Q1 Suppose that $p = 29$; find a generator g for such a p, and then simulate a Diffie-Hellman key exchange with a and b selected at random. Specify what is the final key that Alice and Bob share.

Q2 Suppose that Eve has the power to intercept and modify all the messages that are exchanged between Alice and Bob. Suppose that $p = 29$ as before, and use the generator g from the previous question. Suppose that $a = 5$ and $b = 7$; demonstrate how Eve can mount a "Man-in-the-Middle" attack again Alice and Bob.

Programming Problem Implement in Python (2.7) In homework 5 you developed a rolling checksum procedure. You are going to build on that project for this assignment.

You are going to implement the ElGamal signature scheme. Your program is going to be run as follows:

```
python elg -p 11 -g 6 -a 3 -k 7 <message>
```

Your program is going to run your rolling checksum, and it is going to compute the sum of all the values modulo the prime p (in the above example, 11). Thus $h(\text{message}) = x$ where x is the sum of all the rolling checksums of "message" modulo p.

And then your program will compute the ElGamal signature, for example:

$$m = \texttt{A message.} \quad h(m) = 5 \quad p = 11 \quad g = 6 \quad a = 3 \quad k = 7$$

the signature of 'A message.' will be:

$$\begin{aligned} r &= 6^7 \pmod{11} = 8 \\ s &= 7^{-1}(5 - 3 \cdot 8) \pmod{(11 - 1)} \\ &= 3 \cdot (-19) \pmod{10} = 3 \cdot 1 \pmod{10} = 3 \end{aligned}$$

i.e., sign(A message.) $= (8, 3)$.

Finally, your program will output m' which with the original message, with the signature (pair of numbers) appended at the end.

Provide two message m_1, m_2 that in your scheme get the same signature (under the same p, g, a, k).