Instructor: Fatih Temiz

Name: Yunus Emre Topçu

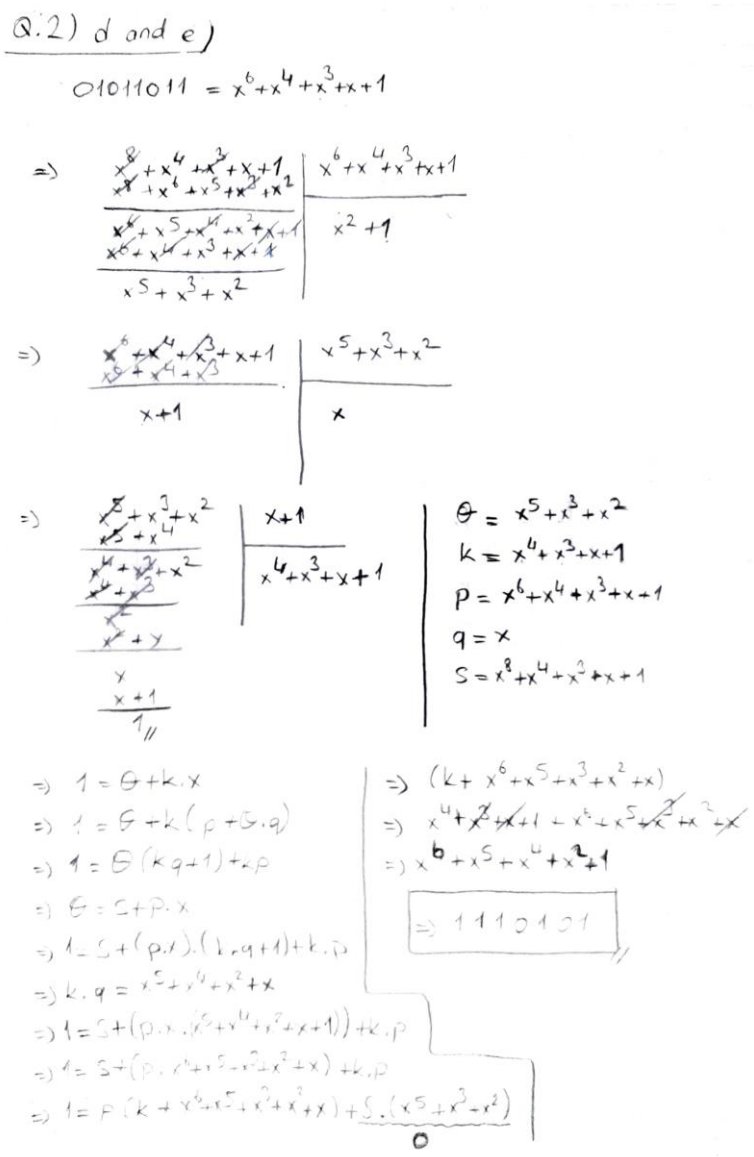
Student No: 180209801

Department: Software Engineering

ANSWERS

Q2)

a) 80209801 (mod2) = 00001001
b) Row number = 82 = 01010010
c) 00001001 (XOR) 01010010 = 01011011
d)
and
e)



Q3)

a)

- ⇨ p = 557
- ⇨ 557 is prime

for 558;

