SYMMETRIC CIPHER IMPLEMENTATION AND ANALYSIS REPORT

Keamanan Informasi Jaringan - A (2022)

Lecturer :

Dr. Baskoro Adi P., S.Kom., M.Kom.

Group Members :

Mohammad Faderik I H	05111940000023
Allam Taju Sarof	05111940000053
Achmad Akbar Irwanda	05111940000138
Iwan Dwi Prakoso	05111940000229

INFORMATICS ENGINEERING DEPARTMENT
FACULTY OF INTELLIGENT ELECTRICAL AND INFORMATION TECHNOLOGY
SEPULUH NOPEMBER INSTITUTE OF TECHNOLOGY

1. **Security**

   In terms of security, AES is the most secure encryption method and has become the de-facto encryption standard in the world today. Otherwise, DES which is an older encryption method compared to AES has a lower level of security. DES has known several weak points. DES encryption can be break by the following methods:

   - Brute-force attack

     This method is the most practical method to solve DES. This is because the key length of the DES method is short. DES requires a key of 64 bits long and which effectively affects the encryption process is 56 bits. This number allows for brute force attacks and this is the main reason DES has lost its credibility.
   - Other attacks:

     There are several other methods besides brute-force attack, but some of these methods are less practical, for instance:
     - linear cryptanalysis
     - differential cryptanalysis
     - davies attack.

   There is another encryption method called stream cipher, that is RC4. RC4 uses a relatively simpler algorithm than AES. In terms of security, RC4 is no more secure than AES.

2. **Features**

   Because RC4 is a stream cipher method, RC4 can be used to encrypt data bit by bit. RC4 is often used to encrypt data in the form of streams such as TSL/SSL and secure shell. Otherwise, AES and DES as block cipher methods can only be used to encrypt a block of data at a time. AES encrypts 16 bytes block data while DES encrypts 8 bytes block data.

3. **Cipher Text Result**

   There are differences in ciphertext results between block ciphers (AES, DES) and stream ciphers (RC4). When executed to encrypt data (.txt) is empty, the block cipher algorithm will still generate encryption data along the block size, namely 16 bytes (AES) and 8 bytes (DES). While the stream cipher encryption results on an empty file is an empty file as well.

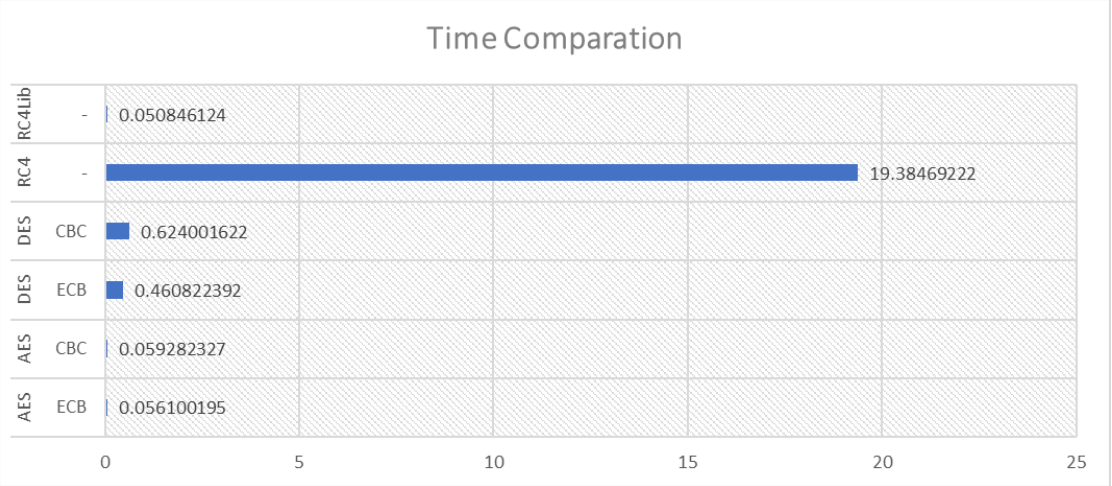
   Similar to the results of encryption on empty files, the results of encryption on files that have a small amount of data, in the experiment carried out with files that only have one character in it, block ciphers still produce encryption results along the block size while stream ciphers produce encryption results as long as the plaintext data .

4. Running Time

Every encryption method has different encryption time. The first try is using 23.9MB text file and each method is executed with 10 iterations with the following results:

Sumary			
Metode	Mode	AVG Time	Std Deviation Time
AES	ECB	0.056100195	0.011628264
AES	CBC	0.059282327	0.001049998
DES	ECB	0.460822392	0.044448078
DES	CBC	0.624001622	0.428596718
RC4	-	19.38469222	0.993373267
RC4Lib	-	0.050846124	0.004045253

