crypto pkc handout: show all work

1. Convert decimal 97 to binary:

   Convert binary `0b 111011` to decimal:

2. • Find the exponent e such that the number printed equals a^e.
   • Shuffle the code so that the number printed equals a^{19}.
   • How many lines of similar code are needed if e has 500 decimal digits? Hint: converting from decimal to binary increases digits by a factor of $\lg(10) \approx 10/3$.

```
x = 1
x = x*x*a
x = x*x*a
x = x*x
x = x*x
x = x*x*a
print x
```

3. Alice and Bob use DHM and email to create a secret key. Give an example of their first email exchange.

   Assume they use base 7 and modulus 11, Bob's secret exponent is 3, and Alice's secret exponent is unknown. What number does Bob send Alice?

   Alice sends Bob the number 4. What secret key do Bob and Alice create?

   You are Eve. Find Alice's exponent. Find Alice and Bob's secret key.

4. Let x, y, n be 1234567809, 12345, 9087654321. My laptop can perform 1 64-bit integer mod operation in 1 microsecond. Estimate the number of seconds needed for each of the following.

   find $x^y (\mod n)$

   find t such that $x^t = 2672633475(\mod n)$

5. Alice's RSA key has $n = 77$ and $e = 7$. Bob encrypts secret message $m = 9$ and sends it to Alice. Eve wants to find m.

   What number β does Bob send Alice?

   Can Eve see β?

   How does Alice recover m from β?

   Show that the number that Alice computes is equal to m.

   How does Eve find m?

   For real world RSA, how long would it take Eve to find m?