**CSE4057 Spring 2022**

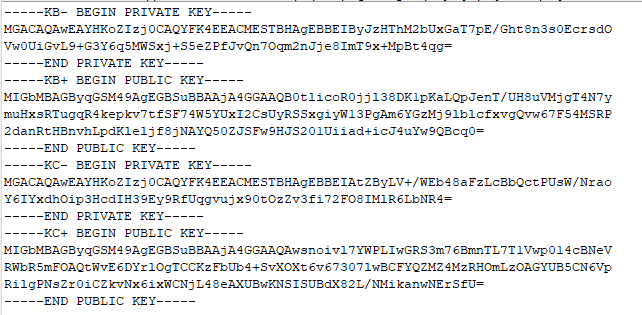
**Homework 1**

**Hasan Hut 150119764**

**Furkan Yapıcıoğlu 150119724**

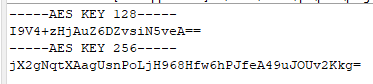
**1-)**

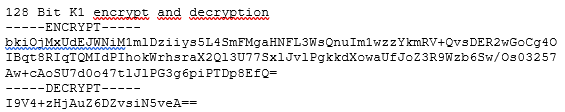
**a-)**

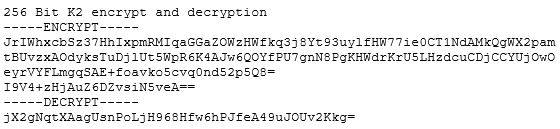
**b-)**

**2-)**

**a-)**



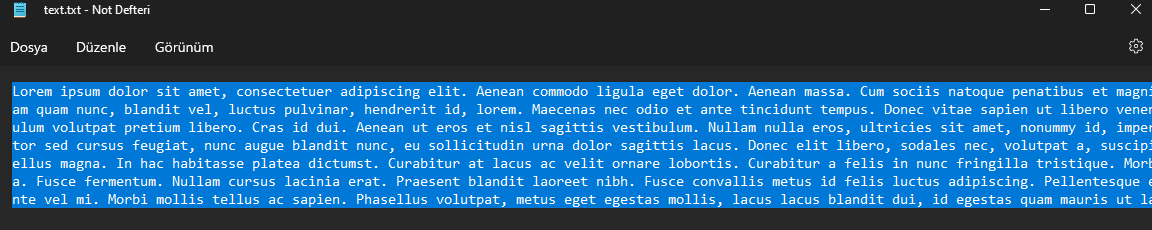


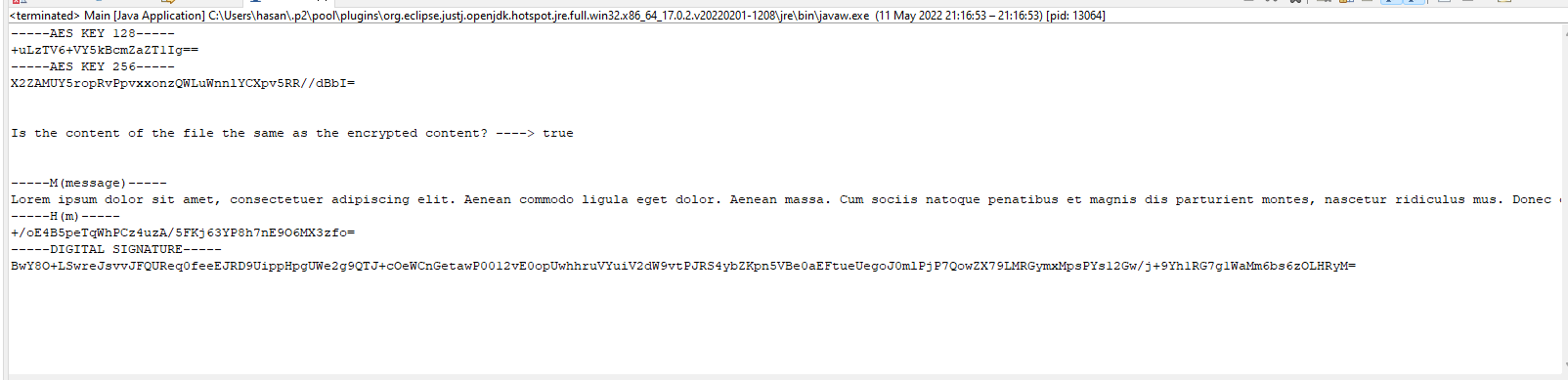


**b-)** NOT COMPLETED

**3-)**

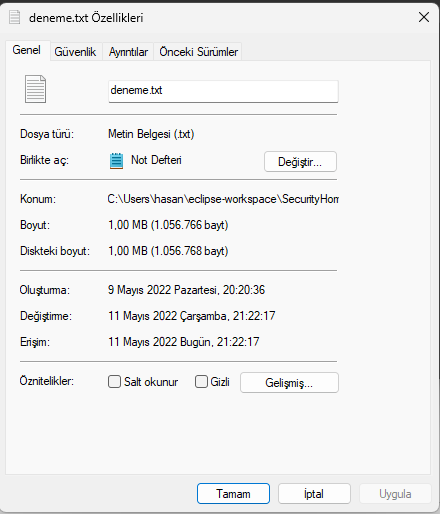
* Text File has 1000 words lorem ipsum:

