Homework #7

Out : October 21, 2:30 pm 1997
Due : October 28, 12:30 pm 1997

The next few problems will require you to apply Euler's Theorem in order to simplify expressions involving modular exponentiations. Recall also the formula for $\phi(m)$, where m is prime. (All of the moduli used in these problems will be prime).

Euler's Theorem: For any modulus m, for any b that is relatively prime to m,

$$b^{\phi(m)} \equiv 1 \pmod{m}$$

This formula implies that if $a \equiv c \pmod{\phi(m)}$, then $b^a \equiv b^c \pmod{m}$.

In the following problems you will use Euler's Theorem and your knowledge of modular arithmetic to simplify a modular exponential expression $b^t \pmod{m}$ to a similar expression where the exponent is a small nonnegative integer. You should assume that the base b is relatively prime to m so that Euler's Theorem is applicable. Show your work.

Example:

Question: modulus $m = 4001$ (a prime). Simplify $b^{12006} \pmod{m}$.
Answer: $\phi(m) = 4000$. We simplify as follows.

$$b^{12006} = b^{3 \cdot 4000 + 6} = (b^{4000})^3 b^6$$

Since $b^{4000} \equiv 1 \pmod{m}$ by Euler's Theorem, we can simplify $(b^{4000})^3 b^6 \pmod{m}$ to $(1)^3 b^6 \pmod{m}$, which is $b^6 \pmod{m}$.

1. In this problem we use the modulus $m = 17$.
   (a) Simplify $b^{19} \pmod{17}$.
   (b) Simplify $b^{33} \pmod{17}$.
   (c) Simplify $b^{52} \pmod{17}$.
   (d) Simplify $b^{213} \pmod{17}$.
2. In this problem we use the modulus $m = 61$.
   (a) Simplify $b^{61} \pmod{61}$.
   (b) Simplify $b^{185} \pmod{61}$.
   (c) Simplify $b^{2410} \pmod{61}$.

3. In this problem we use the modulus $m = 271$.

   (a) Simplify $b^{225} \pmod{143}$.

   (b) Simplify $b^{481} \pmod{143}$.

   (c) Simplify $b^{12037} \pmod{143}$.

4. Which of the following equations are true? Which are false?

   (a) Is $b^{21} \equiv b^4 \pmod{17}$?

   (b) Is $b^{28} \equiv b^6 \pmod{23}$?

   (c) Is $b^{59} \equiv b^{125} \pmod{67}$?

   (d) Is $b^{540} \equiv b^{77} \pmod{463}$?

   (e) Is $b^{723} \equiv b^5 \pmod{719}$?

5. In order to make good choices for our security parameters, we must take into account the speed of both our own encryption algorithm and the best known algorithms for decrypting (without the key). When doing this sort of analysis, we will make the assumption that Eve is using the best possible algorithm and has access to the fastest computers available.

   For systems based upon exponentiation, we have seen that the repeated squaring algorithm offers an efficient means of performing "encryption". A good estimate of the number of ticks required for an exponent of k digits is $13.2 \cdot k^3$. We also know that an algorithm exists for computing the inverse operation, modlog, that requires $k^2 \cdot 10^{\sqrt{(k)(\log_{10} k)}}$ ticks.

   Suppose that Alice's computer runs at 10^8 ticks per second. Although this is by no means slow, she must assume that Eve might posess a machine capable of running at the blinding speed of 10^{11} ticks per second. Is there a value Alice can chose for the security parameter, k, which will allow her to encrypt a block of plaintext in about a second, while preventing Eve from decrypting it without spending volumes more time? Please give such a value for k and explain. Note: You can obtain the answer by using algebra, but in this case it is also perfectly acceptable to use a calculator and try different values of k.