2021-2022 Spring – Midterm Exam **ÜSKÜDAR UNIVERSITY** COME 311 – Data Security

**Instructor:** Fatih Temiz

**Name:** Yunus Emre Topçu

**Student No:** 180209801

**Department:** Software Engineering

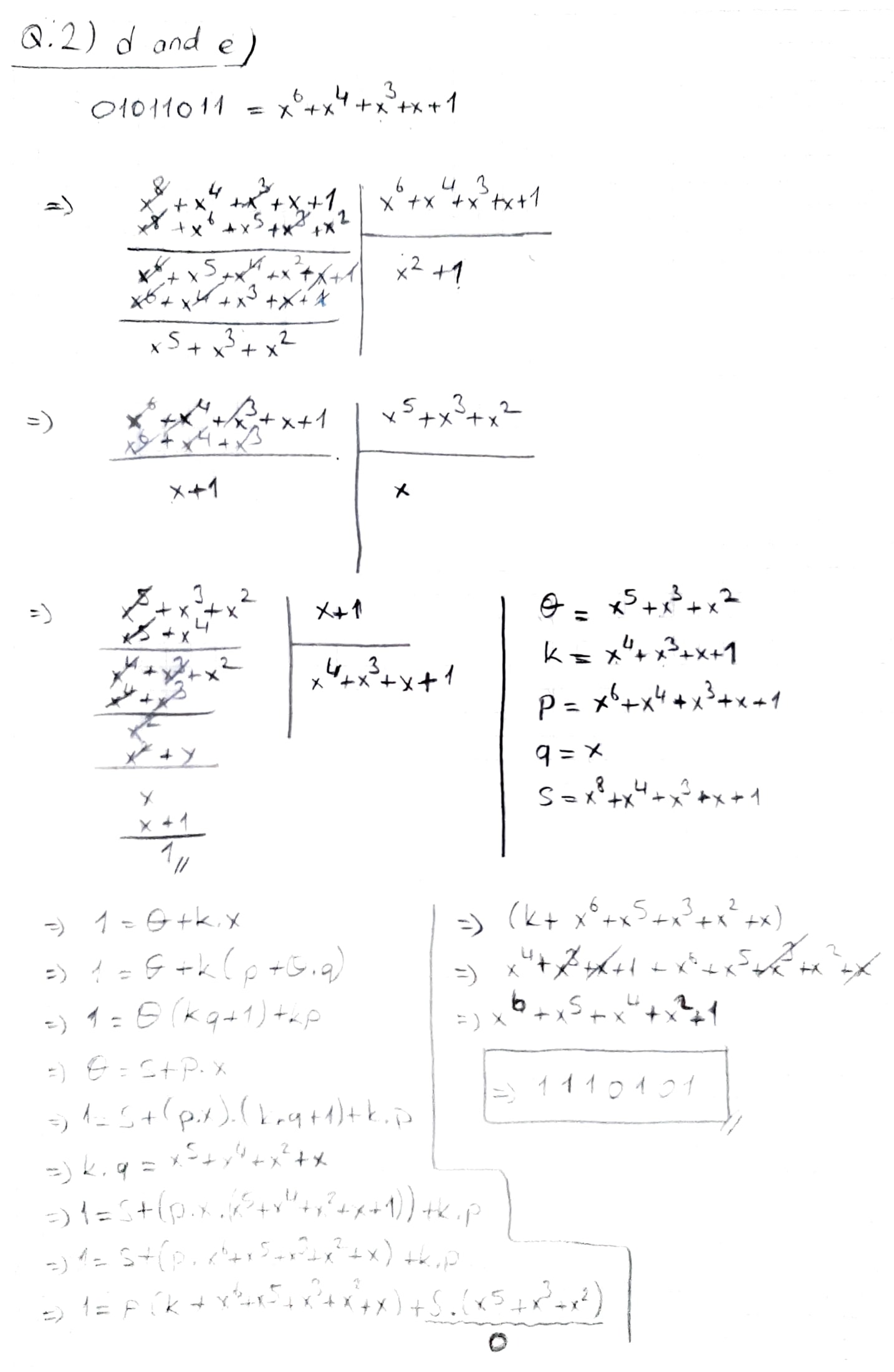
**ANSWERS**

**Q2)**

1. 80209801 (mod2) = 00001001
2. Row number = 82 = 01010010
3. 00001001 (XOR) 01010010 = 01011011

and





**Q3)**

* p = 557
* 557 is prime

for 558;

