Name: _____

UNI: _____

Instructor: Shrenik Shah

MATH UN3025 - Final Examination

December 22, 2016 (170 minutes)

This examination booklet contains 9 normal problems plus 2 extra credit problems. There are 17 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 170 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	15	
2	10	
3	15	
4	15	
5	10	
6	5	
7	10	
8	10	
9	15	
Extra Credit	10.5	
Total	105	

Grades will be posted on CourseWorks.

1.

(a) (5 pts.) Suppose that you were told that Alice and Bob had distinct RSA public keys N_A and N_B, but that the two RSA keys were not relatively prime. Explain briefly how you would efficiently recover the factorization of both keys.

(b) (5 pts.) Use your method to compute this factorization in the case of $N_A = 7747$ and $N_B = 9017$. (Just name one of the factors of each of N_A and N_B.)

Hint: If your calculation is long, you probably made an arithmetic error.

(c) (5 pts.) Now assume instead that Alice and Bob have the *same* RSA public key N, but that their exponents e_A and e_B are relatively prime. If someone encrypted and sent a message m to both Alice and Bob, encrypted via RSA, and you have intercepted both encrypted messages, explain how you can recover m.

2. (10 pts.) This problem is about the first step in the index calculus attack on the discrete log problem mod 19. For each prime p smaller than $B = 8$ (i.e. for $p = 2, 3, 5$, and 7), compute $\log_2(p)$, where we are working with powers of 2 modulo 19. To receive any credit for your solution, you MUST use only the following given equations to compute these values (like we did in class); you should not do any modular exponentiation.

$$2^1 \equiv 2 \pmod{19}$$
$$2^7 \equiv 14 \pmod{19}$$
$$2^{11} \equiv 15 \pmod{19}$$
$$2^{15} \equiv 12 \pmod{19}$$

3. The linear code $C \subseteq \mathbb{F}_2^5$ has generating matrix

$$G = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 & 1 \end{pmatrix}.$$

(a) (2 pts.) Write all the codewords in the code C.

(b) (3 pts.) What is the minimum distance $d(C)$? How many errors can C correct? How many can C detect? (No explanation needed.)

(c) (2 pts.) Write the parity check matrix H in systematic form for C. (No explanation needed.)

(d) (2 pts.) Compute the syndrome of the received message $r = (1, 1, 1, 1, 1)$.

(e) (3 pts.) Write out all the members of the coset $r + C$, and determine the coset leader of this coset.

(f) (3 pts.) What is the nearest neighbor decoding of $(1, 1, 1, 1, 1)$? Explain how you could arrive at your answer using the coset leader in part (e).

4. Recall that in the ElGamal cryptosystem, (p, α, β) are Bob's public key, where $\beta \equiv \alpha^a \pmod{p}$, and a is Bob's private key. Then in order to send a message to Bob, Alice takes her message m with $0 \leq m < p$, picks a random integer k, and computes and sends the pair (r, t) given by $r \equiv \alpha^k \pmod{p}$ and $t \equiv \beta^k m \pmod{p}$.

(a) (10 pts) Carefully and completely explain how to implement the ElGamal cryptosystem on an elliptic curve. Assume that Alice has already encoded her message in the form of a point P on the elliptic curve $E \bmod p$. Your answer should include:

1. Bob's public key and private key
2. Alice's encryption method
3. Bob's decryption method

(b) (2 pts.) If the message m was encoded in the point P by having the x coordinate be of the form $x = m \cdot K + j$, where $0 \leq j < K$, and Bob knows both K and x (but not j), explain how Bob can determine m.

(c) (3 pts.) Explain briefly why there should be, with probability around $1 - \frac{1}{2^K}$, a point on E with x coordinate $x = m \cdot K + j$ with $0 \leq j < K$.

5.

(a) (5 pts.) Explain the intruder-in-the-middle attack on the Diffie-Hellman key exchange. (A diagram of what is going on with a sentence description is fine.)

(b) (5 pts.) State the station-to-station protocol, which can avert this attack.

6.

(a) (1 pt.) Show that $X^3 + 2X + 1$ is irreducible in $\mathbb{F}_3[X]$.