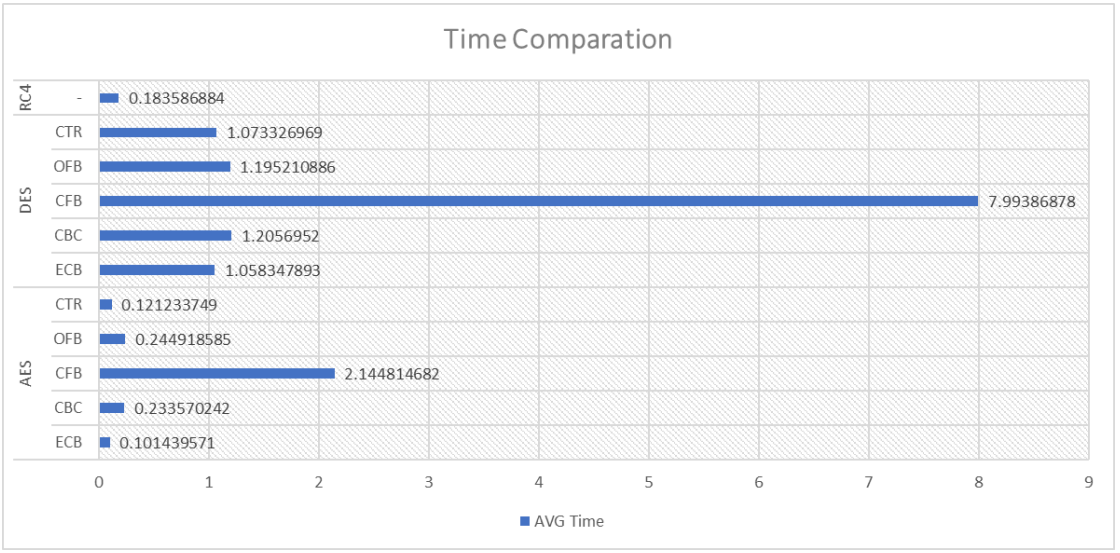
As for RC4 method, we are using two implementations, the first one is with our own implementation (RC4) and the second one we are using library (RC4Lib). From both implementations, it can be concluded that using the library is significantly faster than self implementation. RC4Lib encryption and AES have a time that is not much different while DES is under both.The following are the results in graphical form:

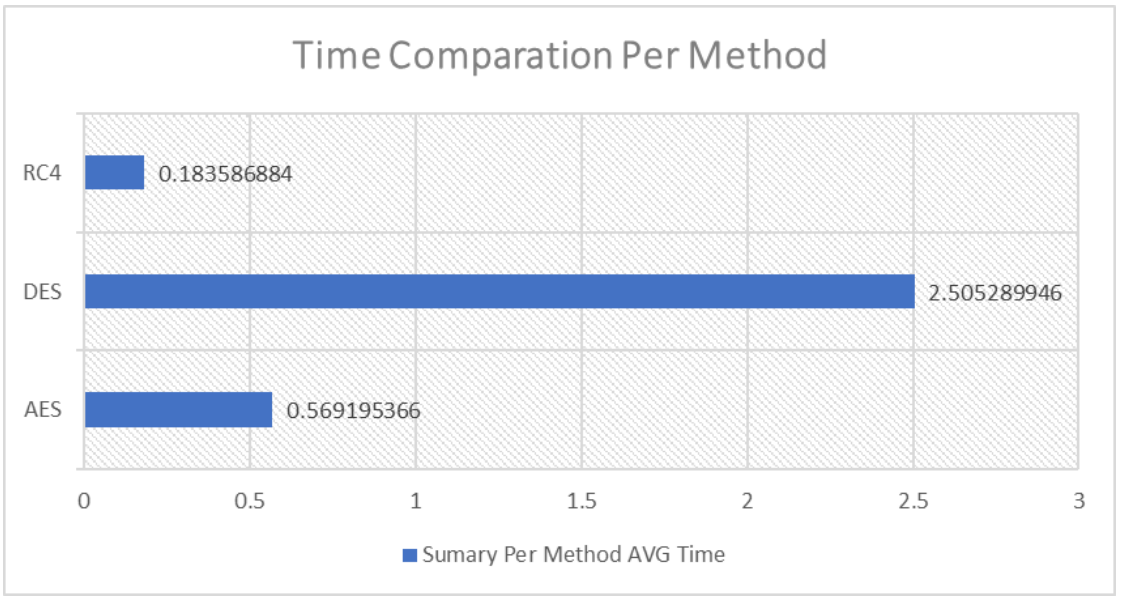


In the second experiment, encryption was performed on the executable file (.exe) with a size of 92.3 MB. In this experiment, 5 iterations were carried out but experimented with more modes on AES and DES. In this experiment we can only use RC4 implementation from the library because our own implementation is not supported for encrypting executable files. The results of the second experiment are as follows:

Sumary					
Metode	Mode	AVG Time	Std Deviation Time	AVG Time	AVG StdDev
AES	ECB	0.10143957	0.003654463	0.569195366	0.011880219
	CBC	0.23357024	0.01059195		
	CFB	2.14481468	0.033621771		
	OFB	0.24491859	0.009607846		
	CTR	0.12123375	0.001925064		
DES	ECB	1.05834789	0.018578108	2.505289946	0.030437001
	CBC	1.2056952	0.022859799		
	CFB	7.99386878	0.065798265		
	OFB	1.19521089	0.031804151		
	CTR	1.07332697	0.01314468		
RC4	-	0.18358688	0.005607027	0.183586884	0.005607027

In the results of this second experiment. On average, RC4 outperforms AES. However, in AES mode ECB and CTR are able to be faster than RC4. This is because in the AES ECB and CTR methods the encryption process can be carried out in parallel so that it runs faster. The DES method in this experiment remains significantly slower than the other two methods. Here are the results of the second experiment in graphical form:




Time Comparation Per Method
RC4
0.183586884
DES
2.505289946
AES
0.569195366
0
0.5
1
1.5
2
2.5
3
Sumary Per Method AVG Time