Computer Security

REPORT

FATIH SULTAN MEHMET VAKIF UNIVERSITY

2019 - 2020

AbderrahmanAbdellatif

1421221042

1) Used Platform:

- netbeans 8.2
- Java language

- First question, I use KeyPairGenerator. getInstance ("RSA") and Cipher. getInstance ("RSA") method for Generator RSA key and for the public and private key I used keys. getPublic (), keys. getPrivate ()

-Second question I use this function Get_SecKey (128, "AES") for 128-bit key and 256-key I used Get_SecKey (256, "AES") after that decrypt them with KA-. Like this cipher. Inuit (Cipher. DECRYPT_MODE, keys. getPrivate ());

-Third question I use Lorem ipsum for generating the text (message) for the apply hashing algorithm I used this code MessageDigest MD = MessageDigest. getInstance (name);
Byte digestarray [] = MD. Digest (inputtxt. getBytes ()) and after that encrypt with private key. To make (Digital signature.) (KA-(hash (M)) I used this code
Digital Signature = cipher. DoFinal (digestArray);

-Fourth Question I find 1MB file to Github and I read this file and write and now by use a now a function
ReadFile (String filename) and WrFile (String FileName, byte [] data). For Initialization Vector I used this
Function IvParameterSpec InitializeVector (int size).

I) AES (128 bit key)
I used this code Cipher. getInstance ("AES/CBC/PKCS5PADDING");
Cipher. Inuit (Cipher. ENCRYPT_MODE, secretKey128, ivParams); For the time System. Meantime ().

ii)AES (256 bit key)
IvParameterSpec ivParams256 = InitializeVector (16);
cipher = Cipher. getInstance
("AES/CBC/PKCS5PADDING");
SecretKeySpec keySpec = new SecretKeySpec (secretKey256.getEncoded (), "AES");

iii) DES in CBC mode
Fort get Des key I used SecretKey DesKey = Get_SecKey (56, "DES"); this function, but The key ostensibly consists of 64 bits; however, only 56 of these are actually used by the algorithm. Eight bits are used solely for checking parity, and are thereafter discarded. Hence the effective key length is 56 bits, And it is never quoted as such. Every 8th bit of the selected key is discarded, i.e. Positions 8, 16, 24, 32, 40, 48, 56, 64 are removed From the 64 bit key leaving behind only the 56 bit key.
IvParameterSpec ivParams3 = InitializeVector (8);
cipher = Cipher. getInstance
("DES/CBC/NoPadding");
Cipher. Inuit (Cipher. ENCRYPT_MODE, DesKey, ivParams3); // 56 bit key

Output:

```
run:
{Private=sun.security.rsa.RSAPrivateCrtKeyImpl@42523, Public=Sun RSA public key, 1024 bits
  modulus: 1016581205126029418149817415653375883762995217531145022489424772010577291477632897635604192787224566229324044856418051351525257121
  public exponent: 65537}
{128 Bit KEY: =0011001000000111010110100011101110010111100101100000010010111111111101110111001101000110010000011011001011110101110010010111(
128 bit Key encrypted: 0010101010100111011001101011100100110011001101001100010111101001011000100000011100001101010011100001110010100001111001
128 bit Key decrypted: 0011001000000111010110100011101110010111100101100000010010111111111101110111001101000110010000011011001011110101110010(

256 bit Key encrypted: 0010010011110111100011000011010001100110111111010110001100010100101001100111000010110101001011000011000101110101010111
256 bit Key decrypted: 0111010111111111101000001111101000011010001010101001000001110001111010110100110101001010011010110111001010111101010111
m: تالي يكون النص الناتج خالي من التكرار، أو أي كلمات أو عبارات غير لائقة أو ما شابه. وهذا ما يجعله أول مولّد نص لوريم إيبسوم حقيقي على الإنترنت
digest: 1011111110110101101110010011001101000000000111111000010110111010001011001001011001110001000000010101011000100111110011100010100000001
digital signature: 1000001010101001111100010001001110001111010100110100110111011100101000011101011011111101011011111000101011100100111000011101
128 bit key time: 0.0227611
 First Initialization Vector: [35, -52, -11, -31, 78, 12, 8, -86, 64, -77, -40, -13, -21, -123, -104, -53, 35, -95, -80, 112, 28, 90, 115, -4
 Second Initialization Vector: [-78, 26, -69, 10, 73, 40, -5, -19, -59, 90, -6, -108, -122, 60, 45, 48, -18, 107, -99, -124, -46, -61, 30, 98
timer with 256 bit : 0.00557
Des timer: 0.05483
BUILD SUCCESSFUL (total time: 20 seconds)
```

The main Idea of homework :

1-B+(S)

2-B-(B+(S))

3- A-B (s)

4- A= S(A-(m))

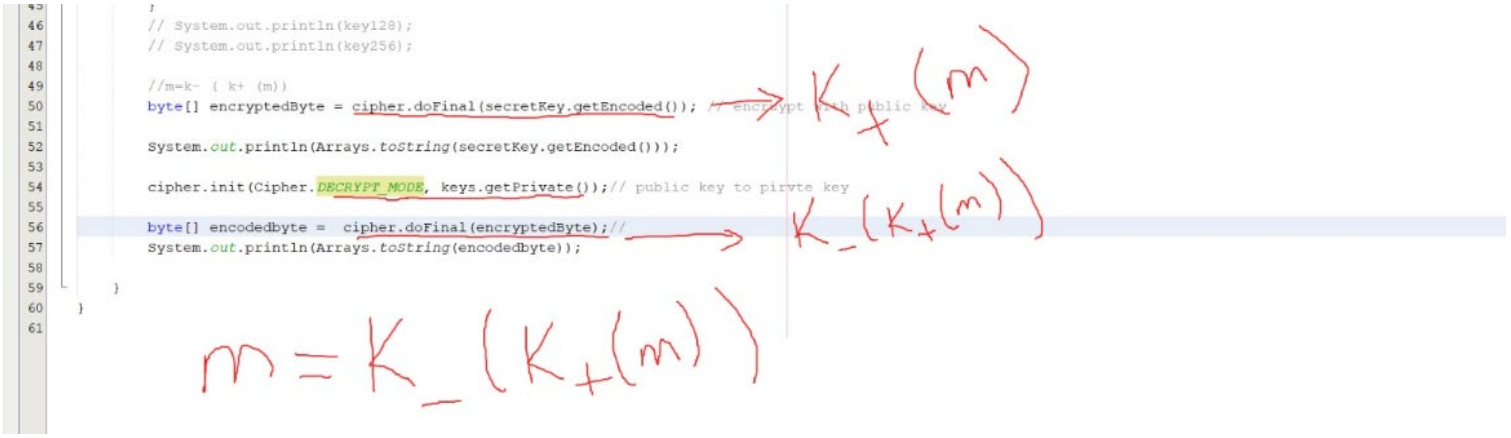
5 - BS(s)->A+(A-)->m

buyuk m olursa ?

hash kullaniyoruz

6- s(A-(hash(m)) ,m)
m kimsinie almamsi icin
s ile yapiyoruz

7- B ->(s) -> A+(A-) -> B->hash(m)->
|___> m = hash(m)



Source:

https://www.oracle.com/java/technologies/javase-jce8-downloads.html
https://docs.oracle.com/javase/7/docs/api/javax/crypto/Cipher.html