CSE 590 TU: Practical Aspects of Modern Cryptography
Winter 2006

Assignment #1

Due in class: Tuesday, January 10

All of the problems on this assignment can be done entirely by hand. You do not need to do any programming.

1. For integers (whole numbers – positive, negative, or zero) r, x, and $m > 0$, we say that $r = x \bmod m$ if (and only if) there is an integer q such that $x = qm + r$.

   (a) Show that for all integers a, b, and $m > 0$, $((a \bmod m)+b) \bmod m = (a+b) \bmod m$.

   (b) Show that for all integers a, b, and $m > 0$, $((a \bmod m)\times b) \bmod m = (a\times b) \bmod m$.

   This justifies our practice of performing additional *mod* operations on intermediate values of a computation.

2. Using exhaustive search, find for each integer x in the range $0 < x < 11$, an integer y such that $x \times y \bmod 11 = 1$. Can you do the same mod12? Why or why not?

3. Compute $3^x \bmod 11$ for each integer value of x such that $0 \leq x \leq 10$.
   Use what you've learned to compute the value

   $$3^{14159265358979323846264338327950288419716939937510582097494459230781640} \bmod 11.$$

4. Find an integer $x > 1$ such that $2^x \bmod 33 = 1$.
   Use what you've leanred to compute the value

   $$2^{7182818284590452353602874713526624977572470936999595749669676277240766} \bmod 33.$$

5. Use the fact (given in class) that when p is prime, $a^{p-1} \bmod p = 1$ for all integers a in the range $0 < a < p$ to prove *without factoring it* that 65 is *not* prime. [Repeated squaring will save you *much* time here.]