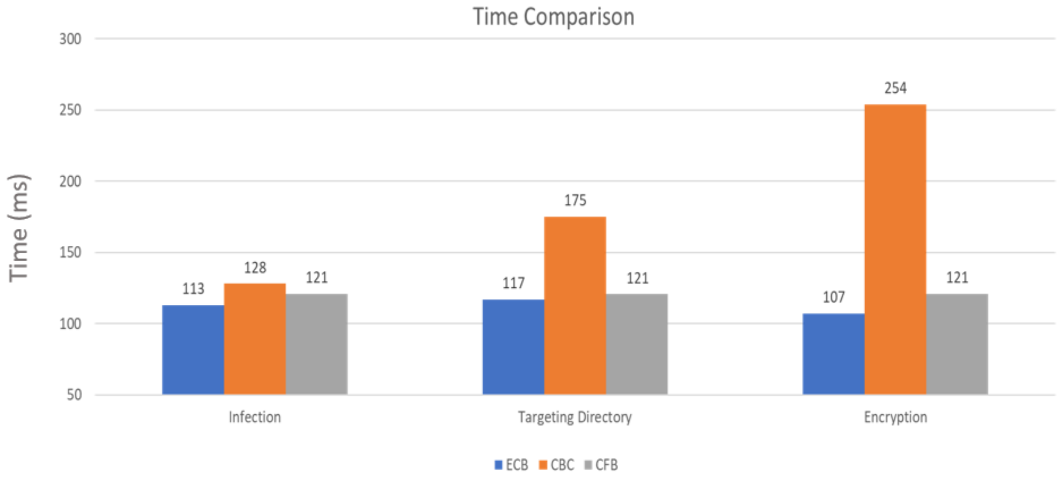


Table 1. Time Comparison

On ECB each block is encrypted using the same key. Meanwhile on CBC block plaintext is combining with the previous block ciphertext. The first block on CBC in combining with IV. On the other hand, CFB is using IV to get an output block. Then the plaintext block is XOR with the output block but only using s most significant bit from the output block where s is an integer parameter. The remaining bit will be discarded. On infection, ECB is 15ms more faster than CBC and 8ms faster than CFB. On targeting directory, ECB is 58ms more faster than CBC and 4ms faster than CFB. For encryption ECB is way faster with 47ms differences with CBC and 14ms differences with CFB. Therefore, the ECB is faster than CBC and CBC are faster than CFB.

4. Conclusion

ECB mode is faster than both CBC and CFB because ECB is resulting the same block chipper from the encrypted block. Because of that, if there is a repetitive text it will be ease to recognize. Meanwhile in CBC and CFB both are using Initialization Vector (IV) for XOR operator. With this the encryption result is always unrecognize or jumble even if that massage a repetitive one.

References

[1] ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT “Malicious Software (Malware): A Security Threat to the Internet Economy” Ministerial Background Report DSTI/ICCP/REG(2007)5/FINAL.

[2] TrendLabs The Global Technical Support & R&D Center of TREND MICRO; “Ransomware: Past, Present, and Future” TREND MICRO 2017.

[3] Savage Kevin, Coogan Peter, Lau Hon; “The evolution of ransomware” Symantec version 1.0 August 6, 2015.

[4] Federal Information Processing Standard (FIPS). “*ADVANCED ENCRPTION STANDARD (AES)”*. Publication 197 November 26, 2001.

[5] Gupta Monika, Mahto Swapnil, Patel Ambresh. “*Implementation of 128, 192 & 256 bits Advanced Encryption Standard on Reconfigurable Logic*”. International Journal of Engineering Trends and Technology (IJETTI) vol 50 num 6 August 2017

[6] Dworkin Morris. “Recommendation for Block Cipher Modes of Operation”. National Institute of Standards and technology (NIST) Special Publication 800-38A 2001 Edition.