CSE 40622 Cryptography, Spring 2018
Written Assignment 04 (Lecture 07-08 & Lecture 09-12)

Name: **Jasmine Walker**

From Note for Lecture 07-08

1. (**Hard**, 20 pts, Page 4) In $\mathbb{Z}_p^*$ with an odd prime p, prove that a QR has exactly two square roots. That is, for any $x \in \mathbb{Z}_p^*$ that is a QR, there exists exactly two distinct y's such that $y^2 = x$.

   - First show that a QR has at least two square roots, and then show that a QR has at most two square roots.
   - Hint: recall that $\mathbb{Z}_p^*$ has exactly $\frac{p-1}{2}$ QRs.

   Answer:
   There are at least two square roots for every QR:
   For every QR $x \in \mathbb{Z}_p^*$, there must be $\exists y \in \mathbb{Z}_p^*$ such that $x \equiv y^2 \pmod{p}$. Then it must be true that, for every x, $x \equiv y^2 \equiv (-y)^2 \equiv (p-y)^2 \pmod{p}$. $p - y$ is also in $\mathbb{Z}_p^*$ because $p > \forall y \in \mathbb{Z}_p^*$. $p - y \neq y$ because p is odd. Then there must be at least two square roots of every QR in $\mathbb{Z}_p^*$, y and $p - y$.

   There are at most two square roots for every QR:
   From Proposition 1, there are $\frac{p-1}{2}$ distinct QRs in $\mathbb{Z}_p^*$. As stated above, there are at least two square roots for every QR called y and $p - y$. For every distinct QR, the QR's respective roots y and $p - y$ must not equal another distinct QR's y and $p - y$, or else the QRs will not be distinct, which is a contradiction. So for every QR, there are two square roots distinct from every other QR's square roots. These square roots account for all elements in $\mathbb{Z}_p^*$ because $\frac{p-1}{2} \times 2 = p - 1 = |\mathbb{Z}_p^*|$. Thus there cannot be more than two square roots in $\mathbb{Z}_p^*$ for every QR in $\mathbb{Z}_p^*$.

   Therefore, since there cannot be more than two square roots for every QR and there cannot be less than two square roots for every QR, there are exactly two square roots for every QR in $\mathbb{Z}_p^*$.

2. (**Hard**, 10 pts, Page 6) Prove that: Given $\mathbb{Z}_p^*$ with $p = 2q + 1$ where p, q are both odd prime numbers, if $g \in \mathbb{Z}_p^*$ satisfies $g^{\frac{p-1}{q}} \mod p \neq 1$, $\langle g \rangle$ must be a subgroup of $\mathbb{Z}_p^*$ which contains ALL of QRs in $\mathbb{Z}_p^*$.

   Answer:
   Since $|\mathbb{Z}_p^*| = p - 1 = 2q$, $|\mathbb{Z}_p^*|$ is divisible only by 1, 2, q, and $2q$. Then from Lagrange's Theorem, only subgroups with orders 1, 2, q, and $2q$ exist in $\mathbb{Z}_p^*$. If $(g^{\frac{p-1}{q}} \mod p = g^2 \mod p) \neq 1$, then $|\langle g \rangle|$ must equal q or $2q$. If $|\langle g \rangle| = 2q$, then g generates $\mathbb{Z}_p^*$, which must contain all QR in $\mathbb{Z}_p^*$. If $|\langle g \rangle| = q$, then this $\langle g \rangle$ must necessarily contain all QRs and only QRs. Proof by contradiction: if $\langle g \rangle$ does not contain all QRs and only QRs, then it must contain at least one QNR, because $|\langle g \rangle| = q$ and there are q QRs in $\mathbb{Z}_p^*$. If g generated at least one QNR in $\langle g \rangle$, then g cannot be a square of $\exists y \in \mathbb{Z}_p^*$, or else g would produce only QRs. Then g^n will produce a QNR for every odd n. Then g^q will produce a QNR because q is odd. Since $|\langle g \rangle| = q$, then $g^q \mod p = 1$. So $(g^q)^2 = g^q \times g^q = g^q$. But then, g^q cannot be a QNR by definition, because $(g^q)^2$ produces g^q. Because of this contradiction, if $|\langle g \rangle| = q$, then $\langle g \rangle$ must produce only QRs. And since there are $\frac{p-1}{2} = q$ QRs in $\mathbb{Z}_p^*$, then $\langle g \rangle$ must produce all QRs.

3. (10 pts, Page 6) What is the consequence if we have $p = kq + 1$ with some positive even number k instead of 2? In other words, what do you need to do **in extra** in order to find a generator of $\mathbb{Z}_p^*$?

   Answer:
   According to Lagrange's Theorem, we know $|\langle g \rangle|$ is a factor of $|\mathbb{Z}_p^*|$ for $\forall g \in \mathbb{Z}_p^*$. If $p = kq + 1$, the order of $\mathbb{Z}_p^*$ is $p - 1 = kq$. When $k = 2$, the only factors are 1, 2, q, and $2q$. Therefore, we only need to check if the factors 1, 2, and q are the order of $\langle g \rangle$. If not, then g is a generator of $\mathbb{Z}_p^*$. If k is some

positive even number instead of 2, then we must find all the factors of kq, which will be more than four. Then we would have to check the order of $\langle g \rangle$ by inserting each factor of kq for n in $g^n \mod p$. If $g^n \mod p = 1$, then n is the order of $\langle g \rangle$, and g does not generate $\mathbb{Z}_p^*$. If none of the factors besides kq inserted into the equation will produce 1, then g is a generator of $\mathbb{Z}_p^*$.

