ASSIGNMENT REPORT
KEAMANAN INFORMASI DAN JARINGAN C

Analyzing Different Symmetric Cipher Method (AES, RC4, DES)

Group 9:

Reyhan Naufal Rahman - 05111940000171
Muhammad Akmal Joedhiawan - 05111940000125
Cliffton Delias Perangin Angin - 05111940000181
Ega Prabu Pamungkas - 05111940000014

Dr. Baskoro Adi P., S.Kom.,M.Kom.
KEAMANAN INFORMASI DAN JARINGAN KELAS C
INSTITUT TEKNOLOGI SEPULUH NOPEMBER

ANALYZE DIFFERENT SYMMETRIC CIPHER METHOD

A. PROGRAM AND DATA

Our group uses **Python** for building our program. The program consists of server and client. The server is using the **"rpyc"** module using **OneShotServer** where it will receive one connection from the client. The client itself will connect to the server and send triggers and data files for either encryption or decryption. The result of encryption or decryption will be saved on a file with the same name and extension.

Our group will test the program using an **1,5 MB TEXT** file filled with words and sentences, and **run it 5 times for each method (encryption and decryption).**

Full documentation of our group symmetric cipher method implementation and data used for encryption can be access on:

- https://github.com/reyhannaufal/encrypt-decrypt

B. ADVANCED ENCRYPTION STANDARD (AES)

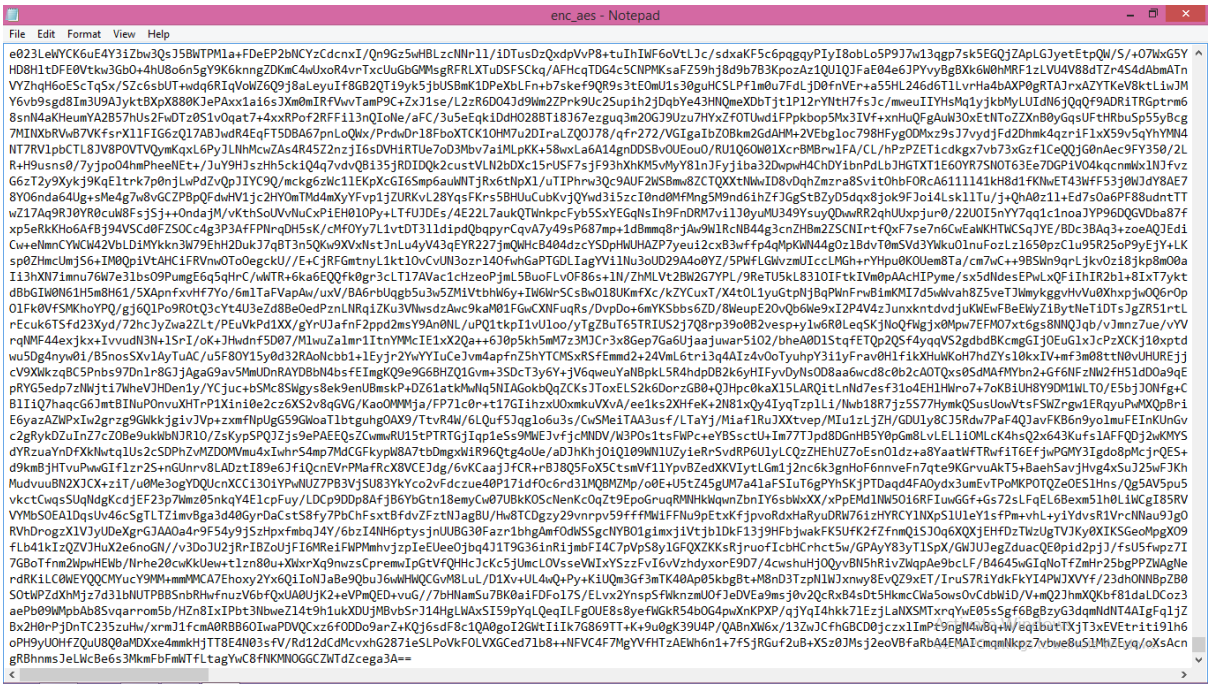
a. Features
   - Using AES with 256 bit long key and using Cipher-Feedback Mode

b. Running Time (in milisecond)

