CSE 40622 Cryptography, Spring 2018
Written Assignment 02 (Lecture 03-05)

Name: **Jasmine Walker**

1. (15 pts, page 5) Prove Fermat's Little Theorem when x is not a positive integer without using Euler's Theorem.

   - Follow the proof in page 5 in the note for Lecture 03-05, but consider that x is either 0 or negative.

   Answer:
   Case 1: $x = 0$
   If $x = 0$, then $0^p \equiv 0 \pmod p$ for any p

   Case 2: $x \epsilon \mathbb{Z}^-$
   If $x \epsilon \mathbb{Z}^-$, $x = -1 - 1 - 1...$ for as many 1's as x. So, for all x in $\mathbb{Z}$,
   $x^p \equiv (\sum_{n=1}^{x} -1)^p \equiv (\sum_{n=1}^{x} (-1)^p) \equiv (\sum_{n=1}^{x} -1) \equiv x \pmod p$
   Note that $(-1)^p$ is always -1 because p is a prime.

2. (**Hard**, 15 pts, page 5) If p in Fermat's Little Theorem is not a prime number, the first step of its proof may not hold any more. Explain this with a special case where $p = q^2$ and q is a prime number.

   - Binomial theorem states

   $$(x+y)^p = \binom{p}{0} x^p y^0 + \binom{p}{1} x^{p-1} y^1 + \binom{p}{2} x^{p-2} y^2 + \cdots + \binom{p}{p-1} x^1 y^{p-1} + \binom{p}{p} x^0 y^p$$

   Is it true that $(x+y)^p \mod p = x^p + y^p$ even though $p = q^2$?

   - Look at the terms $\binom{p}{q}, \binom{p}{q+1}, \binom{p}{q+2}, \cdots$ and see whether they are ALL multiples of p.
   - For example, $\binom{p}{3} = \frac{q^2(q^2-1)(q^2-2)}{3 \cdot 2}$. q^2 cannot be divided by 2 or 3 (since q is prime), and $\binom{p}{3}$ must be an integer. Then, $\frac{(q^2-1)(q^2-2)}{3 \cdot 2}$ must be an integer factor. Therefore, $\binom{p}{3}$ must be a multiple of p, and $\binom{p}{3} \mod p = 0$. The same theory applies to $\binom{p}{4}, \binom{p}{5}, \binom{p}{6}, \cdots$ all the way up to $\binom{p}{q-1}$.

   Answer:
   $\binom{p}{q} = \binom{q^2}{q} = \frac{(q^2)(q^2-1)...(q^2-q+1)}{(q)(q-1)...(2)} = (q) \frac{(q^2-1)...(q^2-q+1)}{(q-1)...(2)}$
   This shows that $\binom{p}{q}$ is some factor of q, but not necessarily some factor of $q^2 = p$. There are some cases (ex. when $p = 4$, $q = 2$, $x = 9$, $y = 5$) where $(x+y)^p \not\equiv (x^p + y^p) \pmod p$ (ex. $(9+5)^4 \not\equiv (9^4 + 5^4) \pmod 4$).

3. (10 pts, page 4 & 5) Use Euler's Theorem to prove Fermat's Little Theorem.

   - There are two cases: when $\gcd(x,p) = 1$ and when $\gcd(x,p) \neq 1$.

   Answer:
   Case 1: $\gcd(x,p) = 1$
   When $\gcd(x,p) = 1$, then $x^{\varphi(p)} \equiv 1 \pmod p$. Multiplying both sides by x,
   $(x^{\varphi(p)} \cdot x) \equiv (1 \cdot x) \pmod p$
   $x^{\varphi(p)+1} \equiv x \pmod p$
   Since p is prime,
   $x^{(p-1)+1} \equiv x \pmod p$
   $x^p \equiv x \pmod p$

Case 2: $\gcd(x, p) \neq 1$
If p is prime and $\gcd(x, p) \neq 1$, then x must be some multiple of p. If this is the case, then $x \mod p = 0$. For any $p \epsilon \mathbb{Z}$, $x^p \equiv x \equiv 0 \pmod{p}$.

4. Suppose we have strong attackers as follows. Describe how he/she can universally break the RSA encryption.

   ** Anyone has access to the public key by default.

   (a) (10 pts, page 7) The attacker can do the factoring of $n = pq$. That is, he/she can figure out p and q from $n = pq$.
   Answer:
   The attacker has n from the public key and e from the public key. The attacker can find p and q from the public key n. Then, the attacker can find $\varphi(n) = (p-1)(q-1)$, which is trivial if the attacker can find p and q from n. The attacker can find d, the private key, from this information by computing the inverse of $e \mod \varphi(n)$. The hacker can then decrypt any cipher given by computing $c^d \mod n = m$, which is the decryption algorithm.

   (b) (10 pts, page 8) The attacker can somehow calculate $\varphi(n)$ from n.
   Answer:
   If the attacker can figure out $\varphi(n)$ from n, then the answer is similar to the one above: Given the public key n and e, the attacker can find $\varphi(n)$, which means the attacker can find $d = e^{-1} \mod \varphi(n)$. Since d is the private key, the attacker can decrypt any cipher encrypted by the public keys by computing $c^d \mod n = m$.

5. (15 pts) Assuming that the factoring of $n = pq$ is hard. Explain why it is hard to infer m in RSA by performing the e-th root modulo n as follows, given that e is a public parameter.

$$\sqrt[e]{c} \mod n = c^{\frac{1}{e}} \mod n = (m^e)^{e^{-1}} \mod n = m^{e \cdot e^{-1}} \mod n = m^1 \mod n = m$$

Answer:
While it is easy to determine $e^{-1} \mod n$, raising c to e^{-1} would not necessarily result in m. Consider, $c^{e^{-1}} \equiv m^{e \cdot e^{-1}} \equiv m^{kn+1} \pmod{n}$ for some integer k
In order for $m^{kn+1} = m$, m^{kn} must equal 1. But we cannot guarantee that $m^{kn} = 1$. Instead of multiplying by the modular multiplicative inverse of $e \mod n$, we should multiply by the modular multiplicative inverse of $e \mod \varphi(n)$, which results in m due to Euler's Theorem:
$c^{e^{-1}} \equiv m^{e \cdot e^{-1}} \equiv m^{k\varphi(n)+1} \equiv m^{k\varphi(n)} m^1 \equiv m \pmod{n}$

6. (10 pts, page 6) The RSA encryption requires that m to be a positive number. Explain why m should not be 0.

Answer:
If m were 0, the ciphertext c of m will be 0 no matter what the public or private key is, meaning that an attacker can infer the message m from the ciphertext c. Which is not ideal.