

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
Cliffon 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:

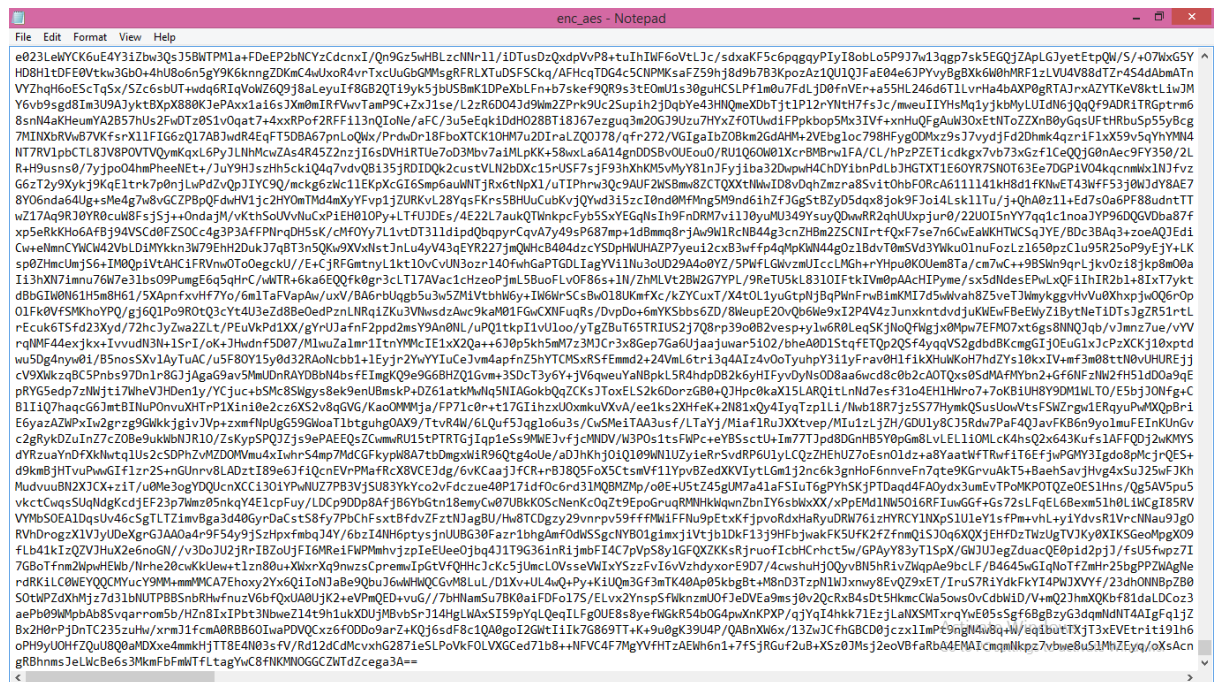
Encryption Time Mean = 506,4 ms (0,5064 seconds)

