CSE 40622 Cryptography
Writing Assignment 07 (Lecture 16-18)

Name: Walker Bagley (wbagley)

1. (20 pts, page 4) Use Chinese Remainder Theorem to prove RSA encryption is ***correct*** when (1) $\gcd(m, n) = q$ where m is the message to be encrypted and n is the RSA modulus $n = pq$, and (2) $q < m < p$.

   - Hint: Compute $c^d \mod p$ and $c^d \mod q$ separately, then use the formula of CRT to compute $c^d \mod n$.
   - Hint 2: $q(q^{-1} \mod p)$ will be equal to 1 with modulo p. Therefore, it can be simplified as $kp + 1$ for some integer k.

   Answer:

$$
\begin{aligned}
(1)\ m^{ed} &\mod p = m^{ed-1}m \mod p \\
m^{ed} &\mod p = m^{1 \mod \varphi(n) - 1}m \mod p \\
m^{ed} &\mod p = m^{1+k(p-1)(q-1)-1}m \mod p \\
m^{ed} &\mod p = m^{k(p-1)(q-1)}m \mod p \\
m^{ed} &\mod p = (m^{(p-1)})^{k(q-1)}m \mod p \\
m^{ed} &\mod p = (m^{\varphi(p)})^{k(q-1)}m \mod p \\
m^{ed} &\mod p = 1^{k(q-1)}m \mod p \\
m^{ed} &\mod p = m \mod p \\
(2)\ m^{ed} &\mod q = (kq)^{ed} \mod q = 0^{ed} \mod q = 0 \mod q
\end{aligned}
$$

$$
\begin{aligned}
m^{ed} \mod n &= \Big[m \cdot [q^{-1} \mod p] \cdot q + 0 \cdot [p^{-1} \mod q] \cdot p\Big] \mod n \\
&= m \cdot [q^{-1} \mod p] \cdot q \mod n \\
&= m \cdot [1 \mod p] \mod n \\
&= m \cdot [jp + 1] \mod n \\
&= jp(kq) + m \mod n \\
&= jk(pq) + m \mod n \\
&= jk(n) + m \mod n \\
&= 0 + m \mod n \\
&= m \mod n
\end{aligned}
$$

2. (20 pts, page 7) $n = 221$ is an RSA number. We found $a^{n-1} \mod n = 121$. Find its four square roots modulo n.

   Answer:

$$a^{n-1} \equiv 4 \pmod{13} \wedge a^{n-1} \equiv 2 \pmod{17}$$

$$(1)\ a^{\frac{n-1}{2}} \equiv 2 \pmod{13} \wedge a^{\frac{n-1}{2}} \equiv 6 \pmod{17}$$
$$(2)\ a^{\frac{n-1}{2}} \equiv 2 \pmod{13} \wedge a^{\frac{n-1}{2}} \equiv 11 \pmod{17}$$
$$(3)\ a^{\frac{n-1}{2}} \equiv 11 \pmod{13} \wedge a^{\frac{n-1}{2}} \equiv 6 \pmod{17}$$
$$(4)\ a^{\frac{n-1}{2}} \equiv 11 \pmod{13} \wedge a^{\frac{n-1}{2}} \equiv 11 \pmod{17}$$

   Using the inverses of p, q and CRT, we can see the following:
   $17^{-1} \mod 13 = 10$
   $13^{-1} \mod 17 = 4$

   In case (1), $a^{\frac{n-1}{2}} = 2 \cdot 10 \cdot 17 + 6 \cdot 4 \cdot 13 \pmod{221} = 210 \pmod{221}$

   In case (2), $a^{\frac{n-1}{2}} = 2 \cdot 10 \cdot 17 + 11 \cdot 4 \cdot 13 \pmod{221} = 28 \pmod{221}$

   In case (3), $a^{\frac{n-1}{2}} = 11 \cdot 10 \cdot 17 + 6 \cdot 4 \cdot 13 \pmod{221} = 193 \pmod{221}$

   In case (4), $a^{\frac{n-1}{2}} = 11 \cdot 10 \cdot 17 + 11 \cdot 4 \cdot 13 \pmod{221} = 11 \pmod{221}$

   Therefore, the four square roots of 121 modulo n is:

   - 11
   - 28
   - 193
   - 210

3. (10 pts, page 7) Based on the ideas in Section 2.3.1, research (*i.e.,* by Googling) how Miller-Rabin test works, and describe the algorithm with your own language or pseudocode (either one).

   Answer: Take some random a such that $\gcd(a, n) = 1$. Calculate $k = a^{n-1} \mod n$. If this $k \neq 1$, declare n composite and stop. Otherwise, continue finding consecutive square roots of k until it is not equal to ± 1 or another square root cannot be taken. If all the square roots are ± 1, then we can say n is prime (with a 1/4 chance of being incorrect), though repeated tests with other randomly selected a's can help improve the accuracy. If at any point, one of the square roots is not equal to ± 1, then we declare n composite and stop.

4. (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 $n = pq$. Describe how to try to factor n using such an a.

   - Hint: Reading Section 3.3.4 in Lecture 03-05 will be helpful.

   Answer: Compute $k = a^{\frac{n-1}{2}}$. If $k = \pm 1$, then a is not useful in factoring n.

   Otherwise, compute $p = \gcd(k + 1, n)$ and $q = \gcd(k - 1, n)$ as $k \pm 1$ is likely to share significant factors with n. If $p, q \neq 1$, then we have found factors of n and can continue reducing it to its prime factorization if necessary.