Name: ____________________________

UNI: ____________________________

Instructor: Shrenik Shah

MATH UN3025 - Midterm 2

November 10, 2016 (75 minutes)

This examination booklet contains 6 problems. There are 10 sheets of paper including the front cover. This is a closed book exam. Do all of your work on the pages of this exam booklet. Show all your computations and justify/explain your answers. Cross out anything you do not want graded. Calculators are NOT allowed.

You have 75 minutes to complete the exam. Do not begin until instructed to do so. When time is up, stop working and close your test booklet. Cell phones, headphones, laptops and other electronic devices are not allowed.

Problem	Possible score	Your score
1	10	
2	10	
3	10	
4	5	
5	10	
6	15	
Extra Credit	6	
Total	60	

Grades will be posted on CourseWorks.

1. Suppose that $n = p \cdot q$ is the product of 2 prime numbers, p and q. Assume that y is a square mod n and that $y \not\equiv 0 \pmod{n}$.

(a) (5 pts.) How many square roots does y have? Explain your answer.

Hint: You will need to consider multiple cases for y.

(b) (5 pts.) Suppose that you know all of the square roots of y. Explain why you can use this information to factor n.

2. Answer the following two questions about hash functions.

(a) (6 pts.) State each of the 3 desired properties of hash functions.

(b) (4 pts.) Consider the following function. Given a message m, divide m into blocks of length 160 bits: $m = M_1||M_2||\ldots||M_\ell$. Let $h(m) = M_1 \oplus \cdots \oplus M_\ell$, where $\oplus$ is the bitwise XOR function. Which of the three properties of a hash function does h satisfy? (Briefly explain why.)

3. The ElGamal signature scheme signing algorithm is as follows. Alice has fixed a public prime p and primitive root α mod p, as well as a secret integer a with $1 \leq a \leq p-2$. She makes $\beta = \alpha^a \pmod{p}$ public. To sign a message m, she:

1. Selects a secret random k such that $\gcd(k, p-1) = 1$.
2. Computes $r \equiv \alpha^k \pmod{p}$, where $0 < r < p$.
3. Computes $s \equiv k^{-1}(m - ar) \pmod{p-1}$.

The signed message is the triple (m, r, s).

(a) (4 pts.) Fill in the blanks in Bob's verification algorithm. (You don't need to prove that it works.)

1. Compute $v_1 \equiv$ __________ $\pmod{p}$ and $v_2 \equiv$ __________ $\pmod{p}$.
2. Check whether $v_1 \equiv v_2 \pmod{p}$. If so, declare that the signature is valid.

(b) (4 pts.) Suppose u, v are any numbers such that $\gcd(v, p-1) = 1$. Compute $r = \beta^v \alpha^u \pmod{p}$ and $s \equiv -rv^{-1} \pmod{p-1}$. Prove that (r, s) is a valid signature for $m = su \pmod{p-1}$. (This is the existential forgery attack from your homework.)

(c) (2 pts.) Explain how hash functions can be used in order to prevent the preceding attack. More precisely, if sign_A denotes Alice's signing function and h is a hash function, explain why it is hard to use the existential forgery attack to construct a triple of values $(m, h(m), \text{sign}_A(h(m)))$.

4. (5 pts.) Consider the following protocol. Let p be a large prime and α a primitive root. Let a be an integer and let $\beta = \alpha^a \pmod{p}$. Suppose p, α, and β is public, and that Peggy wants to prove to Victor that she knows a without revealing it. They agree to use the following protocol.

1. Peggy chooses a random number $r \pmod{p-1}$.
2. Peggy computes $h_1 \equiv \alpha^r \pmod{p}$ and $h_2 \equiv \alpha^{a-r} \pmod{p}$ and sends them to Victor.
3. Victor chooses $i = 1$ or $i = 2$ and asks Peggy to send either $r_1 = r$ or $r_2 = a - r \pmod{p-1}$.
4. Victor verifies that $h_1 h_2 \equiv \beta$ and that $h_i \equiv \alpha^{r_i} \pmod{p}$.

They repeat this several times.

Suppose that Eve is trying to pretend to be Alice by claiming to Victor that she knows a. Assume that Eve has a guess for Victor's choice of i. In terms of Eve's guess (either 1 or 2), what values of h_1 and h_2 should Eve send Victor in each round? (Your choices of h_1 and h_2 should be such that if Eve's guess is right, she is able to respond to Victor's challenge.)

5. Let $\mathbb{F}_2$ be the finite field of 2 elements, and let $P(X) = X^4 + X^3 + 1$ in $\mathbb{F}_2[X]$.

(a) (3 pts.) Prove that $P(X)$ is irreducible. You may assume that X^2+X+1 is the only irreducible polynomial of degree 2 in $\mathbb{F}_2[X]$.

(b) (7 pts.) Define a finite field of 16 elements by $\mathbb{F}_2[X] \pmod{P(X)}$. Find the inverse of $X^2 + 1$ in this field.

6. The addition law for an elliptic curve is on the last page of the exam booklet. You may tear off that page.

(a) (5 pts.) Let E be the elliptic curve $y^2 \equiv x^3 + 2x + 1 \pmod{3}$. Find all the points on E.

(b) (5 pts.) How many points P on E satisfy $P + P = \infty$?

(c) (5 pts.) Find a point Q on E that satisfies $(1, 1) + Q = (1, 2)$. (For reference: E is the curve $y^2 \equiv x^3 + 2x + 1 \pmod{3}$.)

Hint: You do not need to use "guess-and-check" on this problem; try adding something to both sides of the equation.

Extra credit.

(a) (1 pt.) Suppose that two sets of r objects are drawn from the same set of size N. What is the formula from class giving an approximate probability of a match between an object in the first set and an object in the second?

(b) (4 pts.) Suppose that h is a hash function mapping to strings of $n = 60$ bits. Explain in a few sentences the method, discussed in class, that would allow Fred the Forger to trick Alice into signing the hash of a legitimate contract C, while simultaneously obtaining her signature on the hash of a fraudulent contract F. Assume that a success probability of $1 - \frac{1}{e}$ is acceptable.

(c) (1 pt.) How can Alice avoid falling for such a trap?

The addition law for the elliptic curve $y^2 = x^3 + bx + c$ is given by the following formula. Let $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$. Let $P_3 = (x_3, y_3) = P_1 + P_2$. Then the coordinates x_3 and y_3 are defined by

$$\begin{aligned} x_3 &= m^2 - x_1 - x_2 \\ y_3 &= m(x_1 - x_3) - y_1 \end{aligned}$$

where

$$m = \begin{cases} \frac{y_2 - y_1}{x_2 - x_1} & \text{if } P_1 \neq P_2 \\ \frac{3x_1^2 + b}{2y_1} & \text{if } P_1 = P_2. \end{cases}$$

If the slope m is infinite, then $P_3 = \infty$. Moreover, $\infty + P = P$ for all points P.