CSE4057 Spring 2022

Homework 1

Ahmet Emirhan Bakkal 150117056

Yunus Yıldırım 150116006

Muhammed Raşit Ayaz 150118016

# Question – 1

## Generate an RSA public-private key pair.

In the first question, we create an object from the KeypairGenerator class and initialize this object with a size of 1024. Since we want to obtain our keys with the RSA algorithm, we use RSA in the getInstance method of KeyPairGenerator. After this process, we create a KeyPair and use this Keypair to obtain our public and private keys.(Keys in the keys.txt file)

Text

Description automatically generated

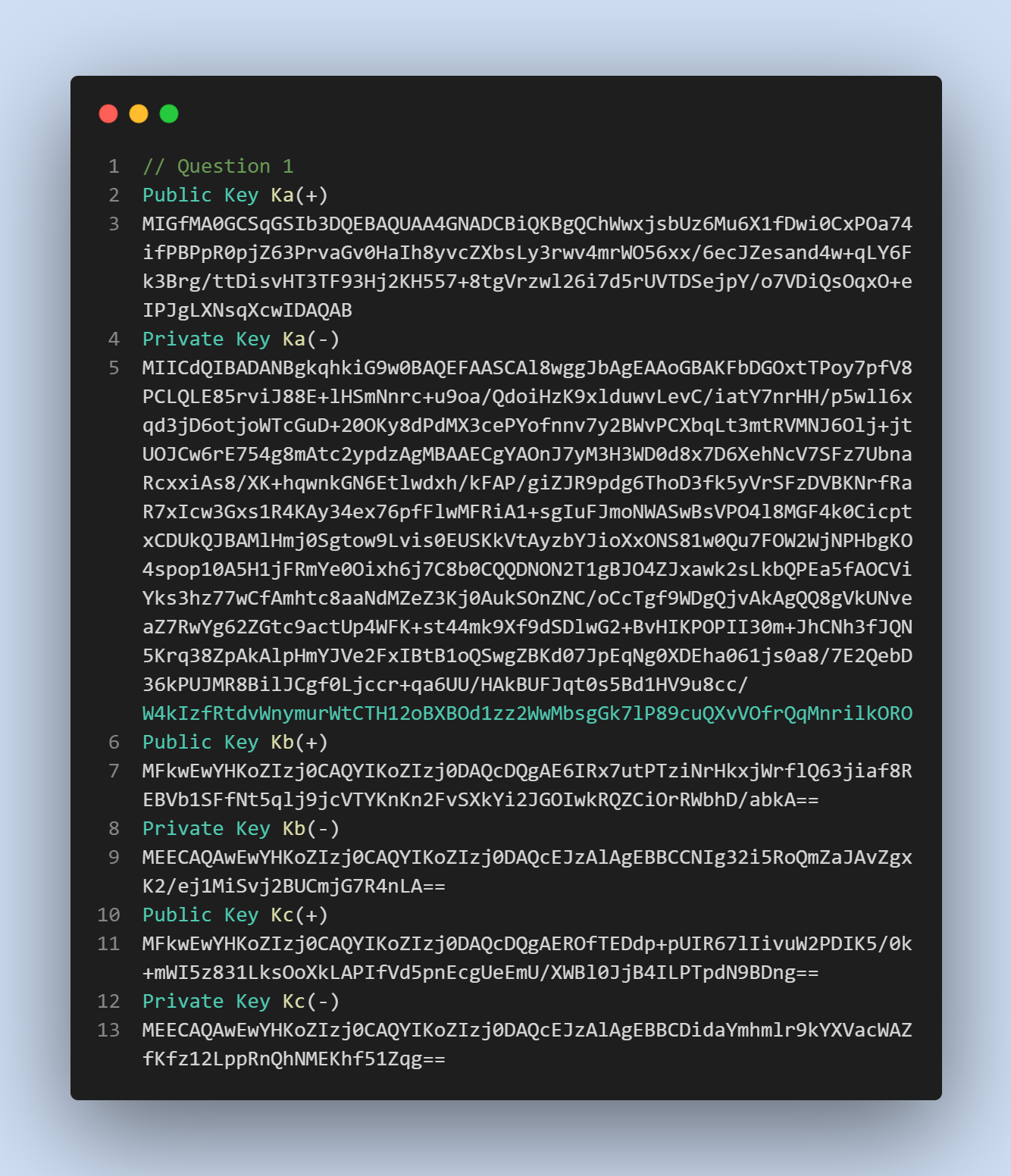
## Generate two Elliptic-Curve Diffie Helman public-private key pairs.

In part B of the question, we are asked to create two key pairs with the Elliptic-Curve Diffie Helman algorithm, and we call the EC algorithm with the getInstance method, different from the operations in option A, and we create two different keypairs to find different public and private keys.

Text

Description automatically generated

KEYS



# Question – 2

## Generate two symmetric keys using a secure key derivation function: 128 bit K1 and 256 bit K2. Encypt them with KA(+), and then decrypt them with KA (-).

In Part A of Question 2, we create two different symmetric keys, one of which is 128 and the other is 256, using Securerandom and AES.

After this process, we create a Cipher with the RSA algorithm. We encrypt this cipher with Ka(+)'s public key and then decrypt it with Ka(-)'s private key.

We repeat the same operations for the 256-bit symmetric key.(Keys in keys.txt file )

Text

Description automatically generated

metin içeren bir resim

Açıklama otomatik olarak oluşturuldu

# Question – 3

## Any text of at least 1000 characters. Apply SHA256 Hash algorithm. Then encrypt it with KA(-). signature.) Then verify the digital signature. Print m, H(m) and digital signature on the screen.

First, we read our message and digested it with the SHA-256 algorithm. Then, we encrypted our message with using RSA cipher and private key of Ka(-). After that, we decrypted message with RSA cipher and public key of Ka(+). Finally we compared the messages and verify the digital signature.

Text

Description automatically generated

Text

Description automatically generated

# Question – 4

## AES (128 bit key) in CBC mode.

Text

Description automatically generated

## AES (256 bit key) in CBC mode.

Text

Description automatically generated

## iii) AES (256 bit key) in CTR mode.

Text

Description automatically generated

## Time Result

Text

Description automatically generated

Encrypted and Decrypted file in the folder

# Question – 5

## Generate a message authentication code (HMAC-SHA256) using any of the symmetric keys. Apply HMAC-SHA256 to K2 in order to generate a new 256 bit key.

Text

Description automatically generated

Text

Description automatically generated