MATH 496/616—Spring 2019
Cryptography
Test 1
February 19–26, 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 Tuesday, February 26 at 5:00 p.m.

Problems

1. Let a be an integer.

   (a) Let b, c, and m be positive integers, and suppose a is relatively prime to m, $a^b \equiv 1 \pmod{m}$, and $a^c \equiv 1 \pmod{m}$. Prove that $a^g \equiv 1 \pmod{m}$, where $g = \gcd(b, c)$.

   (b) Suppose n is a positive integer and p is a prime such that $a^n \equiv 1 \pmod{p}$. Use part (a) (hint: use $b = n$ and $c = p - 1$) to prove that either

   - $a^d \equiv 1 \pmod{p}$ for some proper divisor d of n, or
   - $p \equiv 1 \pmod{n}$.

   (c) Using part (b) to narrow down possible prime factors, factor $2^{35} - 1$ into primes. It will be useful to use the fact that an integer $q > 1$ is prime if and only if it has no prime factors less than $\sqrt{q}$.

2. Let N be a positive integer. Consider an affine cipher on the space of plaintext messages $\mathcal{M} = \mathbb{Z}/N\mathbb{Z}$. The encryption function e is given by the formula

$$e(m) = am + b,$$

   where $a, b \in \mathbb{Z}/N\mathbb{Z}$ and a is invertible modulo N. Assume that $a \not\equiv 1 \pmod{N}$ (so that e doesn't define a Caesar cipher).

   (a) Show that if N is prime, then e fixes exactly one plaintext message in $\mathcal{M}$. (A message m is fixed if $e(m) \equiv m \pmod{N}$.)

   (b) Show that if N is even and $b = 0$, then e fixes at least two plaintext messages in $\mathcal{M}$.

3. Alice decides to use the Elgamal cryptosystem to enable individuals to communicate secret information to her. She chooses to work in the field with

$$297262705009139006771611927$$

elements (this number is prime), and she selects the secret key

$$10384756843984756438549809.$$

Bob sends her the ciphertext

$$(827465920043750348729577 17, 164063768437915425954819351).$$

(a) What is the numerical plaintext that Alice obtains upon decrypting this message?

(b) The numerical plaintext was obtained from alphabetic plaintext in the following way. Plaintext blocks have 18 letters (in the standard 26-letter alphabet). Such an alphabetic block is converted to a decimal string by considering it to be an 18-digit base-26 integer (where A represents 0, B represents 1, etc.) and then taking the decimal expansion of this integer. Find the alphabetic plaintext of Bob's message.

4. Alice and Bob are using an affine cipher to communicate. Their alphabet has 27 symbols: A–Z together with a blank space. They encode by mapping A to 0, B to 1, ..., and the blank space to 26. They apply a certain affine cipher (see the above definition) on each individual number obtained (viewed as elements of $\mathbb{Z}/27\mathbb{Z}$) and then replace the new numbers with their alphabetic equivalents. Eve intercepts the ciphertext `OFJDFOHFXOL` during one of their communications. She learns that the original plaintext started out "I ". Determine the encryption function and find the full plaintext.