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 of 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 is 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

```

enc_des - Notepad
7df30772a3798e9dc965b484d545d2068346222ccc46715b3c7a07688b0e400b5d0bc93ea338d3a419ee381f57795f91dd1b6fc3eb2c132d4566227c10f06a3d4fa7d3c23608662e828256de090103fe11481
d43a5f86978a97b12db6838d7ec3c395d245be5ee18ab895e2052496ed79759ec10894618215badd40461fbc24209a4762fb91833ec15215b7bef77b408e826d2a50b16101d82a369089933a42c507795b4cf4
10c0cb2bb11d0622e06989ec8af60eb9850ac14958e5816808cee4a08ba501ee239ed05f8dc6765f2494df93c6000c4fd563b9f42071251b268a147815cf8f831a8d67e78481678d780b78ee9b1c1ab8b06b99c
6c918b480cee9fd01cdc053aafba0a28ea7b5c21025221c399707f3376117c1907be2e46739c9ea5158d0f3866733dd08665f2846043fb6555f797963df8a2a627d552e82c905a9c8f4c58202850342f5a6665
26f1d226eeb449fd80e566f3f8d32ce7e880b2212faa40bdf5ebced8d090e218bee162b2b0bf7f3f0bd2e0ed97e1e25fa1bf1704d83377d557f16c0b1b9d053b916475ad1778310a709c8f76767d7f0d115
10da8d8e1488737c42780979bb20b7e9eb43d7dab25153cccf1cee22cc76e679989242c00a07e7766b08948ea34627c67516f3c242421e66dee2bd02eca48c4896d33816cc18d1c718f11fa99a5af819cb342311f
0443e43b59c8ef40fb3ee24794dfafba282b15ab03c94e7509b45ebf9d4805426e978cf2de55d63952921e4773de6f04079de9aba0a7d3d0dc757cb1701eb1485002f9c83b5fcd8b34dbd2f4cf6b2c07e93388
a8608caab94de6241257b74316ac3e33002388e84f1207b6368dd16542caab65afcaecf9674c77fc59bd27303399e5b8a69fea7d7eb8f21788ef72a285e1176423c348491fa7b3f1601b51912c30f82532ba09
e87fa8460432dac77e76d5cec1b32c6508c9aa574748f20f32caa3767a2c411eb1f8372ee8b509fb011ad75c430801949b68f3aa0907bad866cc453a89657de421bead2fc38dc4a3b3f8f8b9e254f81f0d784e4
78f7e02ab5051f0cf8a7446eb0859ca32eeb35706083420ba51be2af3cd5fe896afbcc35f8d86595a07ea93197f43eaa1ea025f9b9d9b6a8ea30f243b7f4dcdf3fb39d259f50bc6ded1d7c22cd72ba4296f72210
c84560197be5e960446e3d35c03724ac04c9a0310a1dfaad7919045c151f3b70c9d9f521da62c56a5ee6cd2821ca62e7f9c27d4fa7e2fd90e2b5f69999166099cd51940bc23e786a5040e65806c926bb
21f5c9c431ba549f8187d01e3c946721672653adf2810735c897319835384d487934709ae9c223ffff7280ee857d481ae3ef257939c3d4df641946182da66a1cb55153236091033c4574ba771c08377df4f2
013b4a3ab931455867c1d17e8f3f0e9cd0284a8dc4fbbbc19343d0aac99be5c86f8d34c45634d45326a36493240e4f291b9a10a3c2da2cae1f72862f8ca7634646131a938c7e7ce71d0fa9ee53c74da5e10
684dd9ab3f2e9097ea53ff92566495549090bc4df4b0e0db72c184c5e44dde7f1bee88a321dc15b23a6188f69b7a4c576f5d9a5e14628a299f39df0484cf69cad59c2ceac7f0637b6b50ed16647478d94c86
8d5e103889f9dc576410814a80cd98e1f1d2ef6599817a3674fb8e85a6543f48e7be393da647c2b6d4fe2d097574b2892c9f01c755441436e5d4f500910650fec098c7ad63490f5388d9367408e9f65afdd
727ef3ac8ea93c79e02c5884dc4283bdaf56dfae0f18ee8ec7165273bd53a52e16aab9bda7667467ec43ec24431d49408893b7e106becf06376a85deebf0f631be009a2e032079526cfe084992859098f73fcd70
59fcdac6fb71cd34858a7b5eb52a71c195246a5899a3822c2f367bf3015c0ecbb4125ad84f5496876e30fd88d552f29289a39f55ced548d0b25a3917a2b3c3684bb266f01a99b709c7e4f8edbb9bd07
de9a35f2c35b91f395306becf58c1c584cdddf3c1e012f299e70802ac38b40e96ded45462a9f5d57cb74a128540fd9d4a50c22dd37b288d1769476c4de37059e2762b7cb6f5511137c8ef46bcfdb4f88398
a2531fd93849c405d4971230c5706e5804d3a6d90cf222455eaa1f4418234146d5a54a322f21a2de78c562aa77f85d073431d097aad8b8e62fadac1b1afeeb554de60a84db2b4fb7b17057f839cf432173cc
45511ddb5c1f08c790c206b6ad98e6078d32c39a49b0b53c0f2c7575c0d54377953ab4df573e921bb48145b7f7fa0d2a07d2ce91f194efb53613cf9d560781243856967c0e7c51dcebd154b7f7fa5f58c2c335c
da21ddbf80c42bbf73e015476795d39361a6d1ce332e211cfe82915b3dc4a1119038e1061d06c5e770213b2f2669198f9631d3c3ef37fb23f176e521564c2b748a63ceb22d1bca68accee3ae27467e10fa
40fb1d5a5167822ac42e8be2504d73d9ace3004d2765f45f1604feb340b21ce19270053b3f002b67c5ad5fb8bc905e34a09470ee61032230a1927c64699b954cf8b493cf1a62febe6a3c40474ceda4da4c10
d21b24745df985ee084435a0829ad8a59d4756a74ad9d9ba88308f31cb818bf5d7d2c759a30133f7c85254b147be158f217e7486c4aad47dd7870857837eb95f30611325116d9408cb9d4d333605a4716
3bc822685c098fb4c23bf408f14d8fec779e34b9b595fbd493221e2788a8a4f47398a781d2ab36f154c8d1597965f8fe61cd63d8d5c8eac6a3a357be225278f2c5a36f1bbee506626d25cd028eacfd41ab
adb0e84d626e5d698c77db3bbdb61530a18b4e9898407cb0ed2cf97649abcf74de92086825514ea33bc9e3b9984c4d664c317edc5eac6fa7584c5996272d51a9ef7351fe63f034baba528c00910e81a3b99a050f4
a21f841faed4ad09c8e588ab0b673c9730c41623a661d6c8843359a62d0a19fd8b20be3dbdc19485d7591590f72c8e535356acce73a329e88a8102587d7b149526f0385edd377f1b8c448a253066107f19
3715723232df4beec56b0bc4f8096abeb459badad68702790f99d84e708c320ecfd18a50edfcdafec6589fadcf573b330da6f067fe83f23aaf06af1bcb5622dd6c83f09daee52436835c98f395fd3a3e6
347cf93485dced0fab9e18ef14524a1836be4e241cd0a14e7456dadba0d38ae3a7a29dc6af79a063af0f003f909e9c576944ac1a8336c52c42a289886345f59024548bbba4bc4345e891df2dc6a444af
f9eae4433fbb185838c5d74c50884ad432cb07528038ca149f2da554d66bb58f2633da736f75a5be5d8c8709d16342c806541a8a59015f65caf6173b8b60e0c241d8f8660aecaefae4ae089c526f6cc72daaeca
bc399688b1a961f5749dfbde83ef10ec574d171a09d93ba7210c023b924905e3318229764f7f708e355d8699d16342c806541a8a59015f65caf6173b8b60e0c241d8f8660aecaefae4ae089c526f6cc72daaeca
1271f0ce8b726bda764e948f85a051a8a3bd441924ab3a8a426e8fd9b856d6358c0816323958d2a61a37dd3945f15e2a7f311066efb9d5ad14084fcc37f335e869b123a3250adda743353dbec2b8d6f32ce918
77c6358b080507b6cbfa62c10ccc336f4f19d5c208a56110011d25f28956c2fd2e4b1fb0050d93204bf3621c5c0c470a3b6e26a3e03f020627166a937462f08c75b11ab20161c92f14ee02c839e755b609c1c