Test Number	Encryption Time (ms)	Decryption Time (ms)
1	466,7	722,1
2	517,0	657,6
3	475,2	541,3
4	591,5	669,5
5	479,8	551,2

From the result above we can calculate the mean which is:
Encryption Time Mean = 506,4 ms (0,5064 seconds)
Decryption Time Mean = 628,34 ms (0,62834 seconds)

c. Resulting Ciphertext
Here is one example of the resulting cipher text (cutted).
   - Cipher Text



The cipher text consists of the alphabet, numeric, and symbols. It also almost doubles the size of the original text with a 2,8 MB TEXT file.

d. Security
Because it uses Cipher-Feedback mode the encryption that has been made will be secure mostly because the attacker will need to find the key and each block encrypts each other.

C. RC4

a. Features
- Generates a pseudo-random stream of bits (a key-stream). The stream generated by:
    1. A permutation of all 256 possible bytes (denoted "S" below).
    2. Two 8-bit index-pointers (denoted "i" and "j").
- The permutation is initialized with a variable length key, typically between 40 and 256 bits, using the key-scheduling algorithm (KSA). Then the stream of bits is generated by a pseudo-random generation algorithm.
- The stream will be used for encryption by combining it with the plaintext using bit-wise exclusive-or.

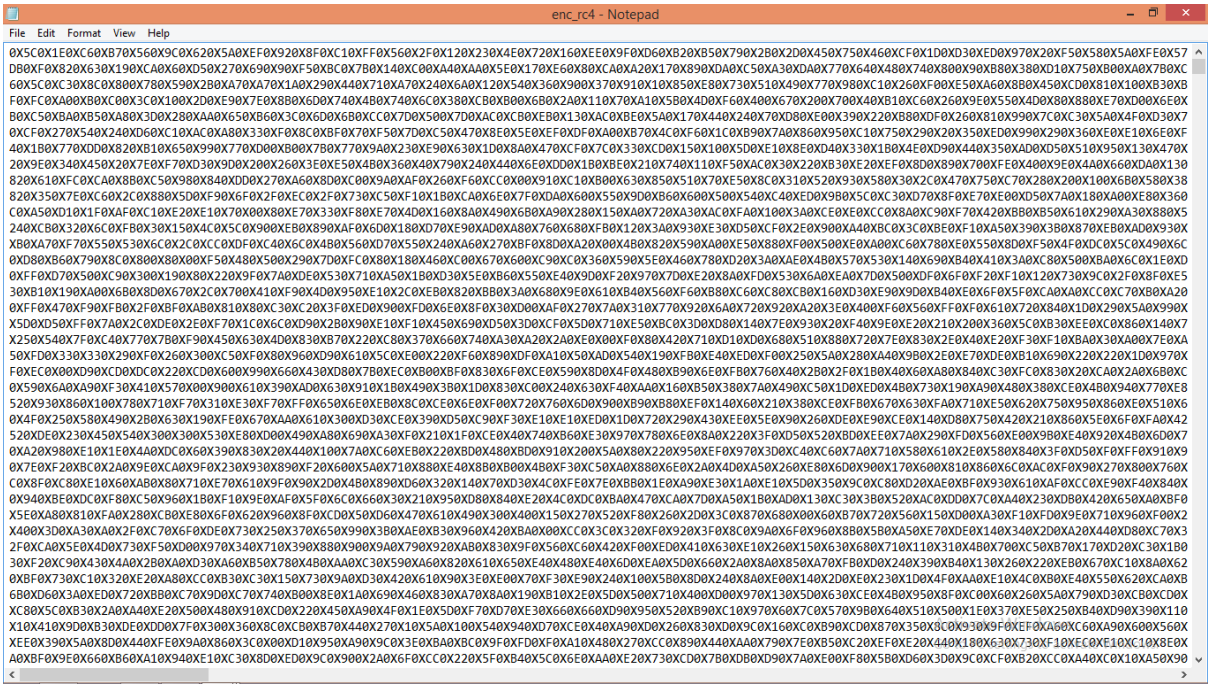
b. Running Time

Test Number	Encryption Time (ms)	Decryption Time (ms)
1	466,7	722,1

2	517,0	657,6
3	475,2	541,3
4	591,5	669,5
5	479,8	551,2

From the result above we can calculate the mean which is:
Encryption Time Mean = 12490,28 ms (12,49028 seconds)
Decryption Time Mean = 7447,06 ms (7,44706 seconds)