4. (5 pts, Coming from nowhere) In class, I said one of the countermeasures to QR/QNR attacks is to use the subset of $\mathbb{Z}_p^*$ which contains all of its QRs and use it as $\mathbb{G}$ in ElGamal encryption. Then, Legendre symbols do not give much information to ciphertexts and public keys since all parameters will be QRs. Why is it not possible to use a subset of $\mathbb{Z}_p^*$ which contains all of its QNRs and use it as $\mathbb{G}$?

   Answer:
   There is no generator g that can create the subset of all QNR in $\mathbb{Z}_p^*$, so this subset cannot be used as $\mathbb{G}$ in ElGamal. Proof by contradiction: If there is a g that creates a subset of only QNRs, then g must be a part of this subset, and g must be a QNR. g^2 must produce an element in the set of QNRs. But g^2 must be a QR by definition, which cannot be in the subset of only QNRs. So there cannot exist a g that generates a set of only QNRs in $\mathbb{Z}_p^*$.

5. (**Hard**, 15 pts, Coming from nowhere) Prove that any generator g of $\mathbb{Z}_p^*$ is a QNR if p is an odd prime number.

   Answer:
   Proof by contradiction: If there is a generator g that generates $\mathbb{Z}_p^*$ that is also a QR, then there must be some $y \in \mathbb{Z}_p^*$ such that $y^2 \equiv g \pmod{p}$. Then every element in $\mathbb{Z}_p^*$ can be represented as $g^n = (y^2)^n$ for some n. The QNRs in $\mathbb{Z}_p^*$ can then be represented as $(y^2)^n = (y^n)^2$, which is a contradiction by definition. So all generators of $\mathbb{Z}_p^*$ must be QNRs.

From Note for Lecture 09-12

1. (5 pts, Page 7) What's the major difference between the semantic security and the ciphertext indistinguishability? From the definition? What does that difference mean conceptually?

   Answer:
   The major difference between the definition of semantic security and the definition of ciphertext indistinguishability is the inclusion of $h(m)$, which is the background information the hacker has about message m. Semantic security includes this parameter in its definition, while ciphertext indistinguishability does not. Conceptually, this means that to determine ciphertext indistinguishability, we do not have to consider the background information that the hacker has, and we only need to concern ourselves with encryption parameters. So ciphertext indistinguishability is concerned with the security of the encryption, while semantic security is concerned with the security of the practical application of the encryption.

2. (5 pts, Page 7) $h(m)$ in the definition of semantic security is a mathematical model of the background knowledge of the attackers. Why should the subtraction be negligible for all polynomial-time computable function h?

   Answer:
   It should be negligible for all polynomial-time computable functions h because we want the encryption to be secure against attackers with any level of background knowledge of m. If the encryption was semantically secure against only some $h(m)$, then there exists some $h(m)$ that the encryption cannot be secure against. Then an attacker can use the latter $h(m)$ to break the encryption, which we want to protect against.

3. (10 pts, Page 8) In both RSA and ElGamal, show that $c_1 = c_2$ implies $m_1 = m_2$ if $c_1 \leftarrow \mathsf{Enc}(m_1, \mathsf{pk})$ and $c_2 \leftarrow \mathsf{Enc}(m_2, \mathsf{pk})$.

- Both c_1, c_2 may be sets of elements (in ElGamal).

Answer:
RSA and ElGamal must both have correct encryption schemes. A correct encryption scheme has a **deterministic** decryption scheme $\mathsf{Dec}(c, \mathsf{sk})$, meaning that if $c_1 = c_2$, then $\mathsf{Dec}(c_1, \mathsf{sk}) = \mathsf{Dec}(c_2, \mathsf{sk})$. We know that $m_1 \leftarrow \mathsf{Dec}(c_1, \mathsf{sk})$ and $m_2 \leftarrow \mathsf{Dec}(c_2, \mathsf{sk})$ in both RSA and ElGamal, because they both have correct encryption schemes and $c_1 \leftarrow \mathsf{Enc}(m_1, \mathsf{pk})$ and $c_2 \leftarrow \mathsf{Enc}(m_2, \mathsf{pk})$. Since $c_1 = c_2$, then $\mathsf{Dec}(c_1, \mathsf{sk}) = \mathsf{Dec}(c_2, \mathsf{sk})$, then $m_1 = m_2$.

4. (20 pts, Page 10) Analyze whether the unpadded RSA is semantically secure in the same way as in Section 2.1 of the note. That is, present the eavesdropping game of the unpadded RSA, then show that the adversary's advantage is not negligible.

Answer:
Eavesdropping game of unpadded RSA encryption.

- The challenger chooses large prime numbers p and q whose product, $n = pq$, is at least k bits. The challenger computes Euler's totient $\varphi(n)$, randomly chooses e from $\mathbb{Z}_{\varphi(n)} - \{0, 1\}$ such that $\gcd(e, \varphi(n)) = 1$, and finds $d := e^{-1} \mod \varphi(n)$. The challenger publishes 1^k, n, and e to the adversary.
- The adversary outputs a pair of messages (m_0,m_1), both of which were drawn from $\mathbb{Z}_n^*$.
- The challenger randomly chooses a bit $b \leftarrow_\$ \{0, 1\}$, and computes $C := (m_b^e \mod n)$, and publishes C to the adversary.
- The adversary outputs the guess b' on b.

The adversary has access to the public keys n and e, so they can encrypt both messages m_0 and m_1 into respective ciphertexts c_0 and c_1. Since encryption is deterministic in unpadded RSA encryption, the published C will match either c_0 or c_1. Since the adversary can correctly match the published ciphertext to either c_0 or c_1, the adversary has an advantage of $\frac{1}{2}$, which is not negligible in regards to k.