1. Approximately 2/3 of the final exam will cover modular arithmetic and the RSA algorithm, and material from RSA and password generation will be especially emphasized. For this material you should make sure that you can do RSA problems as Alice (encrypter), Bob (decrypter), and Eve (enemy spy). You should make sure you can generate password as either Alice or Bob, as in homework problems. You should also make sure that you can use Fermat’s theorem and Euler’s theorem to compute powers and roots in modular arithmetic (Units 14 to 17), and make sure you can compute fractions in modular arithmetic. If there are 15 problems on the final exam, about 10 of these problems will cover material since the second exam.

2. **PRACTICE FINAL**: See the course website for practice finals:
   1. Practice final without answers: www.nd.edu/~sevens/practicefinal.pdf
   2. Practice final with answers: www.nd.edu/~sevens/practicefinalan.pdf

3. For earlier material, I would start with the exams, and make sure you can do problems like the exam problems. Ask for help if there is a problem from Exam I or Exam II that you have trouble doing. Practice problems for earlier exams should be helpful. I would also recommend going over quizzes in the same way. I would expect that problems covering chapter 15 and earlier on the final will be fairly similar to problems from Exam I or II, or from the quizzes.

4. Part I
   Topics: Expect 1 or 2 problems here
   - Basic counting (Unit 1)
   - multiplication and subtraction principles (Units 2 and 3)
   - counting collections (Unit 4)
   - pascal’s triangle and binomial coefficients (Unit 5)

5. Part II
   Topics: Expect 3 or 4 problems here
   - Divisibility of integers, lcm, gcd, Euclidean Algorithm (Unit 6)
   - Combinations (when can you write 1 as a combination of a and b?), the “backwards” Euclidean Algorithm \(^1\). (Unit 7)

\(^1\) Be sure that you can carry out this algorithm when asked to solve equations like \(1 = X \cdot a + Y \cdot b\) for \(X\) and \(Y\)
• Prime numbers, prime factorization, Sieve of Eratosthenes (Unit 8)
• Two definitions of prime number (Unit 9), divisibility of binomial coefficients by primes, uniqueness of prime factorization (unit 9)
• Consequences of prime factorization, e.g. how to compute \( \text{lcm} \) and \( \text{gcd} \) using factorizations, divisibility of fractions and binomial coefficients \(^2\) (unit 9)
• Definition of two numbers being relatively prime, Euler \( \phi \) function and how to compute it using the formula (unit 10)

6. Part III
Topics: Expect about 10 problems here
• Basic modular arithmetic (how to add, subtract, multiply), abstract definition of fractions, reciprocals, roots (Units 11)
• Congruence (how to tell if two numbers are congruent \( \text{(mod} \ n) \)), simple tricks for computing things \( \text{(mod} \ n) \) (Unit 12)
• Division, existence of fractions and reciprocals \( \text{(mod} \ n) \) when \( n \) is prime and when it’s not. You should be able to compute the reciprocal of a number \( \text{(mod} \ n) \) using reverse Euclidean algorithm (Unit 13)
• Powers, how to compute powers using the “method of squaring”, Fermat’s Theorem and how to use it when computing powers, reciprocals, and roots \( \text{(mod} \ n) \) when \( n \) is prime. (Unit 14)
• Roots \( \text{(mod} \ n) \) when \( n \) is prime. In particular how to compute them, and when do they exist. (Unit 16)
• Euler’s Theorem and how to use it when computing powers, reciprocals, and roots \( \text{(mod} \ n) \) when \( n \) is not prime \(^3\). Be sure you know when Euler’s Theorem applies and when it doesn’t (there are things you need to check before you use it) (Units 15 and 17). Also be able to do problems from Quiz 5.

7. Part IV
Topics:
• How the RSA code works and how to implement it \(^4\) (i.e. to encode or decode a message when the numbers involved are small enough to work by hand).

\(^2\)this concept seemed to be difficult for most people

\(^3\)Remember that Fermat’s Theorem is just a special case of Euler’s Theorem. Euler applies no matter whether \( n \) is prime or not.

\(^4\)It’s good to remember what I called the various numbers involved. In particular remember what role \( n \) plays vs. what \( k \) is; also \( p, q, a, \) and \( b. \) Try not to mix up \( n \) (the modulus) and \( k \) (the power), or \( a \) (the original message) and \( b \) (the encoded message).
Creating secure passwords on the internet (see section 24.6). Given $a, p, k,$ and $l$, you should be able to find the password $a^{kl} \pmod{p}$, and you should know that $a^{kl} \equiv D^k \equiv C^l \pmod{p}$, where $C = a^k \pmod{p}$ and $D = a^l \pmod{p}$. Given $a, p, k$ and $D = a^l \pmod{p}$, you should be able to find the password $D^k \pmod{p}$. Given $a, p, l$ and $C = a^k \pmod{p}$, you should be able to find the password $C^l \pmod{p}$. If $p$ is small enough, and you are given $D$ and $C$, you should be able to find the password.

THE END. Good luck on the exam, and have a great summer.

Practice problems

1. Use Euler’s Theorem to answer the following questions:
   (a) What is $7^{1337} \pmod{18}$? (Answer: 13)
   (b) Does $\sqrt[11]{5} \pmod{18}$ exist? If so, compute it. (Answer: 11)
   (c) How many numbers $X \pmod{18}$ satisfy the equation: $X^{12} = 1 \pmod{18}$? (Answer: 6)

Practice problems for RSA

1. (Ch. 22) Alice wants to send a secret message to Bob using public-key cryptography. Upon request, Bob sends her $n = 143$ and $k = 17$. If Alice wants to tell Bob that 2 people are coming to dinner, but she wants to encrypt the message, what should she send Bob? (Answer: 84)

2. (Ch 24.6) Alice and Bob pick $p = 13$ and $a = 2$.
   (a) If Alice picks $k = 5$ and $C = 6$ and $D = 3$, what is the password? (Answer: 9).
   (b) If Bob picks $l = 8$ and $C = 6$ and $D = 9$, what is the password? (Answer: 3)
   (c) If Eve knows $C = 7$ and $D = 10$, what is the password? What are $k$ and $l$? (Answer: password is “4”, $k=11$, $l=10$)