**Case Study 2 – Advanced Encryption Standards (AES) Walkthrough**

Amazon Web Services (AWS) is the world’s most comprehensive and broadly adopted cloud platform. AWS Key Management Service uses the Advanced Encryption Standard (AES) algorithm with 256-bit secret keys for Server-Side Encryption. Advanced Encryption Standard (AES) is a symmetric block cipher encryption that receives 128-bit size for each block and the size of key is 128, 192, and 256 bits. AES procedure involves some encryption rounds, which are determined by the cipher key size. The mentioned standard uses 10 rounds in AES-128, 12 rounds in AES-192, and 14 rounds in AES-256. Through encryption, every round is collected as a set of four main transformations.

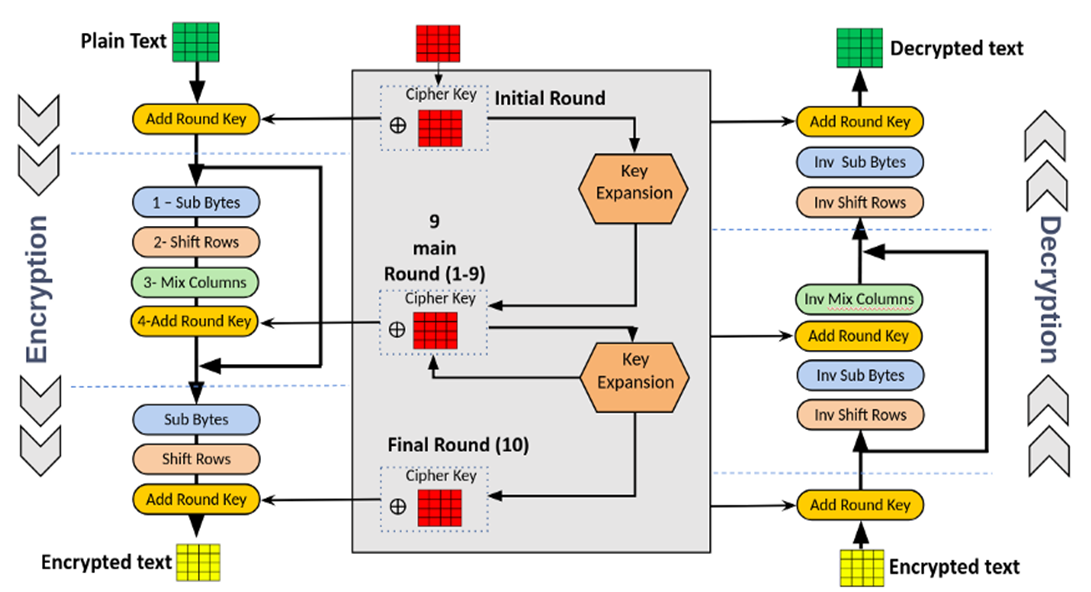


Figure displays the main construction of the encryption in AES method. Each round covers four main transformations: SubByte, Shift Row, Mix Column, and Add Round Key.

Let us start with the following input:

K (secret key):

P (plaintext):

Now perform a round of encryption on the plaintext using AES-128, writing out the following steps:

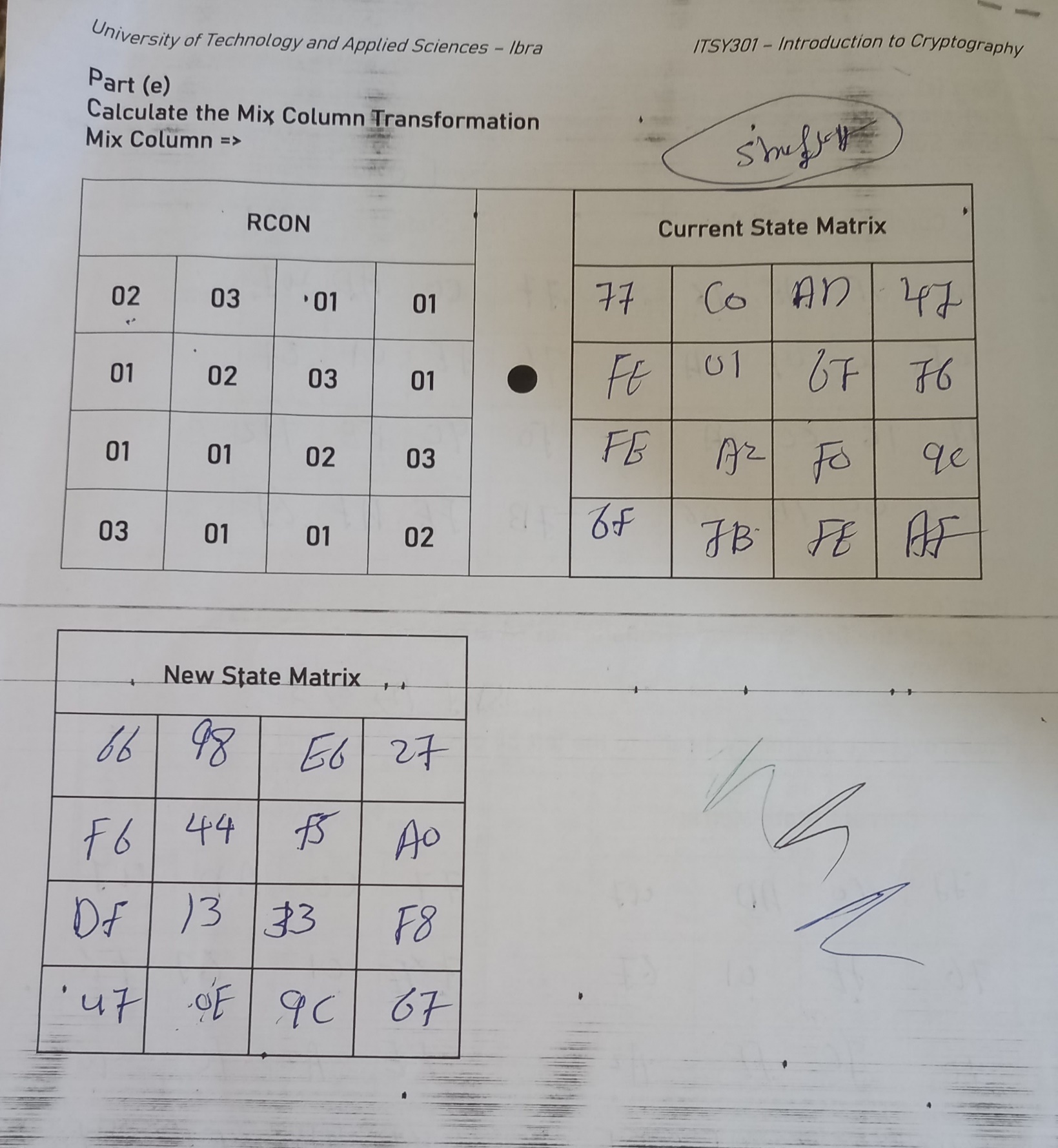
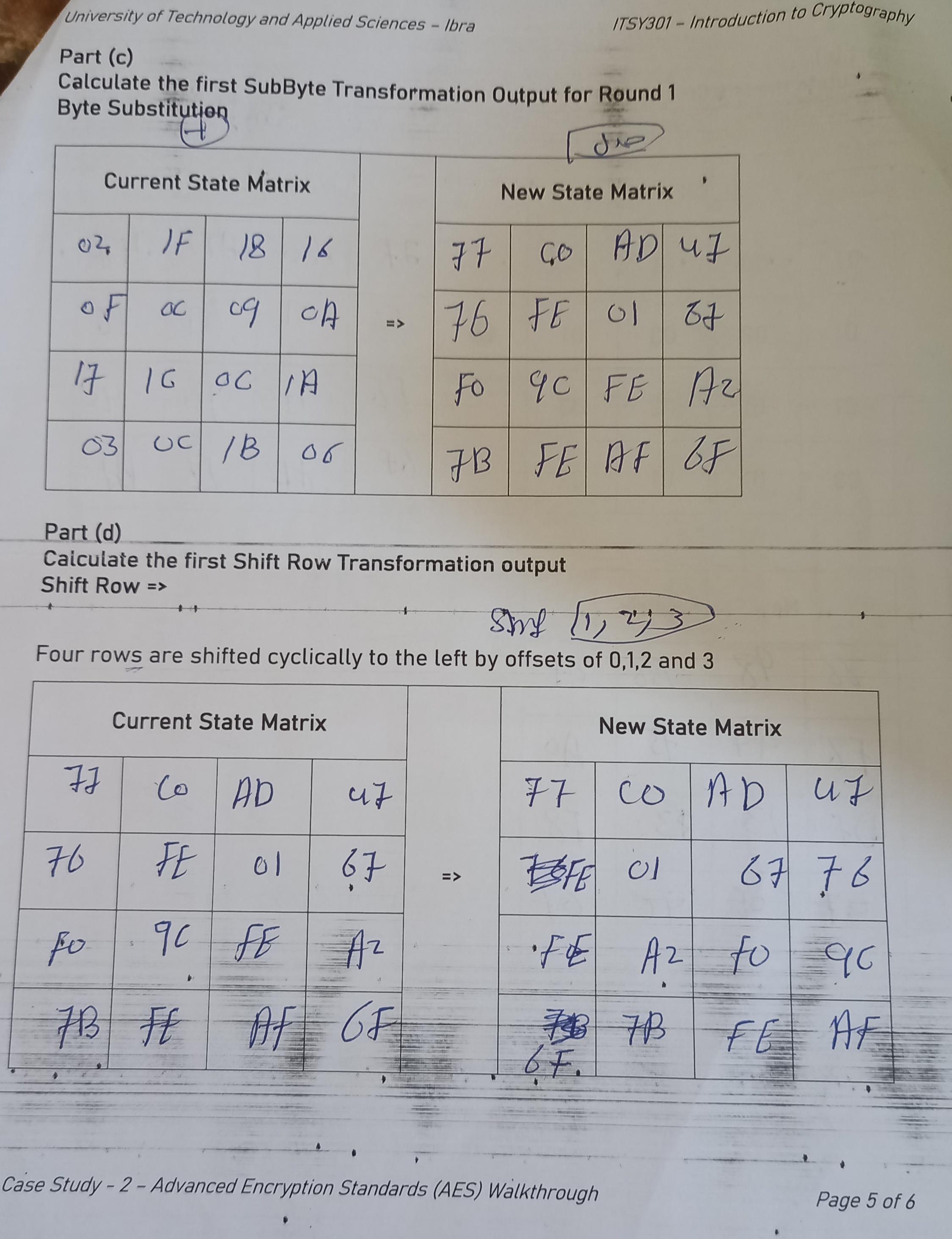
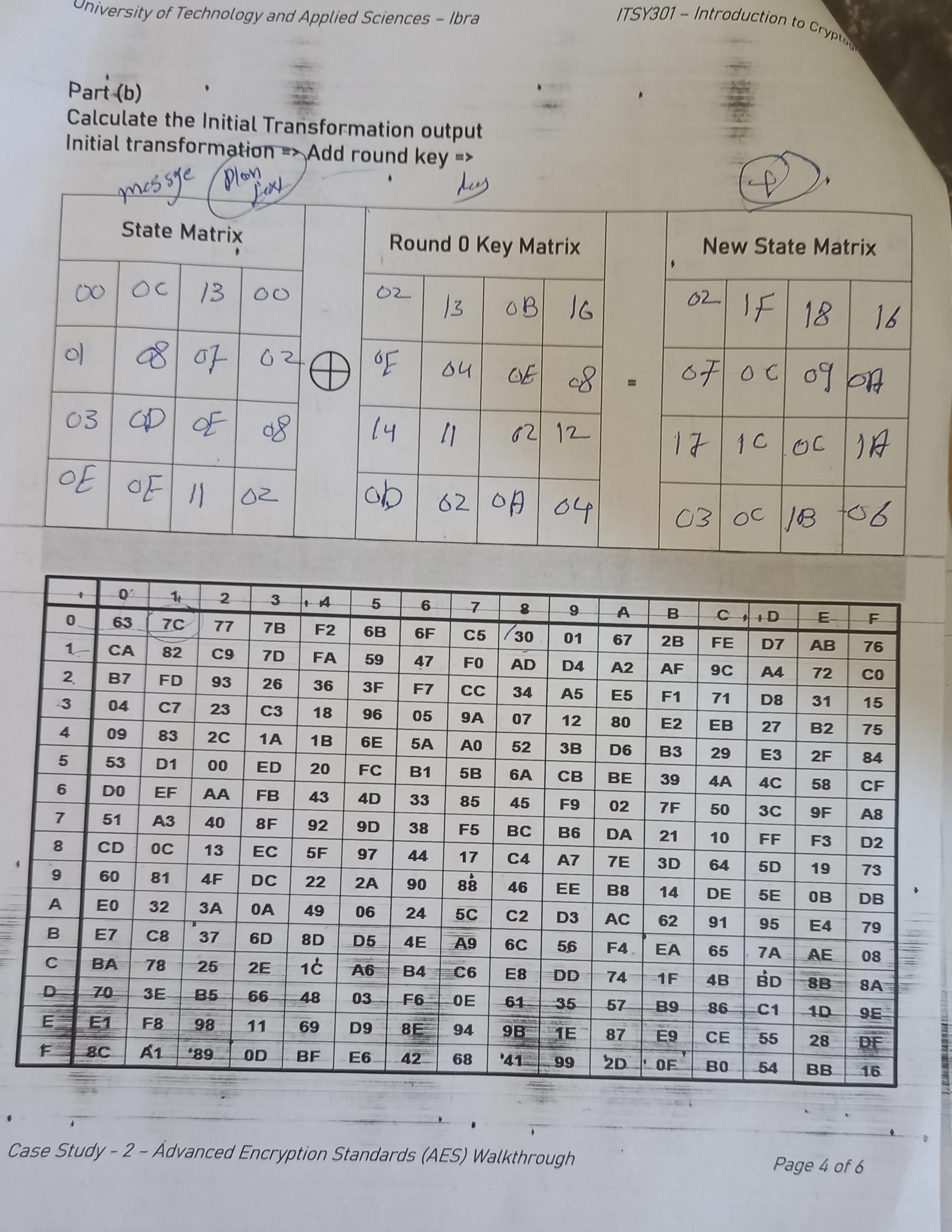