```

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

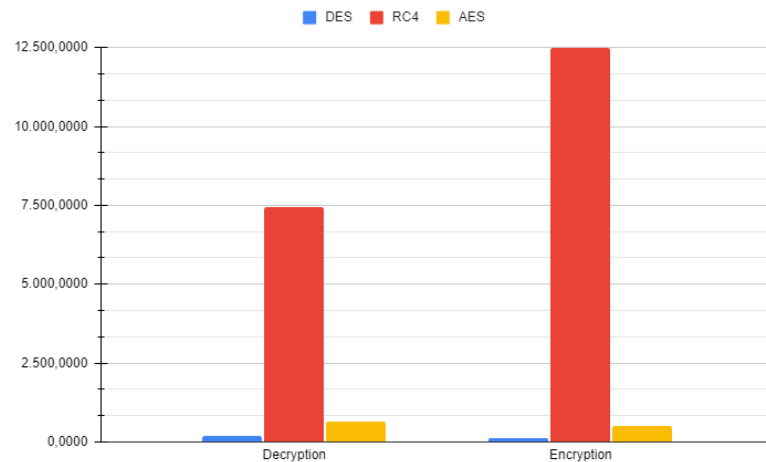
The RC4 uses stream generation keys to encrypt its data and has relatively long keys. But, there is a way by using a middle-man attack to retrieve the key generated and because of that it is now mostly insecure.

E. BETWEEN THE THREE

Based on our report for each symmetric cipher method, there are three 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.