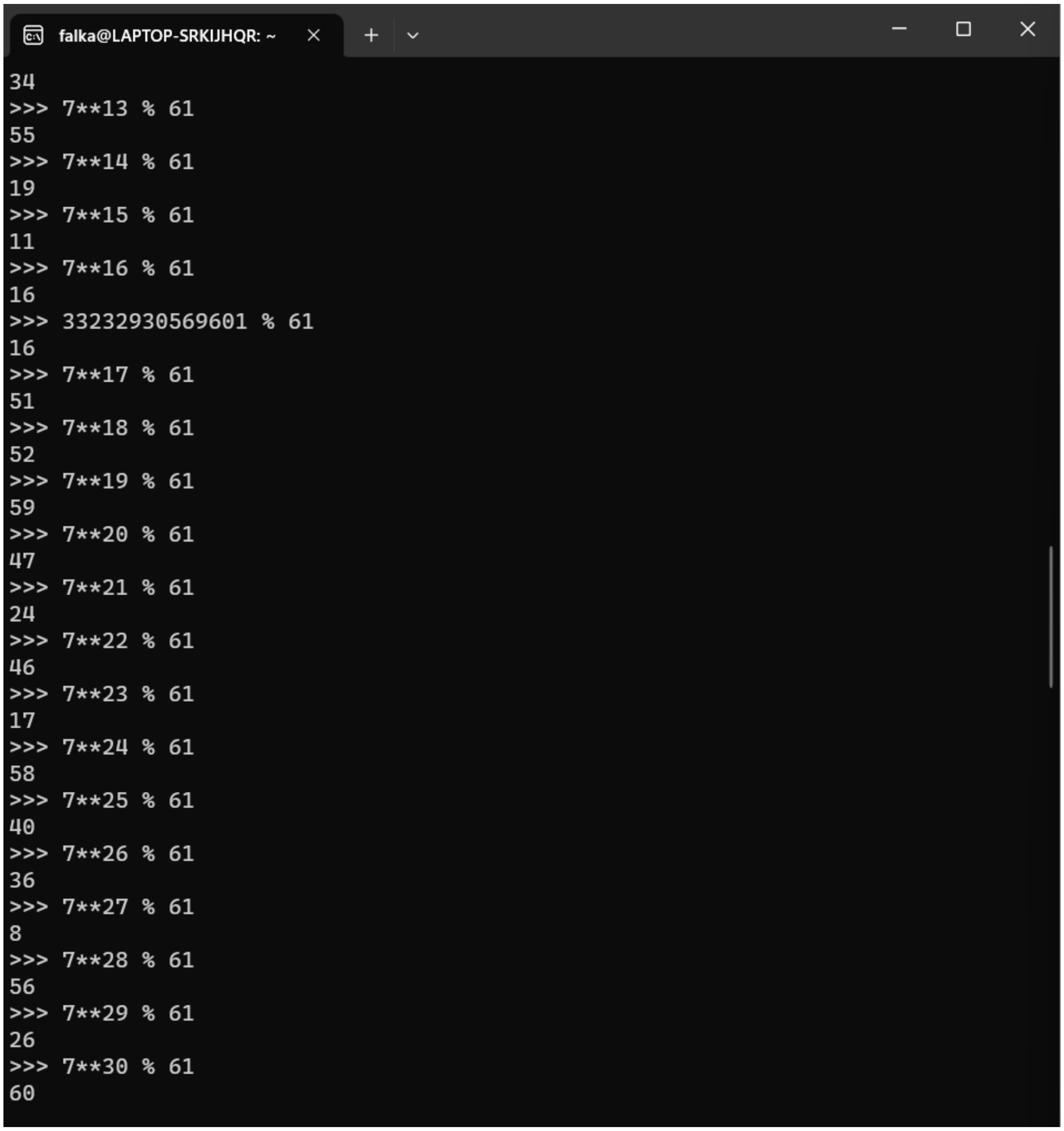
Alex Falk

Diffie-Hellman

1. K = 6
2. We are given g, p, A, B, and the equations A = g^a mod p, B = g^b mod p, K = B^a mod p and K = A^b mod p. We are trying to find Alice or Bob’s secret numbers (a and b). Either one of these will let us get K (I found both just to be sure I had the right K). First, we are trying to solve 1 of 2 equations: A = g^a mod p ⇒ 30 = 7^a mod 61 OR B = g^b mod p ⇒ 30 = 7^b mod 61. To do this, I brute forced it in Ubuntu. I checked 7 to every power mod 61 until the result equalled 30 or 17. Pictured below is a snippet of this effort. I found b = 23 and a = 41. Plugging either of these values (and the other values) into the expressions above for K gives 6.
   K = 17^41 mod 61 = 6 AND K = 30^23 mod 61 = 6

