Math 4981 Spring 2021
Cryptography HW 6
Due Thursday, February 25

1. Consider the text seven-character text `Go now!`

   (a) Use the ASCII table to encode this as a string of seven decimal (base 10) numbers.

   (b) Encode the text as a string of 56 binary digits.

   (c) Encode it as a single decimal number.

   You may use a calculator, but show the steps and reasoning you followed for each of these calculations.

2. You may use a calculator, but show your steps and reasoning for each of these calculations.

   (a) The string `01001100 01100101 01110100 00100111 01110011 00100000 01100111 01101111 00100001` is an ASCII encoding. Determine the original message.

   (b) The decimal number `1017612308680749037850` encodes a message in ASCII. Decode it.

3. Suppose you are doing a Diffie-Hellman key exchange with Alice. You have agreed to use $p = 1373, g = 2$.

   (a) You choose the secret value $b = 871$. What number should you send to Alice?

   (b) Alice sends you $A = 974$. What is the secret shared key?
   (I recommend using Wolfram Alpha or Mathematica or something similar for this one, to avoid long and tedious hand arithmetic).

4. Suppose you are doing another Diffie-Hellman key exchange, this time with Bob. You have chosen $p = 29$ and $g = 12$.

   (a) You choose the secret value $a = 11$. What number should you send to Bob?

   (b) It turns out that Bob has chosen $b = 15$. What number does he send you?

   (c) What is your shared secret?

   (d) How hard would it be for Eve to break your secret? What's unusual about this choice of g?

5. Use the efficient modular exponentiation algorithm (showing your steps) to compute $3^{51} \mod 71$.

6. Use Shanks's algorithm (showing your steps) to solve $11^x \equiv 21 \mod 71$.