Feel free to use Mathematical to help with calculations

1. Bob's public RSA key is $(285869, 7)$.
   Your RSA values are $p = 521, q = 571, e = 11$ so that your public key is $(297491, 11)$.
   (a) You receive the following from Bob. Which messages, if any, have valid RSA signatures?
   $(x, s) = (132136, 184316)$
   $(x, s) = (132136, 176860)$
   $(x, s) = (221821, 250076)$

   (b) Suppose you want to send the message $x = 34372$ to Bob.
   Encrypt it using Bob's public RSA key and sign it using your RSA values.
   What do you send to Bob?

2. The RSA digital signature that we've described is subject to an *existential forgery* attack by Oscar using only your public key. Here is how it works:

   Oscar picks a random signature $s < n$ and computes the plaintext $x \equiv s^e \mod n$

   Oscar sends (x, s) to Bob, claiming to be you.

   Implement this attack using your public key from #1:

   (a) If Oscar picks $s = 137421$, compute the corresponding plaintext x.
   (b) What will Oscar send to Bob?
   (c) What happens when Bob verifies the signature?
   (d) Explain why this example doesn't mean that Oscar can forge *any* message from you.

3. Suppose you want to implement RSA with a 1024-bit key n.
   This means you will need to find 512-bit primes p, q.

   (a) Approximately how many 512-bit primes are there?
   (b) If you choose a 512-bit number at random, what is the probability that it is prime? (We'll see some tests for primality next semester.)
   (c) How many 512-bit numbers would you expect to choose before finding a prime?