CSE 590 YA: Practical Aspects of Modern Cryptography
Winter 2002

Assignment #2

Due in class: Tuesday, January 22

1. Show how to use the extended Euclidean algorithm to find the multiplicative inverse of 24 modulo 67. In other words, find a value x such that $24x \bmod 67 = 1$. Do not just "find" a solution by trial and error, but rather show the actual values computed by each step of the algorithm. Be sure to verify that your answer is correct by checking the value of $24x \bmod 67$.

2. Using Fermat's little theorem and induction on k, prove that if p is prime then $x^{k(p-1)+1} \bmod p = x \bmod p$ for all integers k and x with $k \geq 0$. [Do not re-prove Fermat's little theorem! If you use the result of Fermat's theorem, this problem is a very short induction.]

3. Show that if p and q are distinct primes and $x \bmod p = y$ and $x \bmod q = y$, then $x \bmod pq = y$. [This can be done formally by using the result of the extended Euclidean algorithm, but for these purposes it's sufficient to use to Unique Factorization Theorem which asserts that any positive integer can be expressed uniquely (up to reordering) as a product of primes.]

4. Use the results of the previous two problems to show that for any two distinct primes p and q,
$$x^{K(p-1)(q-1)+1} \bmod pq = x \bmod pq$$
for all integers K and x with $K \geq 0$. Congratulations — you have just proven the correctness of the RSA cryptosystem!

5. An old electronic cash protocol proposed about twenty years ago went something like this. When a customer wants a cash voucher, it generates an identifying string x and a dollar amount y and asks a bank to sign a voucher. The bank would make sure that each of x and y were padded with leading zeros to a fixed length (say 256 bits) to avoid possible ambiguity. It would then use RSA to sign the string $< x, y, x, y >$ and return the signed voucher to the customer. The repetition was intended to add redundancy to the string to deter cheats from claiming that arbitrary strings were signed vouchers.

   Show how an unscrupulous customer could abuse this system to generate signed vouchers of the proper form that were never explicitly signed by the bank.