- ⇨ $2 * 3^2 * 31 = 558$
- ⇨ **A** = 558 / 2 = 279
- ⇨ **B** = 558 / 3 = 186
- ⇨ **C** = 558 / 31 = 18

```
import math
arr = []
i = 2
count = 0

while (i<557):
    if (pow(i,279)%557!=1):
        if (pow(i,186)%557!=1):
            if (pow(i,18)%557!=1):
                arr.append(i)
                count+=1
    i += 1

print(arr)
print("557 has", count, "primitive roots")
```

```
[2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38,
 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64, 65, 66, 67, 68, 69, 70, 71, 72, 73,
 74, 75, 76, 77, 78, 79, 80, 81, 82, 83, 84, 85, 86, 87, 88, 89, 90, 91, 92, 93, 94, 95, 96, 97, 98, 99, 100, 101, 102, 103, 104, 105, 106,
107, 108, 109, 110, 111, 112, 113, 114, 115, 116, 117, 118, 119, 120, 121, 122, 123, 124, 125, 126, 127, 128, 129, 130, 131, 132, 133, 134,
135, 136, 137, 138, 139, 140, 141, 142, 143, 144, 145, 146, 147, 148, 149, 150, 151, 152, 153, 154, 155, 156, 157, 158, 159, 160, 161, 162,
163, 164, 165, 166, 167, 168, 169, 170, 171, 172, 173, 174, 175, 176, 177, 178, 179, 180, 181, 182, 183, 184, 185, 186, 187, 188, 189, 190,
191, 192, 193, 194, 195, 196, 197, 198, 199, 200, 201, 202, 203, 204, 205, 206, 207, 208, 209, 210, 211, 212, 213, 214, 215, 216, 217, 218,
219, 220, 221, 222, 223, 224, 225, 226, 227, 228, 229, 230, 231, 232, 233, 234, 235, 236, 237, 238, 239, 240, 241, 242, 243, 244, 245, 246,
247, 248, 249, 250, 251, 252, 253, 254, 255, 256, 257, 258, 259, 260, 261, 262, 263, 264, 265, 266, 267, 268, 269, 270, 271, 272, 273, 274,
275, 276, 277, 278, 279, 280, 281, 282, 283, 284, 285, 286, 287, 288, 289, 290, 291, 292, 293, 294, 295, 296, 297, 298, 299, 300, 301, 302,
303, 304, 305, 306, 307, 308, 309, 310, 311, 312, 313, 314, 315, 316, 317, 318, 319, 320, 321, 322, 323, 324, 325, 326, 327, 328, 329, 330,
331, 332, 333, 334, 335, 336, 337, 338, 339, 340, 341, 342, 343, 344, 345, 346, 347, 348, 349, 350, 351, 352, 353, 354, 355, 356, 357, 358,
359, 360, 361, 362, 363, 364, 365, 366, 367, 368, 369, 370, 371, 372, 373, 374, 375, 376, 377, 378, 379, 380, 381, 382, 383, 384, 385, 386,
387, 388, 389, 390, 391, 392, 393, 394, 395, 396, 397, 398, 399, 400, 401, 402, 403, 404, 405, 406, 407, 408, 409, 410, 411, 412, 413, 414,
415, 416, 417, 418, 419, 420, 421, 422, 423, 424, 425, 426, 427, 428, 429, 430, 431, 432, 433, 434, 435, 436, 437, 438, 439, 440, 441, 442,
443, 444, 445, 446, 447, 448, 449, 450, 451, 452, 453, 454, 455, 456, 457, 458, 459, 460, 461, 462, 463, 464, 465, 466, 467, 468, 469, 470,
471, 472, 473, 474, 475, 476, 477, 478, 479, 480, 481, 482, 483, 484, 485, 486, 487, 488, 489, 490, 491, 492, 493, 494, 495, 496, 497, 498,
499, 500, 501, 502, 503, 504, 505, 506, 507, 508, 509, 510, 511, 512, 513, 514, 515, 516, 517, 518, 519, 520, 521, 522, 523, 524, 525, 526,
527, 528, 529, 530, 531, 532, 533, 534, 535, 536, 537, 538, 539, 540, 541, 542, 543, 544, 545, 546, 547, 548, 549, 550, 551, 552, 553, 554,
555]
557 has 554 primitive roots
```

for 556;

