In all of the exam problems, you may use without proof any logically preceding result. Note that blank answers will be given 20% of the credit, but answers without merit will not receive any credit.

**Problem 1:** (10 points) Prove Lagrange’s Theorem; namely, if $H$ is a subgroup of finite group $G$ then $|H| \mid |G|$. You may cite and use properties of left cosets without proof.

**Proof:** There is a theorem stating that if $H$ is a subgroup of a finite group $G$ then
1) each left coset for $H$ is the same cardinality as $H$, and also
2) the left cosets partition $G$.
Thus the number of distinct left cosets times $|H|$ is exactly $|G|$, so that $|H| \mid |G|$.

**Problem 2:** (10 points) Suppose that Alice and Bob are all set up for RSA.

a) Give the computational and descriptive difference, between Alice sending message $m$ to Bob using RSA, versus Alice signing a message $m$ for Bob using RSA digital signature.

b) Quantify clearly and explain (as in lecture) the difficulty for Eve to forge Alice’s RSA signature.

**Solution:** a) In RSA Alice would compute $c = m^{e_B} \mod n_B$ using Bob’s RSA apparatus, whereas in RSA signature Alice would compute $s = m^{d_A} \mod n_A$ using Alice’s RSA apparatus.

b) If Eve wants to forge Alice’s signature to the message $m$ then she needs to find $s$ such that $s = m^{d_A} \mod n_A$, ie (taking $e_A$ power of both sides) she needs to find $s$ such that $s^{e_A} = m \mod n_A$. However, this is exactly the RSA problem—with Alice’s RSA apparatus—for obtaining plaintext $s$ from ciphertext $m$. 


Problem 3: (10 points) Suppose $p$ and $q$ are prime numbers, and $n := pq$ is a Rabin modulus that is used in a Rabin cryptosystem. Prove that if Eve can efficiently compute the four square roots mod $n$ for an element that has four square roots then Eve can efficiently factor $n$.

Solution: Say that $m_1$ and $m_2$ are two square roots for the same number, ie $m_1^2 = m_2^2 \mod n$, yet $m_1 \neq \pm m_2 \mod n$. Then $pq = n \mid (m_1^2 - m_2^2) = (m_1 - m_2)(m_1 + m_2)$, yet $pq = n \not\mid (m_1 - m_2)$ and $pq = n \not\mid (m_1 + m_2)$. Hence, by FTA exactly one of $p, q$ divides $m_1 - m_2$. So, $\gcd(n_1 - n_2, n)$ is either $p$ or $q$, and Euclid Algorithm for gcd finds this factor efficiently.

Problem 4: (10 points) a) Prove Euler’s Theorem; namely, if $m \in \mathbb{Z}_n^*$ then $m^{\phi(n)} = 1 \mod n$. You must explicitly use Lagrange’s Theorem. b) Give an efficient way (that does not use Euclid Alg) to invert $m \in \mathbb{Z}_n^*$ if it happens that $\phi(n)$ is known. Be very clear why your method is efficient.

Solution: The subgroup generated by $m$ has order, say, $\ell$, and is a subgroup of $\mathbb{Z}_n^*$. This means that there are $\ell$ elements in the subgroup generated by $m$, and it is also says that $m^{\ell} = 1 \mod n$. By Lagrange’s Thm, $\ell \mid |\mathbb{Z}_n^*| = \phi(n)$, say that $\ell k = \phi(n)$. Now, $m^{\phi(n)} = m^\ell k = (m^\ell)^k = 1^k = 1 \mod n$.

b) The inverse of $m$ is $m^{\phi(n)-1}$ which can be computed using fast exponentiation (efficient!), since $m \cdot m^{\phi(n)-1} = m^{\phi(n)} = 1 \mod n$ by Euler’s Theorem.
Problem 5: (10 points) Suppose that Alice and Bob conduct a Diffie Hellman key exchange. Unbeknownst to them, suppose, for the sake of this question, that Eve has an efficient algorithm for computing discrete logarithms. Write down the computations Eve could perform to obtain the key exchanged between Alice and Bob, and be very clear why each step can be done efficiently.

Solution: Prime number $p$ with primitive root $r$ are known, as are $A$ and $B$. Eve would efficiently compute $a = \text{dlog}_r(A)$ or $b = \text{dlog}_r(B)$, and then she can compute the key $k$ by either of the computations $k = B^a \mod p$, or $k = A^b \mod p$, or $k = r^{ab} \mod p$; this exponentiation could be done efficiently by fast exponentiation.

Problem 6: (10 points) Suppose that Bob chose large primes $p \approx 2^{500}$ and $q \approx 2^{500}$ and computed his RSA modulus $n := pq$. Suppose that Alice randomly chooses a message $m \in \mathbb{Z}_n$ to send Bob.

a) Give the probability that $m$ is not invertible mod $n$, completely simplified via $\approx$.

b) What are the implications if $m$ is not invertible (and is not zero)?

Solution: The probability that $m$ is not invertible is

$$\frac{n - \phi(n)}{n} = \frac{pq - (p - 1)(q - 1)}{pq} = \frac{p + q - 1}{pq} \approx \frac{2^{500} + 2^{500}}{2^{1000}} = \frac{2^{501}}{2^{1000}} = \frac{1}{2^{499}}.$$

Also, if Alice finds a nonzero, noninvertible $m$ then $1 < \gcd(m, n) < n$, and thus Alice can efficiently factor Bob’s RSA modulus $n$ via Euclid Algorithm.