Math 135 (Summer 2006)
Review for Final Exam

Chapter 4 and 5 Topics

- Prove that there are infinitely many primes.
- Use the Euclidean algorithm to find $\gcd(a, b)$.
- Use the extended Euclidean algorithm to find $a^{-1}\,\mathrm{MOD}\,m$.
- State and apply Fermat's Little Theorem and its corollary.
- Apply the corollary to Fermat's Little Theorem to prove that for distinct primes p and q, and positive integers e and d satisfying $d^{-1} \equiv e \pmod{(p-1)(q-1)}$, the functions $E(x) = x^e\,\mathrm{MOD}\,pq$ and $D(y) = y^d\,\mathrm{MOD}\,pq$ are inverses.
- Perform RSA when given p, q, e. Be able to calculate m, n, d; to encrypt a given plaintext; and to decrypt a given ciphertext. This requires the use of the extended Euclidean algorithm to find modular inverses, and repeated squaring to calculated modular exponentials.
- Explain where the security of RSA rests.
- Understand the basics of how online transactions can be made secure.
- Understand the basic operation of the Enigma machine.
- Be able to perform a simple Diffie-Hellman key agreement (when the algorithm is given).
- Understand, basically, what is meant by Advance Encryption Standard (AES), Digital Encryption Standard (DES), Pretty Good Privacy (PGP), Public Key Infrastructure (PKI), Trusted Authority (TA), Kerberos.
- Have a basic awareness of some of the laws and issues regarding cryptography as discussed in Section 5.4.

Selected Review Problems

1. Find the greatest common divisor of 4961 and 4235.

2. The number 1074967 is a product of two distinct primes. At most, how many trial divisions by primes will be required to find these primes? (Consult the primes table to answer this question.)

3. Use the Corollary to Fermat's Little Theorem to help to compute $3^{147}\,\mathrm{MOD}\,95$.

4. Suppose that Alicia is implementing RSA with primes $p = 53$, $q = 31$, and public exponent $e = 17$.

(a) Explain what she does to set up for receiving encrypted messages and calculate all of the numbers that she will use with these choices of p, q, and e.

(b) If Roberto wants to send Alicia the message $x = 224$ encrypted using her public key, determine the ciphertext he produces.

(c) Suppose Alicia receives the encrypted message $y = 775$. Write down the expression that she will need to evaluate in order to decrypt. (Do not actually evaluate this expression.)

5. Read Example 4.5.4 and follow it to solve Section 4.5 #4 on page 305.