MATH 496/616—Spring 2019
Cryptography
Test 2
April 6–12, 2019

Directions (READ CAREFULLY)

There are four problems on this exam. Each problem is worth 25 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 in my mailbox in the Don Myers Technology and Innovation Building on Friday, April 12 at 5:00 p.m.

Problems

1. Alice decides to use the RSA cryptosystem to enable individuals to communicate secret information to her. She chooses the public key $(N, e) = (536813567, 3602561)$. Numerical plaintext is obtained from alphabetic plaintext in the following way. Plaintext blocks have 6 letters (in the standard 26-letter alphabet). Such an alphabetic block is then considered to be a 6-digit base-26 integer (where A represents 0, B represents 1, etc.). Ciphertext consists of 7-digit base-26 integers, which can also be considered as 7-character stings.

   (a) Suppose that Eve successfully cryptanalyzes this key. What decryption exponent d does she find?

   (b) Suppose Bob sends Alice the ciphertext BNBPPKZAVQZLBJ. Help Eve find the alphabetic plaintext for this message.

2. Let a, n be integers, and suppose that $n > 1$ is odd and a is relatively prime to n. In your homework, you showed that if n is prime, then the Legendre symbol

   $$\left(\frac{a}{n}\right) \equiv a^{(n-1)/2} \pmod{n}.$$

   However, in general, this congruence does not hold. If not, we know that n is not prime, and we will call a an *Euler witness* for n.

   Suppose $n \equiv 3 \pmod{4}$. In this problem, you will prove that a is an Euler witness for n if and only if it is a Miller-Rabin witness for n.

   (a) Show that a is *not* a Miller-Rabin witness for n if and only if $a^{(n-1)/2} \equiv \pm 1 \pmod{n}$.

   (b) Use part (a) to show that if a is *not* an Euler witness for n, then a is *not* a Miller-Rabin witness for n.

(c) Show that if $a^{(n-1)/2} \equiv \pm 1 \pmod{n}$, then

$$\left(\frac{a}{n}\right) \equiv a^{(n-1)/2} \pmod{n}.$$

(Hint: use that fact that $\left(\frac{1}{n}\right) = 1$ and $\left(\frac{-1}{n}\right) = -1$ when $n \equiv 3 \pmod{4}$.)

(d) Use (a) and (c) to conclude that if a is *not* a Miller-Rabin witness for n, then a is *not* an Euler witness for n.

3. Let $n > 2$ be an integer, and let m be an integer such that $a^m \equiv 1 \pmod{n}$ for every integer $a \in (\mathbb{Z}/n\mathbb{Z})^*$.

   (a) Show that m is even.

   (b) Suppose that there exists some integer $b \in (\mathbb{Z}/n\mathbb{Z})^*$ such that $b^{m/2} \not\equiv 1 \pmod{n}$. Prove that $a^{m/2} \not\equiv 1 \pmod{n}$ for at least half of the integers $a \in (\mathbb{Z}/n\mathbb{Z})^*$. (Hint: if $a_1^{m/2} \equiv 1 \pmod{n}$, what can you say about $a_1 b$?)

   (c) Suppose that you choose s distinct values of $a \in (\mathbb{Z}/n\mathbb{Z})^*$ and compute that $a^{m/2} \equiv 1 \pmod{n}$ for each a. Prove that the probability that $a^{m/2} \equiv 1 \pmod{n}$ for *all* $a \in (\mathbb{Z}/n\mathbb{Z})^*$ is at least $1 - 1/2^s$.

   This result serves as the first step in a method for determining the factorization of the encryption modulus in RSA if one knows both the encryption and decryption exponents.

4. Samantha chooses the prime 4001 and the primitive root 2938 modulo 4001, and implements the Elgamal signature scheme to sign the document 2437. The signature produced is $(2709, 1750)$. Find the random element k and the secret exponent a that Samantha used, so that you will be able to forge her signature on other documents. Document whatever algorithms you use to solve any intermediate problems.