* 2 \* 3 2 \* 31 = 558
* **A** = 558 / 2 = 279
* **B** = 558 / 3 = 186
* **C** = 558 / 31 = 18

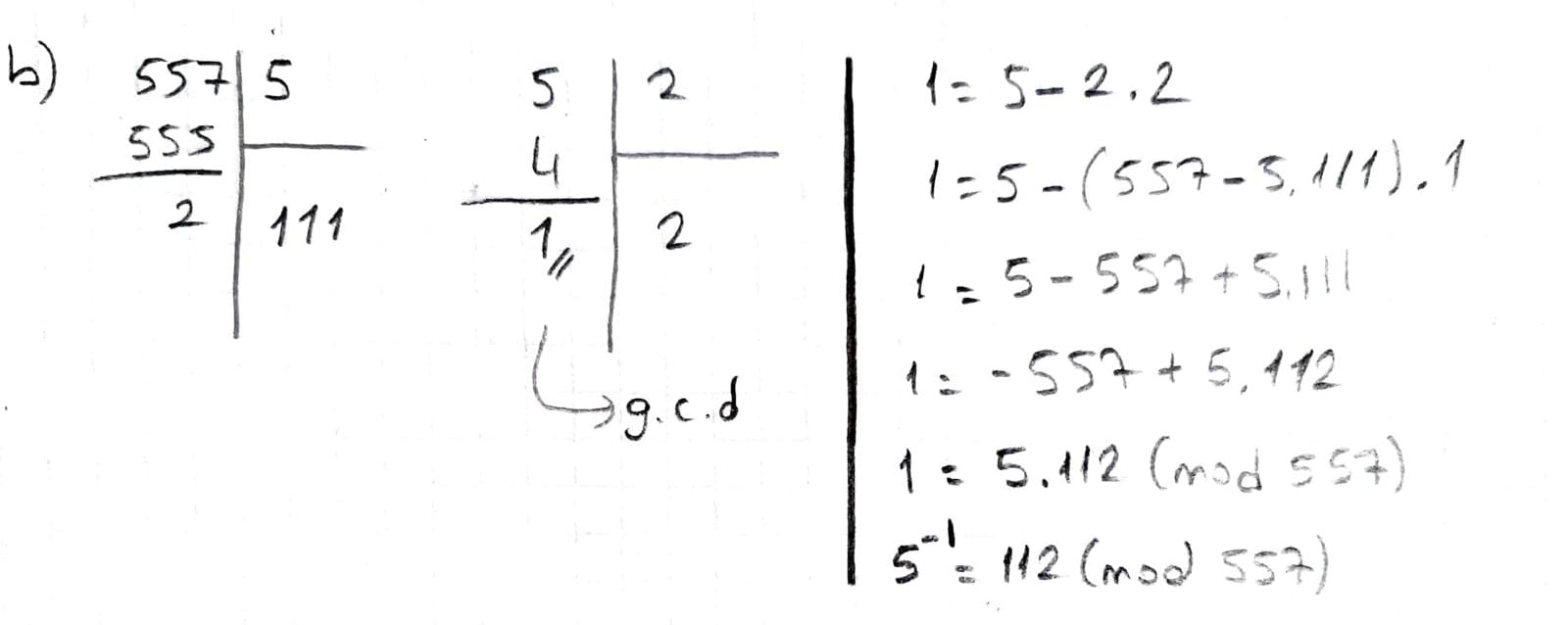


for 556;

* 22 \* 139 = 556
* **A** = 556 / 2 = 278
* **B** = 556 / 139 = 4



b)



**Q4)**



* q = 571
* 571 is prime

for 570;

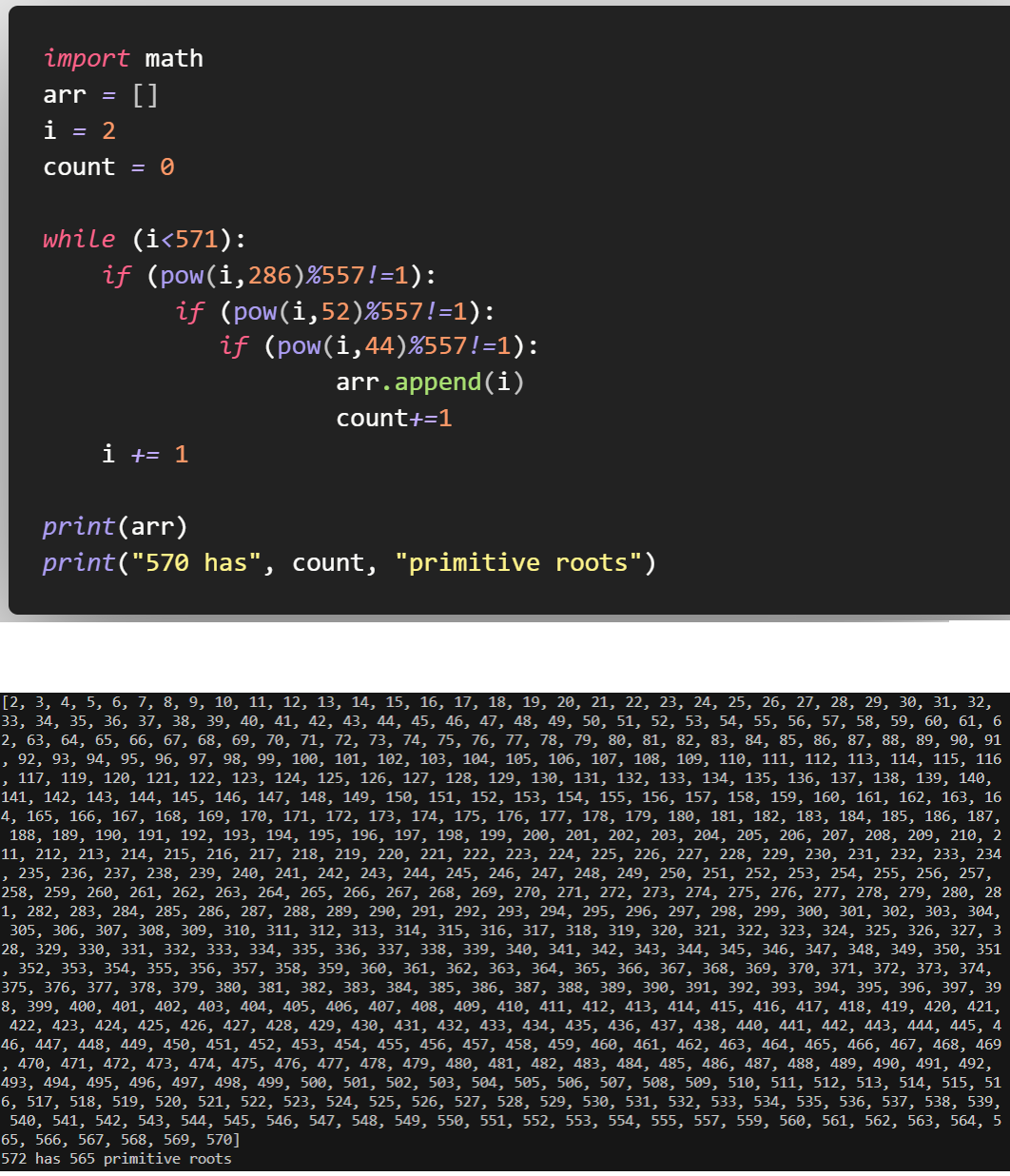
* 2 \* 3 \* 5 \* 19 = 570
* **A** = 570 / 2 = 285
* **B** = 570 / 3 = 190
* **C** = 570 / 5 = 114
* **D** = 570 / 19 = 30