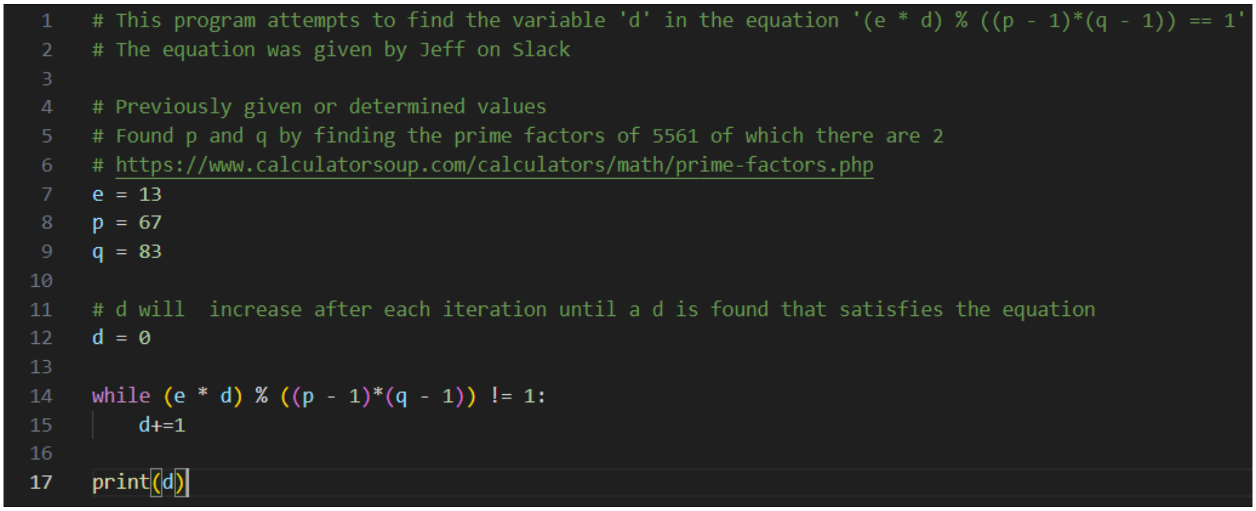


```
34
>>> 7**13 % 61
55
>>> 7**14 % 61
19
>>> 7**15 % 61
11
>>> 7**16 % 61
16
>>> 33232930569601 % 61
16
>>> 7**17 % 61
51
>>> 7**18 % 61
52
>>> 7**19 % 61
59
>>> 7**20 % 61
47
>>> 7**21 % 61
24
>>> 7**22 % 61
46
>>> 7**23 % 61
17
>>> 7**24 % 61
58
>>> 7**25 % 61
40
>>> 7**26 % 61
36
>>> 7**27 % 61
8
>>> 7**28 % 61
56
>>> 7**29 % 61
26
>>> 7**30 % 61
60
```

3. If the integers had been much larger, then it would have been impossible to do the work that I brute forced. That is, it would have been impossible to find a or b. There simply is not enough computing power on the earth to brute force that calculation.

RSA

1. Hey Bob. It's even worse than we thought! Your pal, Alice. https://www.schneier.com/blog/archives/2022/04/airtags-are-used-for-stalking-far-more-than-previously-reported.html
2. We are given Bob's e = 13 and n = 5561. Eventually, we need to find 'd' to satisfy the equation ed = 1 mod (p-1)(q-1). Why? Because d is required for the decoding of Alice's message. First, we focus on p and q. n=pq. We know that p and q are primes. Therefore, p and q can be found by finding the prime factorization of n. I used an online source to find this answer. It is cited in the screenshot of the code below. We find that p = 67 and q = 83 (It doesn't matter which is which). The code below demonstrates how I found that d = 1249. It should be noted that ed = 1 mod (p-1)(q-1) and the equation used below are in some way the same even though the notation is different. Jeff explained this in his slack message. Now that we know d, we can decode Alice's message using x to represent the integers listed on the assignment page and the equation x^d mod n. To translate each integer into the new integer I brute forced it. Proof is in a screenshot below. I compared the resulting integers to an ASCII table to find each corresponding symbol. The result was Alice's message to Bob



