CO 485/685: Assignment #2 Due date: October 6 (Friday)

Some of these exercises are from the textbook. In such cases, the corresponding exercise number from the textbook is provided.

1. (Exercise 2.25.) Suppose $n = pq$ with p and q distinct odd primes.
   (a) Suppose that $\gcd(a, pq) = 1$. Prove that if the equation $x^2 \equiv a \pmod{n}$ has any solutions, then it has four solutions.
   (b) Suppose you had a machine that could find all four solutions for some given a. How could you use this machine to factor n?

2. (a) (Exercise 3.39 (a)) Let p be a prime satisfying $p \equiv 3 \pmod{4}$. Let a be a quadratic residue modulo p. Prove that the number $b \equiv a^{\frac{p+1}{4}} \pmod{p}$ has the property that $b^2 \equiv a \pmod{p}$. (Hint. Write $\frac{p+1}{2}$ as $1 + \frac{p-1}{2}$ and use Exercise 3.37.) This gives an easy way to take square roots modulo p for primes that are congruent to 3 modulo 4.
   (b) Let p be a prime satisfying $p \equiv 1 \pmod{4}$. Let a be a quadratic residue modulo p. Prove that the number $b \equiv a^{\frac{p+1}{4}} \pmod{p}$ has the property that $b^2 \equiv a \pmod{p}$. Explain why this does **not** give an easy way to take square roots modulo p for primes that are congruent to 1 modulo 4.

3. The *Benaloh cryptosystem* (`https://en.wikipedia.org/wiki/Benaloh_cryptosystem`) is defined as follows:

   Key generation: Choose large primes p and q and a small prime r such that $\gcd(r, \frac{p-1}{r}) = 1$, $\gcd(r, q-1) = 1$, and $r \mid (p-1)$. Note that r does not grow with the security parameter. A typical value of r is $r \approx 10^9$. If you wish, you may assume $r < 100$ when doing this problem.
   Set $n = pq$ and $\phi(n) = (p-1)(q-1)$. Choose $y \in (\mathbb{Z}/n)^*$ such that $y^{\frac{\phi(n)}{r}} \not\equiv 1 \pmod{n}$, and set $x = y^{\frac{\phi(n)}{r}} \in (\mathbb{Z}/n)^*$. The public key is (n, y, r). The private key is $(\phi(n), x)$.

   Encryption: The message space is $\mathbb{Z}/r$. To encrypt $m \in \mathbb{Z}/r$, choose $u \leftarrow\!\!\$\ (\mathbb{Z}/n)^*$ at random and compute $c = y^m u^r \in (\mathbb{Z}/n)^*$. The resulting ciphertext is c.

   Decryption: Given a ciphertext $c \in (\mathbb{Z}/n)^*$:
   - Compute $a = c^{\frac{\phi(n)}{r}} \in (\mathbb{Z}/n)^*$.
   - Compute (by brute force) $m = \log_x(a)$; that is, find m such that $x^m = a$.

   The resulting plaintext is m.

   (a) For which elements of the subset $\{x, y, c, a\} \subset (\mathbb{Z}/n)^*$ is the order of the element known? In each case where the order is known, determine the order.
   (b) Prove that decryption is correct. That is, if a message m is correctly encrypted to a ciphertext c under a correct key, and then c is correctly decrypted under a correct key, then the decryption result is equal to m. (Note: In this problem, we assume r is prime. The proof given on Wikipedia is incorrect, because, as noted on Wikipedia, decryption is not always correct if we allow r to be composite. The proof given on Wikipedia does not make use of the assumption that r is prime, and thus if correct would "prove" correctness of decryption even for composite r.)

4. The *composite residuosity assumption* is defined using the following game. Prove that the Benaloh cryptosystem is secure (under which definition of security?) under this assumption.

   $\mathrm{CR}^{\mathcal{A}}_{p,q,r}$

   $$\begin{array}{l}
   (p, q, r) \text{ such that } \gcd(r, \frac{p-1}{r}) = 1 \wedge \gcd(r, q-1) = 1 \wedge r \mid (p-1) \leftarrow\!\!\$\ \mathsf{Pgen}(1^\lambda) \\
   n \leftarrow pq, b \leftarrow\!\!\$\ \{0,1\}, x \leftarrow\!\!\$\ (\mathbb{Z}/n)^*, z \leftarrow x^{r^b} \\
   b' \leftarrow\!\!\$\ \mathcal{A}(1^\lambda, n, r, z) \\
   \textbf{return } b \stackrel{?}{=} b'
   \end{array}$$