CSE 40622 Cryptography, Spring 2018
Written Assignment 06 (Section 1 in Lecture 15-17)

Name: **Jasmine Walker**

1. (**Hard**, 20 pts, page 4) Use Chinese Remainder Theorem to prove RSA encryption works correctly even if $\gcd(m, n) \neq 1$ where m is the message to be encrypted and n is the RSA modulus $n = pq$.

   Answer:
   Since $\gcd(m, n) \neq 1$, we can't use Euler's Theorem to make the conclusion that $m^{\varphi(n)} \equiv 1 \pmod n$. So, from the decryption of cipher c, we have $c^d \equiv m^{ed} \equiv m^{1+k\varphi(n)} \equiv m \cdot (m^{\varphi(n)})^k \pmod n$, and we must prove $m \cdot (m^{\varphi(n)})^k \equiv m \pmod n$. We apply CRT to this term:

   $$m \cdot m^{\varphi(n)k} \equiv a_1 \pmod p$$
   $$m \cdot m^{\varphi(n)k} \equiv a_2 \pmod q$$

   Since $\gcd(m, n) \neq 1$, we know that m is either divisible by p, q, or n. If m is divisible by n, then m is equal to $0 \mod n$, which will work in RSA decryption because 0 to the exponent of anything will equal 0.

   For the other cases, let's assume p is the divisor of m **without loss of generality**. If m is divisible by p, then $m \mod p = 0$ and the remainder a_1 will equal 0 no matter the exponent of m. Since p and q are prime, we can apply Proposition 1 from Lecture 15-17 to the $\mod q$ term:

   $$m \cdot m^{\varphi(n)k} \equiv m \cdot m^{\varphi(pq)k} \equiv m \cdot m^{\varphi(p)\varphi(q)k} \equiv a_2 \pmod q$$

   Because $\gcd(m, q) = 1$, we can apply Euler's Theorem to this term and get

   $$m \cdot m^{\varphi(p)\varphi(q)k} \equiv m \cdot m^{\varphi(q)(\varphi(p)k)} \equiv m \pmod q$$

   We are left with two terms,

   $$m \cdot m^{\varphi(n)k} \equiv x \equiv 0 \equiv a_1 \pmod p$$
   $$m \cdot m^{\varphi(n)k} \equiv x \equiv m \equiv a_2 \pmod q$$

   We can apply CRT's formula of x to get the value of the element in Z_n that will satisfy both these congruences:

   $$x = a_1 \cdot q \cdot q_p^{-1} + a_2 \cdot p \cdot p_q^{-1} \mod n$$

   We know that $a_1 = 0$, so the first term is nulled:

   $$x = a_2 \cdot p \cdot p_q^{-1} \mod n$$

   We also know that $p \cdot p_q^{-1}$ is equivalent to saying $p \cdot p_q^{-1} = 1 + kq$ for some integer k. So the formula is now

   $$x = a_2 \cdot p \cdot p_q^{-1} \mod n = a_2 \cdot (1 + kq) = a_2 + a_2 kq \mod n$$

   By inspection, we can see that x has a remainder a_2 if mod q is applied, and a remainder 0 if mod p is applied. CRT states there is only one unique element in $\mathbb{Z}_n$ that can satisfy both requirements, and since we know $m \mod q = a_2$ and $m \mod p = 0$ from above, we already know what it is: m. Thus, $m \cdot m^{\varphi(n)k} \equiv x \equiv m \pmod n$, so RSA will work even if $\gcd(m, n) \neq 1$.

2. (20 pts, page 7) Based on the ideas in Section 1.3.1, research (*i.e.,* by Googling) how Miller-Rabin test works, and describe the algorithm with your own language or pseudocode (only one is necessary).

Answer:
I researched this answer on Wikipedia: for an integer n and an integer $a \in \mathbb{Z}_n - \{0, 1, n-1\}$, $a^{n-1} \mod n$ must equal 1 if n is prime. The square roots of 1 must be either $1 \mod n$ or $-1 \mod n$ if n is prime. We can use these facts to our advantage in Miller-Rabin primality tests. First, $n-1$ must be factored into the form $2^s \cdot d$, where d is an odd number indivisible by 2. Then we enter into a for loop of k iterations, k being the specifier for how accurate the primality test is.

for k loops:
    x := $a^d \mod n$
    if x == 1 or x == $n-1$:
        continue
    for s - 1 loops:
        x := $x^2 \mod n$
        if x == 1:
            return ”n is not prime”
        if x == $n-1$:
            continue (back to k loops)
    return ”n is not prime”
return ”n is probably prime”

3. (**Hard**, 20 pts, page 7) If $a \in \mathbb{Z}_n$ with an RSA modulus $n = pq$ satisfies $a^{n-1} \mod n = 1$, a may be useful in factoring $n = pq$. Explain why this is so.

    - Hint: Reading Section 2.4.4 in Lecture 03-05 will be helpful.

Answer:

We can use the steps of the Miller-Rabin primality test to find the factors of $n = pq$. If we are given an a such that $a^{n-1} \mod n = 1$, we first factor $n-1$ into the form $2^s \cdot d$, d being an odd number. Then we compute $x := a^d \mod n$, and check to see if this number is congruent to $1 \mod n$ or $-1 \mod n$. If it is, it is useless. If it is not, then we square x into x^2 and check x^2 to see if it congruent to $1 \mod n$ or $-1 \mod n$. If it is not equal to either, we square it again into $x^{2 \cdot 2} \mod n$ and check it against $-1 \mod n$ or $1 \mod n$ again. If some $x^{2m} \mod n$ is found to be equal to $-1 \mod n$, then it is useless. But if there is some $x^{2m} \equiv 1 \pmod{n}$, then we can factor $n = pq$. If $x^{2m} \equiv 1 \pmod{n}$, and one if its square roots is $x^{2(m-1)}$ that is not equal to $-1 \mod n$ or $1 \mod n$, then either $x^{2(m-1)} \equiv 1 \pmod{p}$, $x^{2(m-1)} \equiv -1 \pmod{q}$ OR $x^{2(m-1)} \equiv -1 \pmod{p}$, $x^{2(m-1)} \equiv 1 \pmod{q}$, as it says in Section 2.4.4 in Lecture 03-05. Then $\gcd(x^{2(n-1)} - 1, n)$ and $\gcd(x^{2(n-1)} + 1, n)$ are the factors of n.