Anna Karlin, 426C Sieg

# Homework # 5
# Due November 26

1. Consider a cryptosystem where the number of keys is equal to the number of possible plaintexts which is also equal to the number of possible ciphertexts. Suppose that for every plaintext $p$ and every ciphertext $c$, there is a unique key $K$ such that $E_K(p) = c$. ($E_K$ is the encryption function using the key $K$.) Prove that the cryptosystem provides perfect secrecy, i.e., that for every plaintext $p$ and ciphertext $c$, the a posteriori probability of $p$, given that the ciphertext is $c$ is equal to the a priori probability of $p$.

2. Compute the multiplicative inverse of 13 modulo 504 using the Extended Euclidean Algorithm.

3. Public-Key Cryptography:

   - What is the primary advantage of public-key cryptography over symmetric cryptography?
   - Consider a message $M$ encrypted using the RSA public-key cryptosystem. Let $E(M)$ be the ciphertext produced. Give an algorithm for determining $M$. What is the running time of your algorithm as a function of the number of bits in $n$ (the modulus $= pq$)?
   - To encrypt a plaintext $M$ using the RSA public-key cryptosystem, the message is first broken up into chunks of at most $k$ bits, where $k$ is the number of bits in the modulus $n$. Why can't we just encrypt the entire message in one fell swoop?

4. Consider the following symmetric cryptosystem, the *exponentiation cipher*. First, choose a prime modulus $m$, known to everyone. Choose a key $k$ less than $m$ at random. (We will see later that not all keys $k$ are possible.) $k$ is kept secret. Then the encryption function $E_k(M)$ is defined as

   $$E_k(M) = M^k (\bmod m).$$

   Let $s$ be the mod $\phi(m)$ multiplicative inverse of $k$. Then the decryption function is

   $$D_k(C) = C^s (\bmod m),$$

   where $C = E_k(M)$.

   - Prove that the cryptosystem works, i.e., that $D_k(C) = M$.
   - Characterize the set of keys $k < m$ for which this system works.
   - Give an argument for why this cryptosystem is probably not vulnerable to known plaintext attack (i.e., recovering the key, given a message and its encryption).