metin içeren bir resim

Açıklama otomatik olarak oluşturuldu

for 572;

* 22 \* 11\* 13 = 572
* **A** = 572 / 2 = 286
* **B** = 572 / 11 = 52
* **C** = 572 / 13 = 44





Step 1 🡪 Alice and Bob get public numbers q=571, G = 7

Step 2 🡪 Alice selected private key a = 32 and Bob selected private key b = 64

Step 3 🡪 Compute the values

* Alice: x = (732 mod 571) = 377
* Bob: y = (764 mod 571) = 521

Step 4 🡪 Alice and Bob Exchange the numbers

Step 5 🡪 Alice receives public key y = 521 and bob receives public key x=377

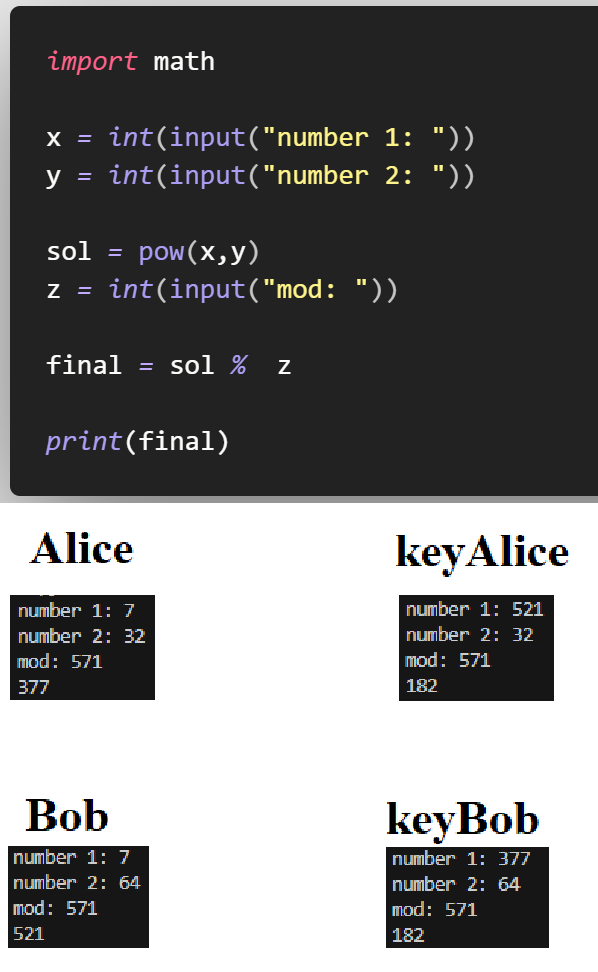
Step 5 🡪 Compute symmetric keys

keyAlice = (52132 mod 571) = 182

keyBob = (37764 mod 571) = 182

Step 7 🡪 182 is the shared secret.

My code:



1. I used the code I gave in option b.

a = 7, q = 571

* a-1 = aq-2 (mod q)
* 7-1 = 7569 (mod 571)
* 408

metin içeren bir resim

Açıklama otomatik olarak oluşturuldu