Mathematics 496/616—Spring 2019
Cryptography
Final Exam
April 28–May 7, 2019

Directions (READ CAREFULLY)

There are five problems on this exam. Each problem is worth 20 points. On each of the problems you do, you should *justify all of your answers rigorously, using results from the text, from your homework, or from class.* (You don't have to quote the numbers of the theorems from the text though!) Do as much as you can on each of the problems you work on, but leave out arguments that you know are wrong. You shouldn't hand in scratch work (although writing down all of your thoughts and deductions on scrap paper is VERY helpful in coming up with a correct proof). Write up your answers clearly and neatly. The proofs will be graded for *mathematical correctness, clarity, and grammar.* (Use punctuation, capital letters to begin sentences, etc.)

Feel free to e-mail me if you have any questions about the exam, and I'll get back to you as soon as possible

You may consult any of the sections in the text that we have covered in class, as well as your class notes, but do not consult other sources, and DO NOT WORK WITH OTHER STUDENTS.

The exam is due (either in my mailbox in the Don Myers Technology and Innovation Building or via e-mail) on Tuesday, May 7 at 5:00 p.m.

Problems

1. (a) Suppose G is a cyclic group generated by $g \in G$, i.e., $G = \{e, g, g^2, \dots g^{n-1}\}$, where n is the order of g. It can be shown that if $0 \le k \le n-1$, then the order of g^k is
$$\frac{n}{\gcd(k,n)}.$$
Use this to prove that G has at most one element of order 2.

   Now let p be a prime, and let E be an elliptic curve over $\mathbb{F}_p$. Suppose E is defined by the Weierstrass equation $Y^2 = X^3 + AX + B$.

   (b) Suppose $X^3 + AX + B$ has three roots in $\mathbb{F}_p$. Use (a) to prove that $E(\mathbb{F}_p)$ is *not* cyclic.

   (c) Suppose $X^3 + AX + B$ has at least one root in $\mathbb{F}_p$. Prove that $\#E(\mathbb{F}_p)$ is even.

2. Employ Lenstra's algorithm to factor the integer $N = 28102844557$, using the elliptic curve $E : Y^2 = X^3 + 18X - 453$ and the point $P = (7, 4) \in E(\mathbb{Z}/N\mathbb{Z})$.

3. Let p and q be odd primes, and let $N = pq$. Let t be a positive integer such that $a^{2t} \equiv 1 \pmod{N}$ for all $a \in (\mathbb{Z}/N\mathbb{Z})^*$, but the congruence $a^t \equiv 1 \pmod{N}$ does *not* hold for all $a \in (\mathbb{Z}/N\mathbb{Z})^*$.

   (a) Prove that either $p - 1 \nmid t$ or $q - 1 \nmid t$.

   (b) Use (a) to show that for 50% of the numbers $a \in (\mathbb{Z}/N/Z)^*$, a^t is congruent to 1 modulo one of the primes p, q and is congruent to -1 modulo the other prime. You can use that fact that the relations of congruence modulo p and q are completely independent of each other. (Hint: by (a), either exactly one of $p-1, q-1$ divides t, or neither of $p-1, q-1$ divide t. Consider these cases separately.)

   (c) Show that by choosing s numbers $a \in \mathbb{F}_p$ at random and computing $\gcd(a^t - 1, N)$ for each a, we can find a prime factor of N with probability $1 - 1/2^s$.

4. Let p be a prime, and let E be an elliptic curve over $\mathbb{F}_p$. Then E is given by the equation $Y^2 = f(X)$, where f is a cubic polynomial with coefficients in $\mathbb{F}_p$. This problem investigates a method for encoding plaintexts as points in $E(\mathbb{F}_p)$.

   Let M and s be positive integers such that $p > Ms$. Suppose numerical plaintexts are integers m such that $0 \le m < M$. Given a plaintext m, let S_m be the list of numbers $ms + 1, ms + 2, \ldots, ms + s = (m + 1)s$. I.e.,

$$S_0 = \{1, \ldots, s\}, \quad S_1 = \{s + 1, \ldots, 2s\}, \quad S_2 = \{2s + 1, \ldots, 3s\}, \quad \ldots$$

   We now describe a scheme for encoding m as as a point P_m in $E(\mathbb{F}_p)$ whose x-coordinate lies in S_m. Let $x = ms + 1$. If $f(x)$ is a square in $\mathbb{F}_p$, find y such that $y^2 = f(x)$, and set $P_m = (x, y)$. Otherwise, increment x by 1, and repeat the process with this new value of x. Continue if necessary until $x = (m + 1)s$.

   (a) Show that the probability that this method fails in associating a point P_m to m is approximately $1/2^s$.

   (b) Show that if s is sufficiently large, the probability that this method succeeds in finding a point $P_m \in E(\mathbb{F}_p)$ for every plaintext m is about $1 - M/2^s$. (Hint: You might want to use the binomial approximation $(1 + x)^k \approx 1 + kx$ for small x.)

   (c) Assuming we have found $x \in S_m$ such that $f(x)$ is a square, write down a formula for m in terms of $P_m = (x, y)$ and s.

5. Do Problem 6.20 in the text.