(b) (4 pts.) Compute the inverse of $X + 1$ in $\mathbb{F}_3[X] \pmod{X^3 + 2X + 1}$.

7. (10 pts.) Suppose that a code $C \subseteq \mathbb{F}_2^n$ is cyclic. Identify $\mathbb{F}_2^n$ with $\mathbb{F}_2[X] \pmod{X^n - 1}$ via

$$(a_0, a_1, \ldots, a_{n-1}) \leftrightarrow a_0 + a_1 X + a_2 X^2 + \cdots + a_{n-1} X^{n-1}$$

as we did in class. Prove that for any codeword $m(X) \in C$ and any polynomial $f(X) \in \mathbb{F}_2[X]$, the product $m(X) \cdot f(X)$, viewed as an element of $\mathbb{F}_2[X] \pmod{X^n - 1}$, is also in C.

Hint: The first step is to show that C is closed under multiplication by X (i.e. the special case $f(X) = X$). After that, explain how you can use this special case together with linearity (i.e. the fact that C is closed under $+$ and scalar multiplication) to extend the result to all $f(X) \in \mathbb{F}_2[X]$.

8. (10 pts.) Compute all of the square roots of 191 (mod 209). (Note that $209 = 11 \cdot 19$.) Although the square roots mod 11 and 19 will be obvious, you *must* correctly use both

- the Chinese remainder theorem and
- the algorithm we learned in class for finding square roots (at least when finding the square roots mod 11)

to get full points on this problem.

9. Let $g(X) = X^3 + X^2 + 1$, a polynomial in $\mathbb{F}_2[X]$.

(a) (3 pts.) Show that $g(X)|(X^7 - 1)$. Thus $g(X)$ is the generating polynomial for a cyclic code $C \subseteq \mathbb{F}[X] \pmod{X^7 - 1}$.

(b) (1 pt.) Name a function $h(X)$ so that $m(X)h(X) \equiv 0 \pmod{X^7 - 1}$ exactly when $m(X) \in C$. (No explanation needed.)

(c) (3 pts.) How many codewords are in the cyclic code generated by $g(X)$? Explain your answer by briefly stating the relevant part of the main theorem for cyclic codes.

(d) (2 pts.) How many cosets does C have? (No explanation needed.)

(e) (2 pts.) Explain why $d(C) \leq 3$.

(f) (4 pts.) Write down the generating matrix G and parity check matrix H for the code C. (No explanation needed.)

Extra credit.

Note: This problem will take a long time compared to the number of points it is worth. So return to it once you have finished the other problems.

(a) (2 pts.) Over $\mathbb{F}_2$, factor $X^7 - 1$ into a product of irreducible polynomials $f_1(X) \cdot f_2(X) \cdot f_3(X)$. One of the irreducible factors will be $g(X) = X^3 + X^2 + 1$ from Problem 9; call that $f_1(X)$.

(b) (3 pts.) Let α be a root of $g(X) = f_1(X)$. Compute all of the polynomials $q_i(X)$, where $q_i(X) = f_j(X)$ for the value of j such that $f_j(\alpha^i) = 0$. There is extra space for your answer on the next page.

Hint: This will be easy as soon as you check that α^2 is also a root of $g(X)$. (The argument that α is a root implies α^2 is a root also implies that $(\alpha^2)^2 = \alpha^4$ is a root; now use the fact that g has at most 3 roots and you will be done.)

Continue your answer to (b) here.

(c) (1.5 pts.) Let C be the code from problem 9, which is generated by $g(X)$. Use the BCH bound to show that $d(C) \geq 3$. Combined with part (b) of problem 9, this will show that $d(C) = 3$.

Extra credit, continued.

(4 pts.) State the coin-flipping protocol from class. Recall that in this protocol, Alice begins by sending Bob a number $n = pq$ for secret primes p and q, and Bob responds by choosing y a square modulo n. Fill in the remaining steps, and explain carefully why Bob cannot cheat in order to win.

Note: This problem will take a long time compared to the number of points it is worth. So return to it once you have finished the other problems.

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.