- ⇨ $2^2 * 139 = 556$
- ⇨ **A** = 556 / 2 = 278
- ⇨ **B** = 556 / 139 = 4

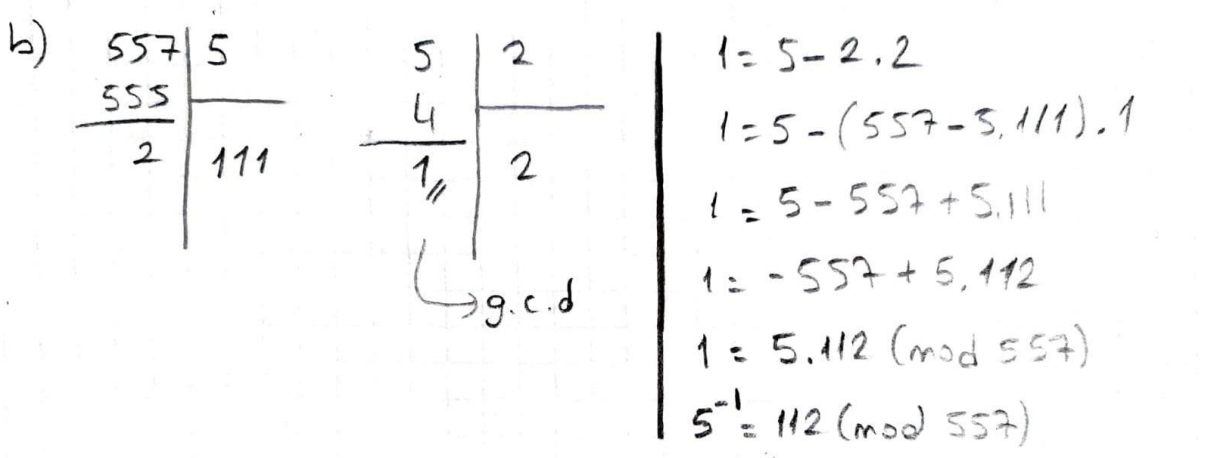
```
import math
arr = []
i = 2
count = 0

while (i<557):
    if (pow(i,278)%557!=1):
        if (pow(i,4)%557!=1):
                arr.append(i)
                count+=1
    i += 1

print(arr)
print("557 has", count, "primitive roots")
```

```
[2, 3, 5, 8, 11, 12, 13, 14, 18, 20, 21, 23, 27, 30, 31, 32, 34, 35, 37, 38, 41, 44, 45, 47, 48, 50, 51, 52, 53, 56,
57, 58, 61, 66, 72, 75, 77, 78, 80, 84, 85, 86, 87, 89, 91, 92, 95, 98, 99, 103, 107, 108, 110, 117, 120, 124, 125, 1
26, 128, 129, 130, 134, 136, 138, 140, 142, 145, 146, 147, 148, 151, 152, 158, 161, 162, 163, 164, 165, 166, 176, 177
, 180, 186, 187, 188, 189, 191, 192, 193, 194, 195, 199, 200, 201, 202, 204, 207, 208, 209, 210, 211, 212, 213, 215,
217, 218, 219, 221, 222, 223, 224, 226, 228, 230, 232, 237, 238, 239, 242, 243, 244, 245, 246, 247, 249, 251, 254, 25
7, 259, 262, 264, 266, 269, 270, 271, 274, 275, 278, 279, 282, 283, 286, 287, 288, 291, 293, 295, 298, 300, 303, 306,
 308, 310, 311, 312, 313, 314, 315, 318, 319, 320, 325, 327, 329, 331, 333, 334, 335, 336, 338, 339, 340, 342, 344, 3
45, 346, 347, 348, 349, 350, 353, 355, 356, 357, 358, 362, 363, 364, 365, 366, 368, 369, 370, 371, 377, 380, 381, 391
, 392, 393, 394, 395, 396, 399, 405, 406, 409, 410, 411, 412, 415, 417, 419, 421, 423, 427, 428, 429, 431, 432, 433,
437, 440, 447, 449, 450, 454, 458, 459, 462, 465, 466, 468, 470, 471, 472, 473, 477, 479, 480, 482, 485, 491, 496, 49
9, 500, 501, 504, 505, 506, 507, 509, 510, 512, 513, 516, 519, 520, 522, 523, 525, 526, 527, 530, 534, 536, 537, 539,
 543, 544, 545, 546, 549, 552, 554, 555]
557 has 276 primitive roots
```

b)



Q4)

a)