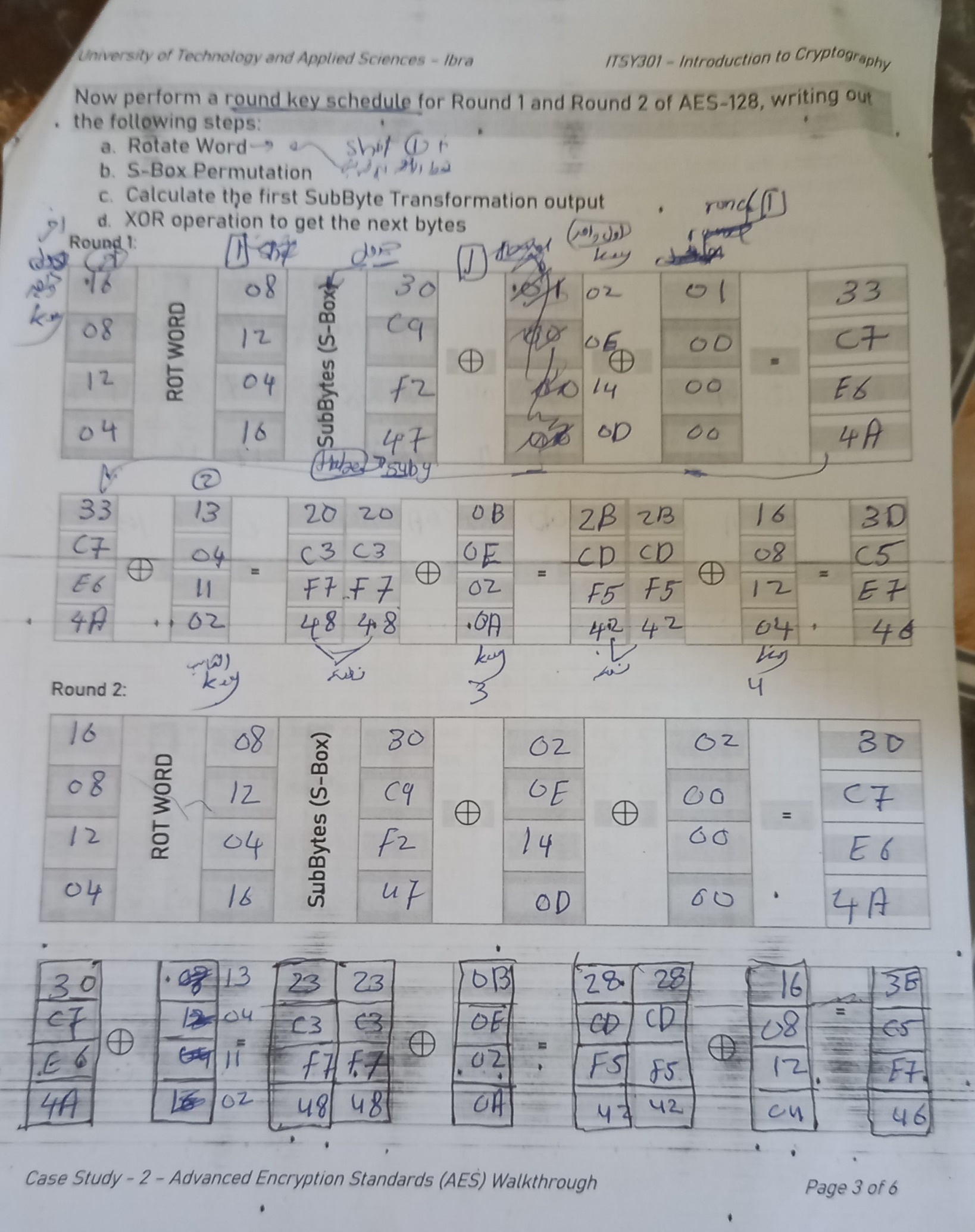
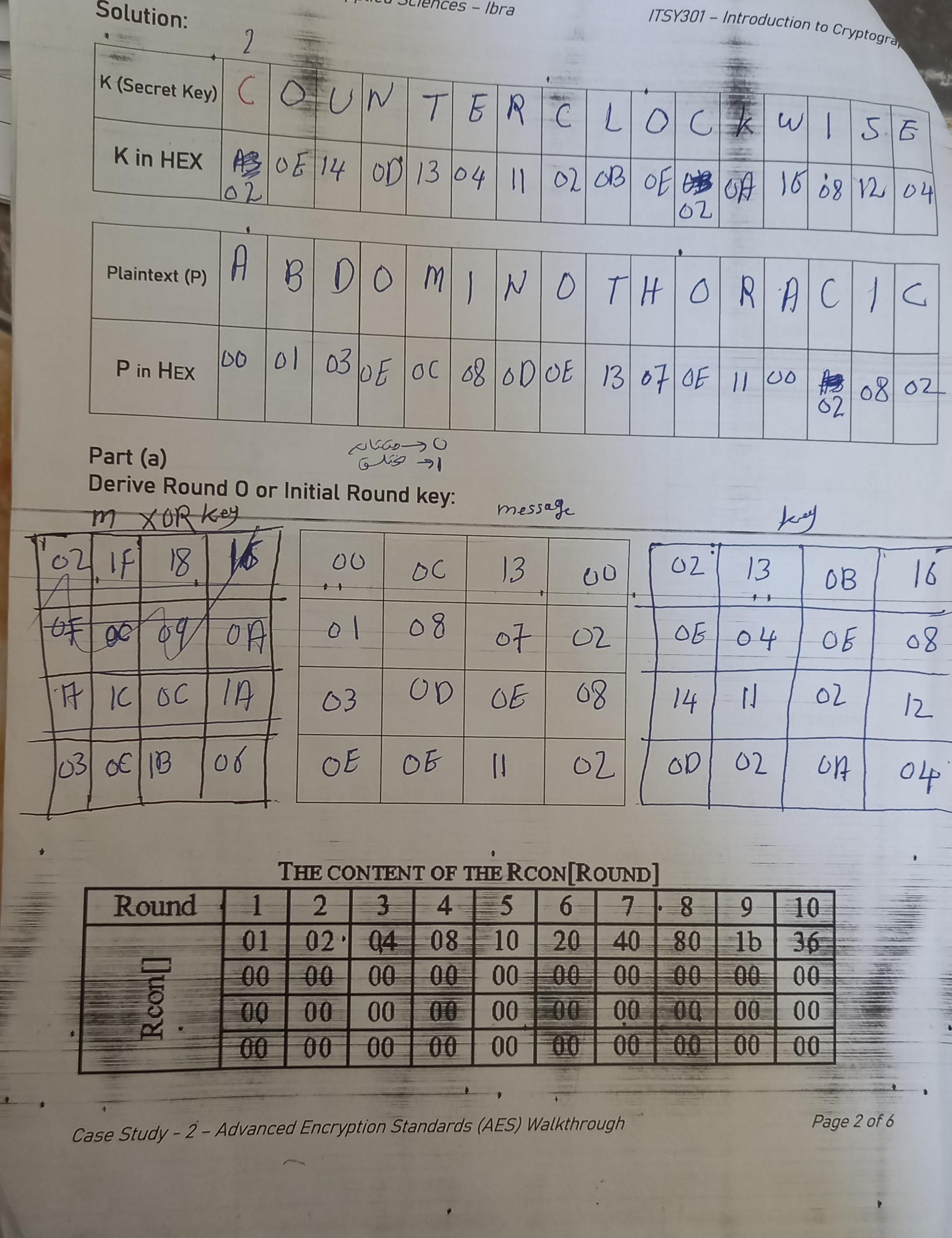
(a) Derive Round 0 key (16 bytes)

(b) Calculate the Initial Transformation output

(c) Calculate the first SubByte Transformation output

(d) Calculate the first Shift Row Transformation output

(e) Calculate the first Mix Column Transformation output

****