Math 259 - Spring 2019
Homework 1

This homework is due on Monday, January 28.

1. (SRS *Cryptography*, Section 12.9 problem 1) Suppose that $p = 3701$, $q = 7537$, and Alice chooses her encryption key to be $e = 443$.

   (a) What is her decryption key d?

   (b) Bob wishes to send the plaintext message $m = 11034007$. What is his ciphertext?

   (c) Bob sends another message, and his ciphertext is $c = 3003890$. What was his plaintext message?

   This problem was mostly just to make sure you can use the computer/do the necessary computation. It is okay to briefly say what you are asking the computer to do.

2. (SRS *Cryptography*, Section 12.9 problem 2) Alice decides to use RSA to allow others to send her messages, and she chooses her modulus to be $N = pq = 3259499$. Through a breach in security, Eve discovers that $\varphi(N) = (p-1)(q-1) = 3255840$. Determine p and q without asking a computer to factor N. Show your work (but you might want to use a computer/calculator for the intermediate steps).

3. (TW *Coding Theory*, Section 6.8 problem 12) You are trying to factor $N = 642401$. Suppose you discover that
$$516107^2 \equiv 7 \pmod{N},$$
and that
$$187722^2 \equiv 2^2 \cdot 7 \pmod{N}.$$
Use this information to factor N, but do not just ask a computer to factor N. Show your work (but you again you might want to use a computer/calculator for the intermediate steps).

4. (SRS *Cryptography*, Section 12.9 problem 7) Suppose that k different RSA users all use the same small encryption exponent $e \leq k$, but different, relatively prime moduli $N_1, N_2, \ldots N_k$. Suppose that Bob encrypts for each of them the same message m, resulting in ciphertexts $c_1, c_2, \ldots, c_k$. Show that if Eve intercepts the ciphertexts, she can recover the original message. (Hint: You may assume without proof that using the Chinese Remainder Theorem, Eve can compute a number
$$c < \prod_{i=1}^{k} N_i$$
such that for each i,
$$c \equiv c_i \pmod{N_i}.)$$

5. (SRS *Cryptography*, Section 12.9 problem 5) Alice and Bob are such good friends that they choose to use RSA with the same modulus N, but they use different encryption exponents e and f, that happen to be relatively prime. Charles encrypts and sends the same message m to Alice and Bob. If Eve intercepts both of his ciphertexts, how can she recover the plaintext m? (Hint: You may assume without proof that since e and f are relatively prime, Eve can compute integers a and b with $ae + bf = 1$.)

6. (adapted from SRS *Cryptography*, Section 11.8 problem 7) Bob wishes to send Alice the message $m = 62$. Alice's DLP problem has $(p, g, h) = (73, 5, 49)$. Bob chooses $b = 33$ as his random secret exponent. What is the ciphertext pair (c_1, c_2) that he sends?

7. (adapted from TW *Coding Theory*, Section 7.6 problem 3) To show you how hard solving the discrete logarithm problem is, let $p = 1223$ and $g = 5$. Try to find a such that $5^a \equiv 3 \pmod{1223}$. For your work for this problem, just write down what you tried and how you finally got the answer.

8. Throughout this problem, let $p = 17$. In this case, 3 is a primitive root of 17. Use the properties of the discrete logarithm, and the information given if any, to compute the following. Please show your work.
   (a) $\log_3(1)$
   (b) $\log_3(3)$
   (c) $\log_3(5)$, given that $\log_3(7) \equiv 11 \pmod{16}$, $\log_3(8) \equiv 10 \pmod{16}$ and $7 \times 8 \equiv 5 \pmod{17}$
   (d) $\log_3(10)$, given that $\log_3(12) \equiv 13 \pmod{16}$ and $10 \times 12 \equiv 1 \pmod{17}$

9. Let $p = 101$. The goal of this problem will be to compute a such that $3^a \equiv 17 \pmod{101}$, using a simplified version of the index calculus attack.
   (a) We will first compute x such that $3^x \equiv 2 \pmod{101}$. We do this by following these steps:
      - Compute 2^7 and reduce your answer modulo 101.
      - Factor the new number that you obtained.
      - This should give you an equation satisfied by x. Solve this equation.
   (b) What is $17^{-1} \pmod{101}$? Compute this number and call it b.
   (c) Use that $17b \equiv 1 \pmod{101}$ to get a relationship between x from part a) and a such that $3^a \equiv 17 \pmod{101}$. Using the value of x you computed in part (a), solve this equation for a.

Extra problems for graduate credit:

1. (TW *Coding Theory*, Section 6.8, problem 19) Let $N = pq$ be the product of two distinct primes.

(a) Let k be a multiple of $\varphi(N)$. Show that if $\gcd(a, N) = 1$, then $a^k \equiv 1 \pmod p$ and $a^k \equiv 1 \pmod q$.

(b) Suppose k is as in part (a), and let a be arbitrary now (so possibly $\gcd(a, N) \neq 1$). Show that $a^{k+1} \equiv a \pmod p$ and $a^{k+1} \equiv a \pmod q$.

(c) Let e and d be encryption and decryption exponents for RSA with modulus N. Show that $a^{ed} \equiv a \pmod N$ for all a. This shows that we do not need to assume $\gcd(a, N) = 1$ in order to use RSA.

2. (SRS *Cryptography*, Section 12.9 problem 10) Suppose that $N = pq$ is a product of two primes and $\gcd(a, pq) = 1$.

   (a) Show that if $x^2 \equiv a \pmod N$ has any solutions in $\mathbb{Z}/N\mathbb{Z}$, then it has exactly four solutions.

   (b) If, for some $a \in \mathbb{Z}/N\mathbb{Z}$, you know all four solutions, show that you can quickly factor N.

3. (adapted from SRS *Cryptography*) Let p be a prime and let $g \in (\mathbb{Z}/p\mathbb{Z})^\times$.

   (a) Show that if g is a primitive root modulo p, then $\log_g(ab) \equiv \log_g(a) + \log_g(b) \pmod{p-1}$.

   (b) If g is not a primitive root, give a counterexample to part (a). Give a corrected formula that *is* true.

   (c) Again assume that g is a primitive root modulo p. Show that

      i. $\log_g(1) \equiv 0 \pmod{p-1}$ and $\log_g(g) \equiv 1 \pmod{p-1}$.

      ii. $\log_g(a^{-1}) \equiv -\log_g(a) \pmod{p-1}$ and more generally for any integer $\log_g(a^r) \equiv r\log_g(a) \pmod{p-1}$.