CSE4057 INFORMATION SYSTEM SECURTIY

HOMEWORK 1

GÜLŞAH YILMAZ – 150113854

HALE ŞAHİN – 150116841

The Goal:

In this assignment our goal is to compare encryption time of various cryptographic algorithms. For this purpose, we generated a data of 128Kbytes and encrypt it with the following algorithms: DES, 3DES, AES – 128 bit key, AES – 256 bit key, RSA – 1024 bit key, RSA – 2048 bit key.

The Process:

We write down the code in java for these encryption algorithms. We used libraries existed in java. Then we created a text data which is 128 kb size. And run the algorithms with this input, algorithms gave us the encrypted output. We looked their execution time and took screenshots. Then we compared the algorithms according to their encryption time.

AES 128 & 256:

AES comprises three block ciphers: AES-128and AES-256. Each cipher encrypts and decrypts data in blocks of 128 bits using cryptographic keys of 128-and 256-bits, respectively. Symmetric (also known as secret-key) ciphers use the same key for encrypting and decrypting, so the sender and the receiver must both know and use the same secret key. There are 10 rounds for 128-bit keys and 14 rounds for 256-bit keys , a round consists of several processing steps that include substitution, transposition and mixing of the input plaintext and transform it into the final output of cipher text.

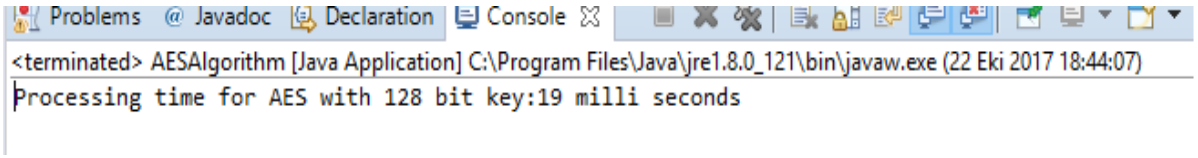


Figure 1. Encryption time for AES 128

Figure 2. Encryption time for AES 256

DES & 3DES:

DES uses a 56-bit key and runs through 16 cycles of 48-bit subkeys. When decrypting the data, the exact reverse operation is performed, using the same algorithm. The same key is used for the entire process. On the other hand, 3DES expands the size of the key by running the algorithm in succession with three different keys. It makes 48 passes through the algorithm. The resulting key is 168 bits; this can be hard to implement, so there is also a two-key option provided in 3DES that runs through a method called Encrypt-Decrypt-Encrypt (EDE):

1. Encrypt: The encryption is applied to the content using key 1.
2. Decrypt: This encrypted text is decrypted using key 2.
3. Encrypt: Lastly, the decrypted text from step 2 is encrypted again using key 2.

In the three-key method (which is much more cumbersome, but also more secure), the text is encrypted three times in succession. The text is encrypted with key 1, then that text is encrypted using key 2, and finally key 3 encrypts the last message/text.

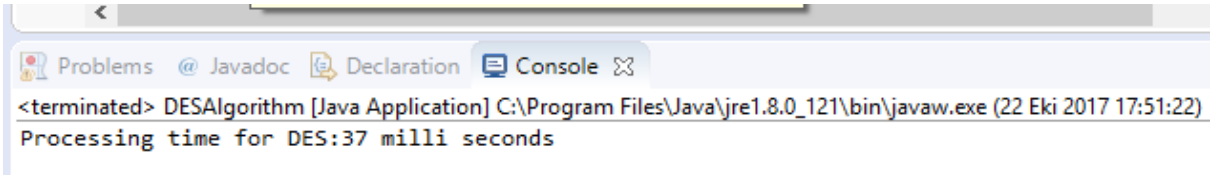


Figure 3. Encryption time for DES

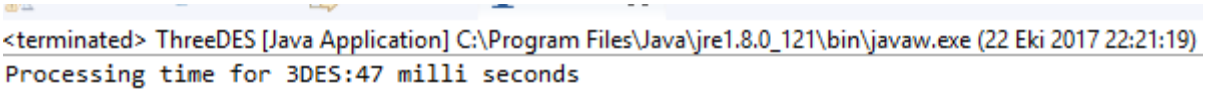


Figure 4. Encryption time for 3DES

RSA 1024 & RSA 2048:

RSA is an asymmetric system, which means that a key pair will be generated, a public key and a private key, obviously you keep your private key secure and pass around the public one.