⇨ 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

```
import math
arr = []
i = 2
count = 0

while (i<571):
    if (pow(i,285)%557!=1):
         if (pow(i,190)%557!=1):
            if (pow(i,114)%557!=1):
                   if (pow(i,30)%557!=1):
                        arr.append(i)
                        count+=1
    i += 1

print(arr)
print("570 has", count, "primitive roots")
```

```
[2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32,
33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 6
2, 63, 64, 65, 66, 67, 68, 69, 70, 71, 72, 73, 74, 75, 76, 77, 78, 79, 80, 81, 82, 83, 84, 85, 86, 87, 88, 89, 90, 91
, 92, 93, 94, 95, 96, 97, 98, 99, 100, 101, 102, 103, 104, 105, 106, 107, 108, 109, 110, 111, 112, 113, 114, 115, 116
, 117, 118, 119, 120, 121, 122, 123, 124, 125, 126, 127, 128, 129, 130, 131, 132, 133, 134, 135, 136, 137, 138, 139,
140, 141, 142, 143, 144, 145, 146, 147, 148, 149, 150, 151, 152, 153, 154, 155, 156, 157, 158, 159, 160, 161, 162, 16
3, 164, 165, 166, 167, 168, 169, 170, 171, 172, 173, 174, 175, 176, 177, 178, 179, 180, 181, 182, 183, 184, 185, 186,
 187, 188, 189, 190, 191, 192, 193, 194, 195, 196, 197, 198, 199, 200, 201, 202, 203, 204, 205, 206, 207, 208, 209, 2
10, 211, 212, 213, 214, 215, 216, 217, 218, 219, 220, 221, 222, 223, 224, 225, 226, 227, 228, 229, 230, 231, 232, 233
, 234, 235, 236, 237, 238, 239, 240, 241, 242, 243, 244, 245, 246, 247, 248, 249, 250, 251, 252, 253, 254, 255, 256,
257, 258, 259, 260, 261, 262, 263, 264, 265, 266, 267, 268, 269, 270, 271, 272, 273, 274, 275, 276, 277, 278, 279, 28
0, 281, 282, 283, 284, 285, 286, 287, 288, 289, 290, 291, 292, 293, 294, 295, 296, 297, 298, 299, 300, 301, 302, 303,
 304, 305, 306, 307, 308, 309, 310, 311, 312, 313, 314, 315, 316, 317, 318, 319, 320, 321, 322, 323, 324, 325, 326, 3
27, 328, 329, 330, 331, 332, 333, 334, 335, 336, 337, 338, 339, 340, 341, 342, 343, 344, 345, 346, 347, 348, 349, 350
, 351, 352, 353, 354, 355, 356, 357, 358, 359, 360, 361, 362, 363, 364, 365, 366, 367, 368, 369, 370, 371, 372, 373,
374, 375, 376, 377, 378, 379, 380, 381, 382, 383, 384, 385, 386, 387, 388, 389, 390, 391, 392, 393, 394, 395, 396, 39
7, 398, 399, 400, 401, 402, 403, 404, 405, 406, 407, 408, 409, 410, 411, 412, 413, 414, 415, 416, 417, 418, 419, 420,
 421, 422, 423, 424, 425, 426, 427, 428, 429, 430, 431, 432, 433, 434, 435, 436, 437, 438, 439, 440, 441, 442, 443, 4
44, 445, 446, 447, 448, 449, 450, 451, 452, 453, 454, 455, 456, 457, 458, 459, 460, 461, 462, 463, 464, 465, 466, 467
, 468, 469, 470, 471, 472, 473, 474, 475, 476, 477, 478, 479, 480, 481, 482, 483, 484, 485, 486, 487, 488, 489, 490,
491, 492, 493, 494, 495, 496, 497, 498, 499, 500, 501, 502, 503, 504, 505, 506, 507, 508, 509, 510, 511, 512, 513, 51
4, 515, 516, 517, 518, 519, 520, 521, 522, 523, 524, 525, 526, 527, 528, 529, 530, 531, 532, 533, 534, 535, 536, 537,
 538, 539, 540, 541, 542, 543, 544, 545, 546, 547, 548, 549, 550, 551, 552, 553, 554, 555, 557, 559, 560, 561, 562, 5
63, 564, 565, 566, 567, 568, 569, 570]
570 has 567 primitive roots
```

for 572;

