COMS453 - hw2 report

Benjamin Lee, Feifei Cheng, Marios Tsekitsidis

1. See separate report.
2. (a) See 2(d)

   (b) i. Alice generates a key pair (pk, sk).

   ii. Alice sends the pk and its encrypted matrix to Bob.

   iii. Bob performs matrix multiplication on the encypted matrix and his matrix B.

   iv. Alice decrypts the results with her private key sk.

   The core part is the third step, where Bob calculates the production of B and the encrypted A from Alice. By leveraging properties of Homomorphic Encryption as follows:

$$E(a) * E(b) = E(a+b)$$

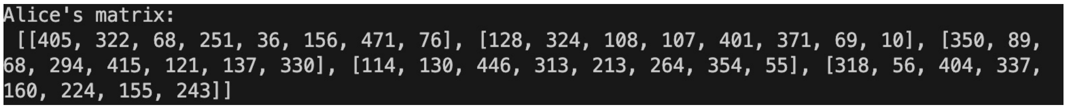
$$E(a)^b = E(a * b)$$

   Let the ith row of A be $A_i = [a_1, a_2, ..., a_8]$ and jth column of B be $B_i = [b_1, b_2, ..., b_8]$, the element C_{ij} of encrypted product is:

$$E(A_i * B_j) = E \sum_{k=1}^{8} (a_k * b_k) = \prod_{k=1}^{8} E(a_k * b_k) = \prod_{k=1}^{8} E(a_k)^{b_k}$$

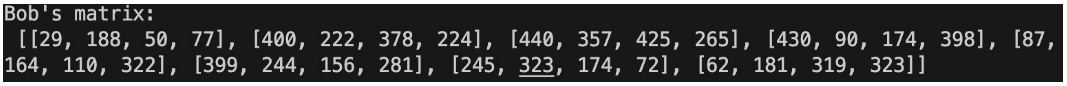
   (c) See code HW3-2.py

   (d) The input matrices:



```
Alice's matrix:
 [[405, 322, 68, 251, 36, 156, 471, 76], [128, 324, 108, 107, 401, 371, 69, 10], [350, 89,
68, 294, 415, 121, 137, 330], [114, 130, 446, 313, 213, 264, 354, 55], [318, 56, 404, 337,
160, 224, 155, 243]]
```

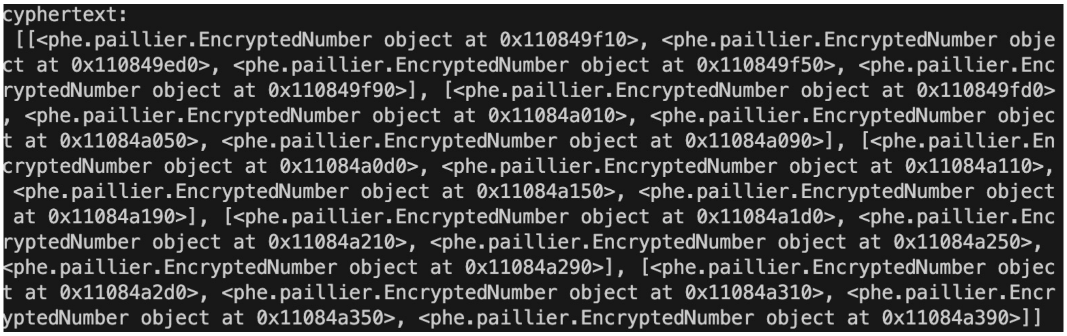
Figure 1: Alice's matrix A



```
Bob's matrix:
 [[29, 188, 50, 77], [400, 222, 378, 224], [440, 357, 425, 265], [430, 90, 174, 398], [87,
164, 110, 322], [399, 244, 156, 281], [245, 323, 174, 72], [62, 181, 319, 323]]
```

Figure 2: Bob's matrix B

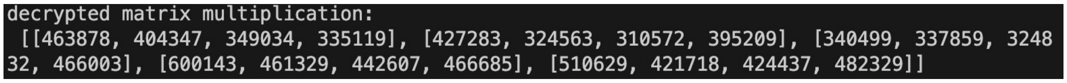
Encrypted result:



```
cyphertext:
 [[<phe.paillier.EncryptedNumber object at 0x110849f10>, <phe.paillier.EncryptedNumber obje
ct at 0x110849ed0>, <phe.paillier.EncryptedNumber object at 0x110849f50>, <phe.paillier.Enc
ryptedNumber object at 0x110849f90>], [<phe.paillier.EncryptedNumber object at 0x110849fd0>
, <phe.paillier.EncryptedNumber object at 0x11084a010>, <phe.paillier.EncryptedNumber objec
t at 0x11084a050>, <phe.paillier.EncryptedNumber object at 0x11084a090>], [<phe.paillier.En
cryptedNumber object at 0x11084a0d0>, <phe.paillier.EncryptedNumber object at 0x11084a110>,
 <phe.paillier.EncryptedNumber object at 0x11084a150>, <phe.paillier.EncryptedNumber object
 at 0x11084a190>], [<phe.paillier.EncryptedNumber object at 0x11084a1d0>, <phe.paillier.Enc
ryptedNumber object at 0x11084a210>, <phe.paillier.EncryptedNumber object at 0x11084a250>,
<phe.paillier.EncryptedNumber object at 0x11084a290>], [<phe.paillier.EncryptedNumber objec
t at 0x11084a2d0>, <phe.paillier.EncryptedNumber object at 0x11084a310>, <phe.paillier.Encr
yptedNumber object at 0x11084a350>, <phe.paillier.EncryptedNumber object at 0x11084a390>]]
```

Figure 3: cipher product of A and B

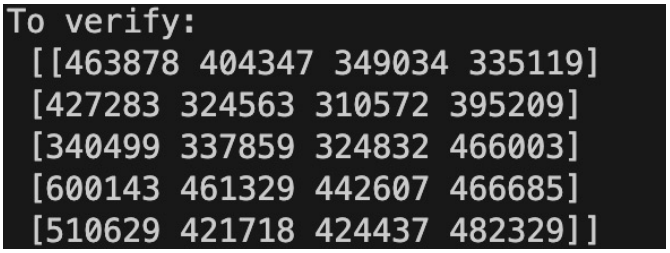
Decrypted result:



```
decrypted matrix multiplication:
 [[463878, 404347, 349034, 335119], [427283, 324563, 310572, 395209], [340499, 337859, 3248
32, 466003], [600143, 461329, 442607, 466685], [510629, 421718, 424437, 482329]]
```

Figure 4: cipher product of A and B

Verification with the product of two plain matrices:



```
To verify:
 [[463878 404347 349034 335119]
 [427283 324563 310572 395209]
 [340499 337859 324832 466003]
 [600143 461329 442607 466685]
 [510629 421718 424437 482329]]
```

Figure 5: plain product of A and B

3. See separate report.