Joshua Grossman

Diffie-Hellman

1. The secret number is 6.
2. We are given g,p,A,B, and A = g^a mod p, B = g^b mod p, K = B^a mod p and K = A^b mob p. We need to solve at least one set of the equations. A = g^a mod p -> 30 = 7^a mod 61 OR B = g^b mod p -> 30 = 7^b mod 61. After brute forcing values in the software of your choice (or by hand but oh boy), one arrives at b = 23 and a = 41. Plugging either in for K yields 6 as the answer.
3. If the integers were much larger, it would have been impossible to brute force and find an a or b. A similar problem to running an algorithm to prove fermat's last theorem, it would simply take too much power and too much time.

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. We need to find d to satisfy the equation ed = 1 mod (p-1)(q-1) because d is required to decode Alice's message. We know that p and q are primes and therefore we can find p and q through the prime factorization of n. For 5561, we find that 67 and 83 are prime factors of 5561, and assign them respectively.

   Running the program below, we find that d = 1249. Now that we have d, we decode Alice's message using x to represent the integers listed on the assignment page and the equation x^d mod n.

   Users > joshuagrossman > Desktop > FolderILike > discrete-dynamical-systems > eee.py >

```python
e = 13
p = 67
q = 83

d = 0

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

print(d)
```

From here, I used an ascii table and translated each value, such as 653*1249 % 5561 = 115, and used an ASCII table, to translate the message.

3. Ed = 1 mod (p-1)(q-1) is incalculable when values are too high because it requires too much computing power.
4. Alice encrypted her message one letter at a time, which is insecure because a code such as this will be broken be using letter frequencies and a dictionary. This means that this encryption method is useless