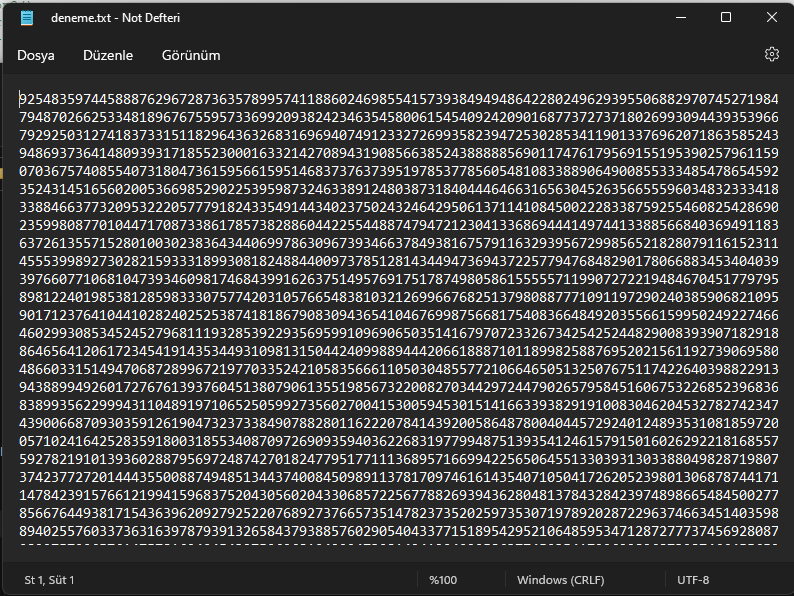




**4-)**

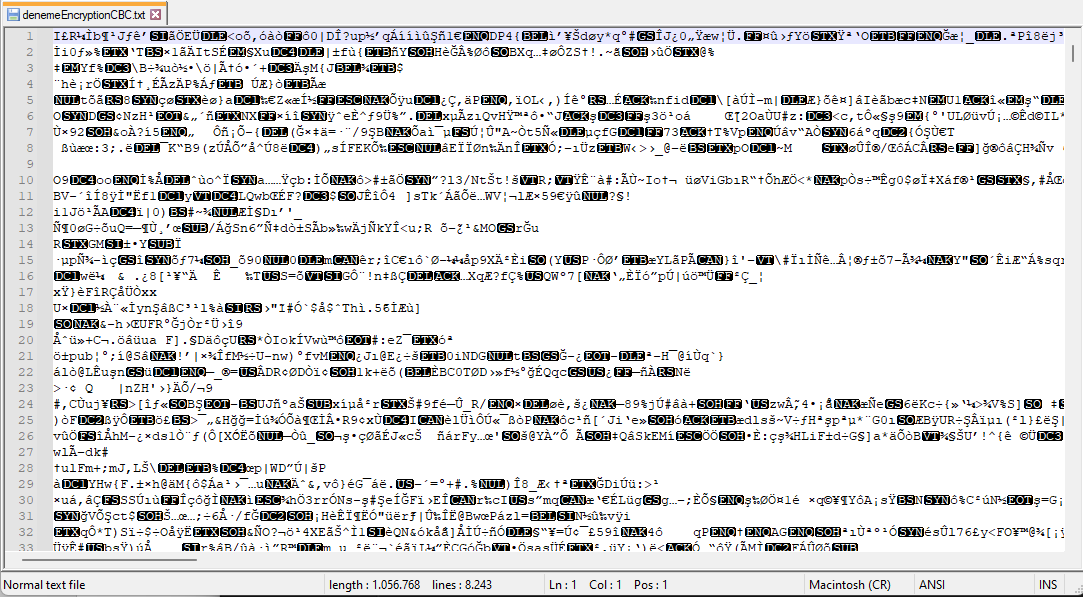
* We have 1Mb deneme.txt file:



