Math 4981 Spring 2021
Cryptography HW 6 Solutions
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.

   Solution:

   (a) 071 111 032 110 111 119 033

   (b) 01000111 01101111 00100000 01101110 01101111 01110111 00100001

   (c) 20106908428891937

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.

   Solution:

   (a) These numbers convert to `076 101 116 039 115 032 103 111 033` in decimal and thus to `Let's go!` in text.

   (b) We can peel this apart into the binary string `00110111 00101010 00110101 00101011 00110100 00111101 00110011 00111001 00011010`. This represents the decimal string `055 042 053 043 052 061 051 057 026`, which decodes via ASCII to `7*5+4=39(eof)`.

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).

Solution:

(a) You send $g^b \equiv 2^{871} \equiv 805 \mod 1373$.

(b) The secret shared key is $B' = K \equiv A^b \equiv 974^{871} \equiv 397 \mod 1373$.

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?

Solution:

(a) You send $12^{11} \equiv 17 \mod 29$.

(b) Bob sends $12^{15} \equiv 17 \mod 29$.

(c) Your shared secret is $17^{11} \equiv 12 \mod 29$.

(d) Eve would only need to try three values to find your secret number. This is because $g = 12$ is not a primitive root, and repeats itself every fourth exponent. This means Eve will never need to try more than four numbers to break the "logarithm" problem here.

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

Solution: We compute

$$3^1 \equiv 3 \qquad 3^2 \equiv 9 \qquad 3^4 \equiv 81 \equiv 10$$
$$3^8 \equiv 100 \equiv 29 \qquad 3^{16} \equiv 841 \equiv -11 \qquad 3^{32} \equiv 121 \equiv 50$$

Then we have

$$3^{51} = 3^{32}3^{16}3^2 3^1 \equiv 50 \cdot -11 \cdot 9 \cdot 3 \equiv 50 \cdot -28 \cdot 3 \equiv 50 \cdot -13 \equiv 60 \mod 71.$$

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

Solution:

We take $n = 9$. Then we have

$$11^1 \equiv 11 \qquad 11^2 \equiv 50 \qquad 11^3 \equiv 53$$
$$11^4 \equiv 15 \qquad 11^5 \equiv 23 \qquad 11^6 \equiv 40$$
$$11^7 \equiv 14 \qquad 11^8 \equiv 12 \qquad 11^9 \equiv 61$$

and so $11^{-9} \equiv 7 \mod 71$. Now we compute

$$\begin{aligned} 21 \cdot 7 &\equiv 5 \\ 21 \cdot 7^2 &\equiv 35 \\ 21 \cdot 7^3 &\equiv 32 \\ 21 \cdot 7^4 &\equiv 11 \end{aligned}$$

and we have a match. We have $i = 1$ and $j = 4$ so $x = i + jn = 1 + 4 \cdot 9 = 37$.