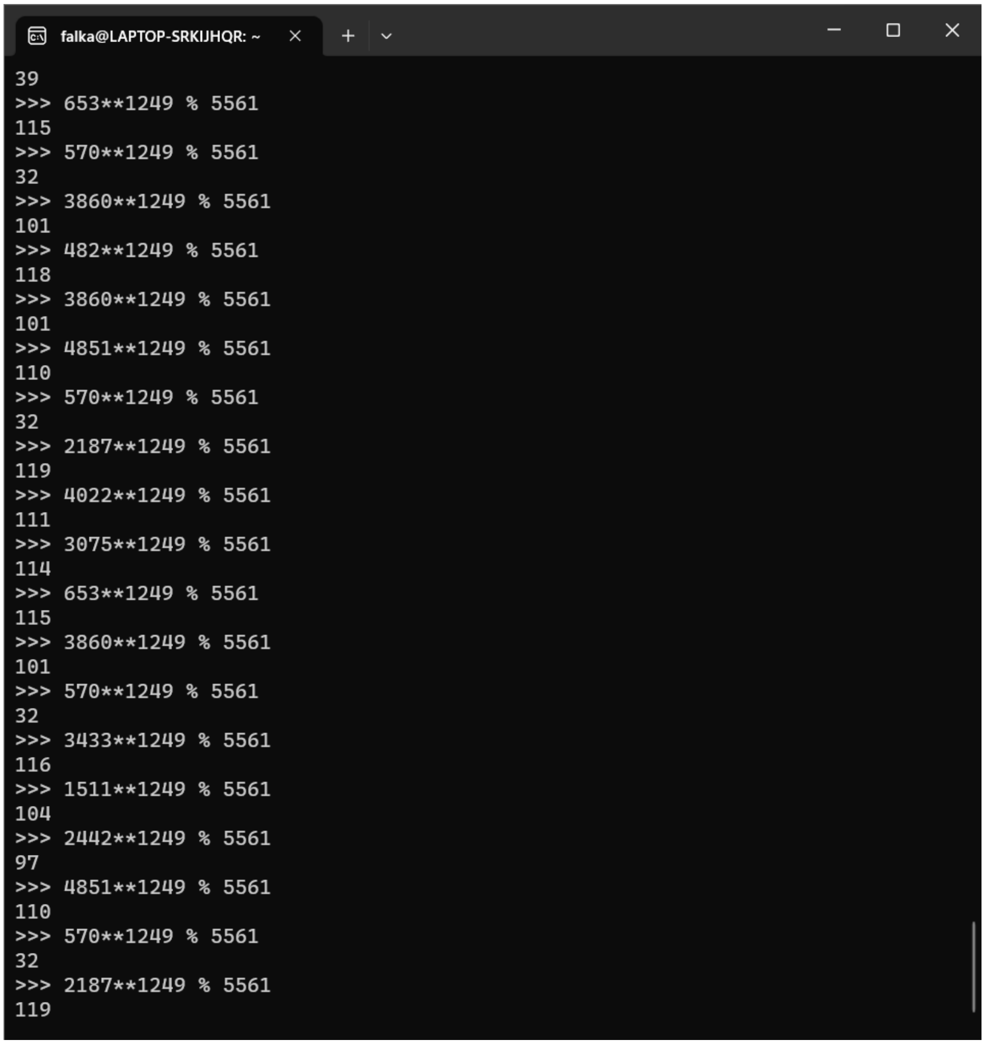
```
# This program attempts to find the variable 'd' in the equation '(e * d) % ((p - 1)*(q - 1)) == 1'
# The equation was given by Jeff on Slack

# Previously given or determined values
# Found p and q by finding the prime factors of 5561 of which there are 2
# https://www.calculatorsoup.com/calculators/math/prime-factors.php
e = 13
p = 67
q = 83

# d will  increase after each iteration until a d is found that satisfies the equation
d = 0

while (e * d) % ((p - 1)*(q - 1)) != 1:
    d+=1

print(d)
```



```
39
>>> 653**1249 % 5561
115
>>> 570**1249 % 5561
32
>>> 3860**1249 % 5561
101
>>> 482**1249 % 5561
118
>>> 3860**1249 % 5561
101
>>> 4851**1249 % 5561
110
>>> 570**1249 % 5561
32
>>> 2187**1249 % 5561
119
>>> 4022**1249 % 5561
111
>>> 3075**1249 % 5561
114
>>> 653**1249 % 5561
115
>>> 3860**1249 % 5561
101
>>> 570**1249 % 5561
32
>>> 3433**1249 % 5561
116
>>> 1511**1249 % 5561
104
>>> 2442**1249 % 5561
97
>>> 4851**1249 % 5561
110
>>> 570**1249 % 5561
32
>>> 2187**1249 % 5561
119
```

3. ed = 1 mod (p-1)(q-1) is not calculable when the values are too high. It requires too much computing power.
4. Eve is encrypting her message one letter at a time. This is insecure because the code can be broken “using letter frequencies and a dictionary” (https://cs.carleton.edu/faculty/jondich/courses/cs338_f23/assignments/07-lab-dh-and-rsa.html). This renders the encrypting method obsolete.

SCRATCH WORK

Hey Bob. It's even worse than we thought! Your pal, Alice.
https://www.schneier.com/blog/archives/2022/04/airtags-are-used-for-stalking-far-more-than-previously-reported.html

72 101 121 32 66 111 98 46 32 73 116 39 115 32 101 118 101 110 32 119 111 114 115 101 32 116 104 97 110 32 119 101 32 116 104 111 117 103 104 116 33 32 89 111 117 114 32 112 97 108 44 32 65 108 105 99 101 46 32 104 116 116 112 115 58 47 47 119 119 119 46 115 99 104 110 101 105 101 114 46 99 111 109 47 98 108 111 103 47 97 114 99 104 105 118 101 115 47

50 48 50 50 47 48 52 47 97 105 114 116 97 103 115 45 97 114 101 45 117 115 101 100 45 102 111 114 45 115 116 97 108 107 105 110 103 45 102 97 114 45 109 111 114 101 45 116 104 97 110 45 112 114 101 118 105 111 117 115 108 121 45 114 101 112 111 114 116 101 100 46 104 116 109 108