⇨ 2^2 * 11 * 13 = 572

⇨ **A** = 572 / 2 = 286

⇨ **B** = 572 / 11 = 52

⇨ **C** = 572 / 13 = 44

```python
import math
arr = []
i = 2
count = 0

while (i<571):
    if (pow(i,286)%557!=1):
        if (pow(i,52)%557!=1):
            if (pow(i,44)%557!=1):
                arr.append(i)
                count+=1
    i += 1

print(arr)
print("570 has", count, "primitive roots")
```

```
[2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32,
33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 6
2, 63, 64, 65, 66, 67, 68, 69, 70, 71, 72, 73, 74, 75, 76, 77, 78, 79, 80, 81, 82, 83, 84, 85, 86, 87, 88, 89, 90, 91
, 92, 93, 94, 95, 96, 97, 98, 99, 100, 101, 102, 103, 104, 105, 106, 107, 108, 109, 110, 111, 112, 113, 114, 115, 116
, 117, 119, 120, 121, 122, 123, 124, 125, 126, 127, 128, 129, 130, 131, 132, 133, 134, 135, 136, 137, 138, 139, 140,
141, 142, 143, 144, 145, 146, 147, 148, 149, 150, 151, 152, 153, 154, 155, 156, 157, 158, 159, 160, 161, 162, 163, 16
4, 165, 166, 167, 168, 169, 170, 171, 172, 173, 174, 175, 176, 177, 178, 179, 180, 181, 182, 183, 184, 185, 186, 187,
 188, 189, 190, 191, 192, 193, 194, 195, 196, 197, 198, 199, 200, 201, 202, 203, 204, 205, 206, 207, 208, 209, 210, 2
11, 212, 213, 214, 215, 216, 217, 218, 219, 220, 221, 222, 223, 224, 225, 226, 227, 228, 229, 230, 231, 232, 233, 234
, 235, 236, 237, 238, 239, 240, 241, 242, 243, 244, 245, 246, 247, 248, 249, 250, 251, 252, 253, 254, 255, 256, 257,
258, 259, 260, 261, 262, 263, 264, 265, 266, 267, 268, 269, 270, 271, 272, 273, 274, 275, 276, 277, 278, 279, 280, 28
1, 282, 283, 284, 285, 286, 287, 288, 289, 290, 291, 292, 293, 294, 295, 296, 297, 298, 299, 300, 301, 302, 303, 304,
 305, 306, 307, 308, 309, 310, 311, 312, 313, 314, 315, 316, 317, 318, 319, 320, 321, 322, 323, 324, 325, 326, 327, 3
28, 329, 330, 331, 332, 333, 334, 335, 336, 337, 338, 339, 340, 341, 342, 343, 344, 345, 346, 347, 348, 349, 350, 351
, 352, 353, 354, 355, 356, 357, 358, 359, 360, 361, 362, 363, 364, 365, 366, 367, 368, 369, 370, 371, 372, 373, 374,
375, 376, 377, 378, 379, 380, 381, 382, 383, 384, 385, 386, 387, 388, 389, 390, 391, 392, 393, 394, 395, 396, 397, 39
8, 399, 400, 401, 402, 403, 404, 405, 406, 407, 408, 409, 410, 411, 412, 413, 414, 415, 416, 417, 418, 419, 420, 421,
 422, 423, 424, 425, 426, 427, 428, 429, 430, 431, 432, 433, 434, 435, 436, 437, 438, 440, 441, 442, 443, 444, 445, 4
46, 447, 448, 449, 450, 451, 452, 453, 454, 455, 456, 457, 458, 459, 460, 461, 462, 463, 464, 465, 466, 467, 468, 469
, 470, 471, 472, 473, 474, 475, 476, 477, 478, 479, 480, 481, 482, 483, 484, 485, 486, 487, 488, 489, 490, 491, 492,
493, 494, 495, 496, 497, 498, 499, 500, 501, 502, 503, 504, 505, 506, 507, 508, 509, 510, 511, 512, 513, 514, 515, 51
6, 517, 518, 519, 520, 521, 522, 523, 524, 525, 526, 527, 528, 529, 530, 531, 532, 533, 534, 535, 536, 537, 538, 539,
 540, 541, 542, 543, 544, 545, 546, 547, 548, 549, 550, 551, 552, 553, 554, 555, 557, 559, 560, 561, 562, 563, 564, 5
65, 566, 567, 568, 569, 570]
572 has 565 primitive roots
```

b)

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: $x = (7^{32} \bmod 571) = 377$
- ⇨ Bob: $y = (7^{64} \bmod 571) = 521$

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 = $(521^{32} \bmod 571)$ = 182

keyBob = $(377^{64} \bmod 571)$ = 182

Step 7 → 182 is the shared secret.

My code:

```
import math

x = int(input("number 1: "))
y = int(input("number 2: "))

sol = pow(x,y)
z = int(input("mod: "))

final = sol %  z

print(final)
```

Alice

```
number 1: 7
number 2: 32
mod: 571
377
```

keyAlice

```
number 1: 521
number 2: 32
mod: 571
182
```

Bob

```
number 1: 7
number 2: 64
mod: 571
521
```

keyBob

```
number 1: 377
number 2: 64
mod: 571
182
```

c) I used the code I gave in option b.

a = 7, q = 571

- ⇨ $a^{-1} = a^{q-2} \pmod q$
- ⇨ $7^{-1} = 7^{569} \pmod{571}$
- ⇨ 408

```
number 1: 7
number 2: 569
mod: 571
408
```