Math 401 Fall 2019
Cryptology HW 5 Solutions
Due Thursday, October 3

1. Is 2 a primitive root mod 31? Prove or disprove your answer.

   Solution: $2^5 = 32 \equiv 1 \mod 31$ so 2 is not a primitive root mod 31.

2. Is 17 a primitive root mod 31? Prove or disprove your answer.

   Solution: We compute

$$\begin{array}{llll} 17 \equiv 17 \mod 31 & 17^2 \equiv 10 \mod 31 & 17^3 \equiv 15 \mod 31 & 17^4 \equiv 7 \mod 31 \\ 17^5 \equiv 26 \mod 31 & 17^6 \equiv 8 \mod 31 & 17^7 \equiv 12 \mod 31 & 17^8 \equiv 18 \mod 31 \\ 17^9 \equiv 27 \mod 31 & 17^{10} \equiv 25 \mod 31 & 17^{11} \equiv 22 \mod 31 & 17^{12} \equiv 2 \mod 31 \\ 17^{13} \equiv 3 \mod 31 & 17^{14} \equiv 20 \mod 31 & 17^{15} \equiv 30 \mod 31 & 17^{16} \equiv 14 \mod 31 \end{array}$$

   Since it hasn't repeated already, it won't, so 17 is a primitive root.

   We could in fact save ourselves some work by only checking the exponents $1, 2, 3, 5, 6, 10, 15$.

3. Compute $\log_5(17) \mod 23$ and $\log 10(22) \mod 47$.

   Solution: $\log_5(17) = 7 \mod 23$ and $\log_{10}(22) = 11 \mod 47$.

4. 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 $B' = K \equiv A^b \equiv 974^{871} \equiv 397 \mod 1373$.

5. 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.

6. From the definition of big-O notation, prove that $x^2 + \sqrt{x} = O(x^2)$.

   Solution: When $x \geq 1$, we have $\sqrt{x} \leq x^2$ so $x^2 + \sqrt{x} \leq x^2 + x^2 = 2x^2$. Thus we can take $C = 1$ and $c = 2$.

7. Prove (using the definition or the limit property) that:

   (a) $k^{300} = O(2^k)$

   (b) $(\log_2(k))^{100} = O(k)$.

   Solution:

   (a) $\lim_{k\to\infty} \frac{k^{300}}{2^k} = 0$ so $k^{300} = O(2^k)$.

   (b) $\lim_{k\to\infty} \frac{\log_2(k)^{100}}{k} = 0$ so $\log_2(k)^{100} = O(k)$.

8. 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

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

9. 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 $x = i + jn = 1 + 4 \cdot 9 = 37$.