BEING EVE

Author: Sydney Nguyen

Diffie Hellman:

Given Information

- Alice and Bob agree on $g = 11$ and $p = 59$.
- Alice sent Bob the number 57.
- Bob sent Alice the number 44.

First I will begin by defining a few variables that will be used in multiple equations.

X = Alice's private integer
Y = Bob's private integer
K = Shared key between the two

We know the following information regarding the keys.

$$x \,\&\, y < p$$
$$57 = 11^{x} \bmod 59$$
$$44 = 11^{y} \bmod 59$$

I then simply just made a loop in python

```
for i in range(0,59):
        if (((11**i) % 59) == 57):
                print( i )
```

```
for f in range(0,59):
        if (((11**f) % 59) == 44):
                print( f )
```

Output:

```
36
15
```

Now that we have these values we will input them into the shared equations:

$$44^{i} \bmod 59 \qquad i = 36$$
$$57^{f} \bmod 59 \qquad i = 15$$

Both these equations give us the value or shared key of 36. It is important to note that there is a major downfall in this strategy. To find the i and f values we had to loop through all numbers from 0 to 59. Our algorithm is O(2n) since there are two for loops and it is a very inefficient algorithm since it is necessary to go through all numbers to find an important piece of information. It wouldn't necessarily work for finding the integer, but by the time the integer is found the information and keys may have changed.

RSA:

Given Information

- Bob's public key - $(e_b n_b) = (13, 5561)$

Since we are attempting to decrypt the message between Alice and Bob I need to calculate the private key of one of the two and since we are given Bob's public key we must solve for his private key which can be represented as $(d_b n_b)$. To solve for d_b we are given all the necessary information to solve for d_b.

$$e_b d_b \text{ mod } \lambda(n_b) = 1$$
$$\lambda(n_b) \ = \text{lcm}(\ p\text{-}1,\ q\text{-}1)$$

To solve for the factors of 5561 I plugged it into WolframAlpha which gave the 67 and 83. We then can plug these values into the second equation listed above to get the value 2706. We now have all variables to solve for d_b.

$$13 d_b \text{ mod } 2706 = 1$$

Again utilizing the wonderful WolframAlpha I am given the formula:

$$x = 2706n + 1249$$

Plugging in n = 0 we get $d_b = 1249$. Now that I have the key to decrypt the text I placed the secret message into an array. I then plugged each value into the equation x^{13}mod5561 and then plugged the values into an ASCII table to get this message:

> 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

An area to pay attention to is when solving for n_b one must factor the integer into two large prime numbers that may give many options for prime numbers. We then would have to use all pairs and solve and check to see if the integers allow us to solve for the private key of the message. It is also important to note that the encoding is insecure because it encodes characters one at a time. It could also be simply broken similarly to the substitution cipher by taking note of numbers that appear often that also appear often in the language text and solving with the simple patterns of text.

Citation:

https://cs.carleton.edu/faculty/jondich/courses/cs338_s22/assignments/07-lab-dh-and-rsa.html

https://www.wolframalpha.com/