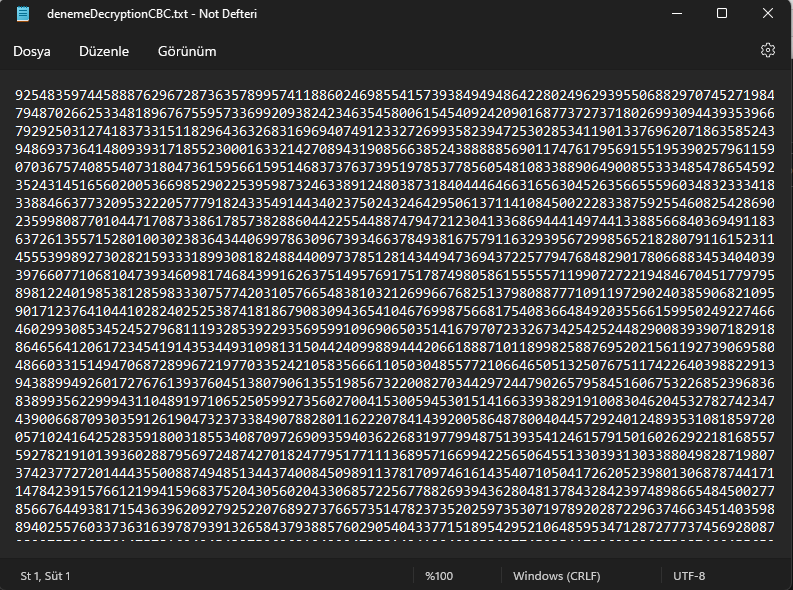


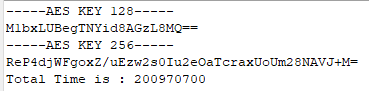
* **128 Bit CBC:**
  + Encryption File:

You have to open with Notpad++ for encryption file.



* + Decryption File:



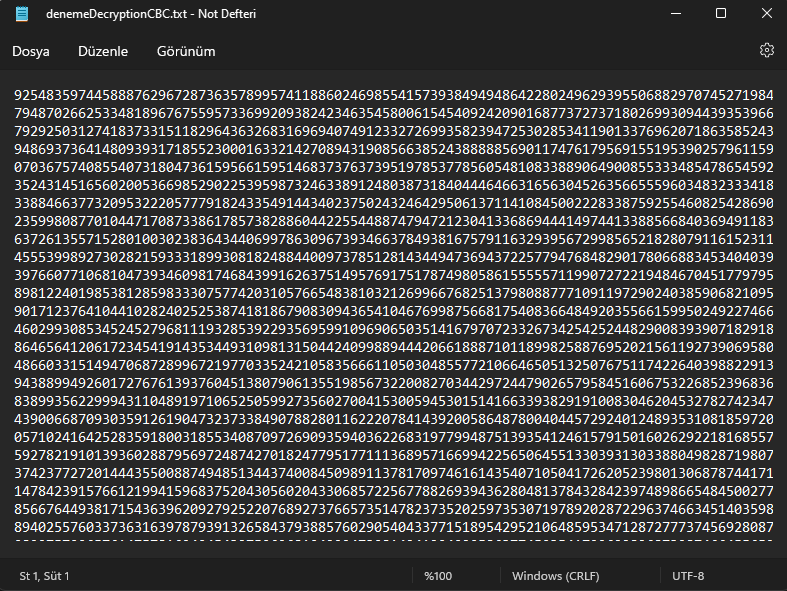
* + Total Time:

256 Bit CBC:

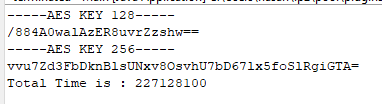
* **256 Bit CBC**
  + Encryption File:



* + Decryption File:



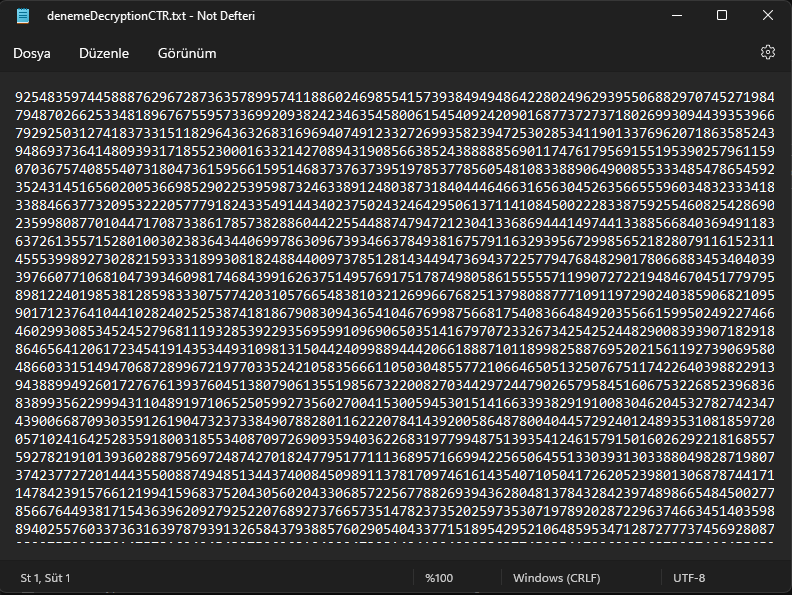
* + Total Time is:



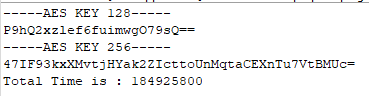
* **256 bit CTR**
  + Encryption File:



* + Decryption File:



* + Total Time is:



* 256 Bit CTR is much faster than others.

For Question 4, D part is not completed.

**5-)** NOT COMPLETED