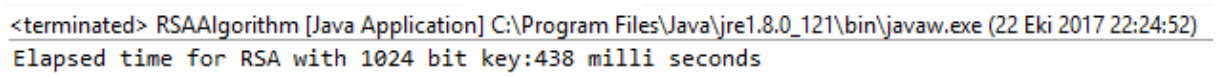


Figure 5.Encryption time for RSA 1024

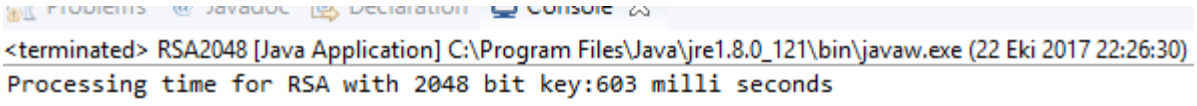
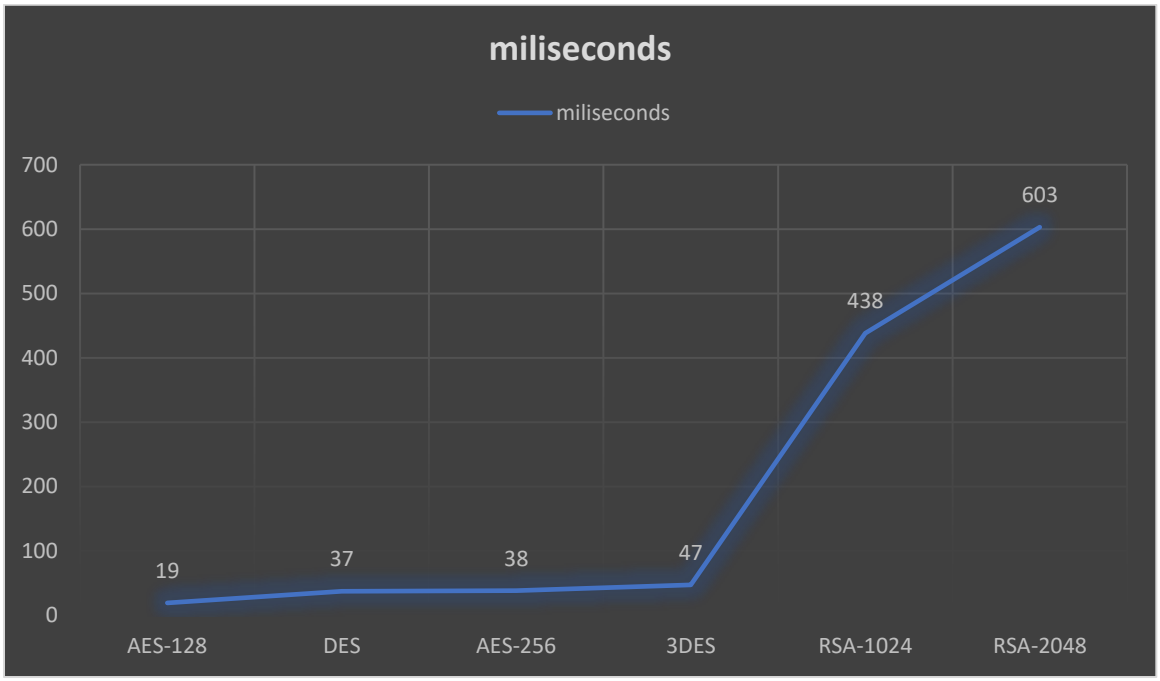


Figure 6. Encryption time for RSA 2048

Table 1. Encryption Time for the algorithms

Encryption Algorithm	Execution Time
AES-128	19ms
DES	37ms
AES-256	38ms
3DES	47ms
RSA-1024	438ms
RSA-2048	603ms

Table 2. Comparision of the encryption time



Result:

By looking at the encryption time of the algorithm, we can see that the longest time belongs to the RSA 2048 and slowest time is in the AES 128. This means RSA 2048 has more process doing encryption and it safer than others.