c. Resulting Ciphertext
Here is one example of the resulting cipher text (cutted).
- Cipher Text



The size of the ciphertext is 4 times the original size which isi 6,2 MB TEXT file.

d. Security
The DES method uses a short key size therefore it is mostly insecure.

D. DATA ENCRYPTION STANDARD (DES)

a. Features
- For DES our group use Cipher-Block Chaining Mode

b. Running Time

Test Number	Encryption Time (ms)	Decryption Time (ms)
1	466,7	722,1

2	517,0	657,6
3	475,2	541,3
4	591,5	669,5
5	479,8	551,2

From the result above we can calculate the mean which is:
Encryption Time Mean = 131,66 ms (0,13166 seconds)
Decryption Time Mean = 182,88 ms (0,18288 seconds)

c. Resulting Ciphertext
Here is one example of the resulting cipher text (cutted).
- Cipher Text

The resulting ciphertext consists of the alphabet and numeric. The size of the ciphertext doubles the size of the original plain text which is a 3,1 MB TEXT file.

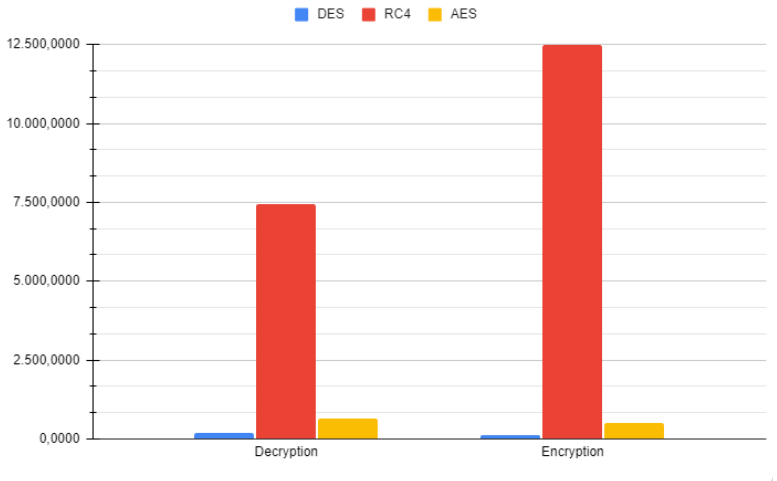
d. Security
The RC4 uses stream generation keys to encrypt its data and has relatively long keys. But, there is a way by using a middle-man attack to retrieve the key generated and because of that it is now mostly insecure.

E. BETWEEN THE THREE

Based on our report for each symmetric cipher method, there are a few points that can be concluded between the three methods.

1. It can be seen on the diagram below that DES is the fastest in encryption and decryption method, while RC4 is the slowest one. As seen on the diagram

below which maps the mean of each encryption and decryption method in milliseconds.



2. It can also be seen that for decryption both AES and DES are slower compared to its encryption, but RC4 has faster decryption compared to its encryption.
3. The **file size** for the cipher text, RC4 is the biggest with 6,2 MB followed by DES 3,2 MB and AES 2,8 MB TEXT file.
4. The difference in the ciphertext where AES and DES both contain alphabet and numeric, even though in AES it also contains symbols, whereas RC4 only contains uppercase alphabet and numeric.

F. CONCLUSION

Based on our report it is known that DES is the fastest in encrypt and also decrypt the data. But, it is not the most secure method to use for higher security. Between the three, the most recommended and standard use of the symmetric cipher method is AES 256 because it uses a relatively long key and the resulting ciphertext creates the smallest size between the three.