Name:____________________

Introduction to Cryptography

Modular Exponentiation and the Repeated Squaring Algorithm

(1) By hand, use the repeated squaring algorithm to compute $18^{156} \mod 37$.

(2) Let x and n be positive integers. Using the repeated squaring algorithm, determine how many squarings are required to compute each of the following quantities.
  (a) $x^4 \mod n$
  (b) $x^6 \mod n$
  (c) $x^8 \mod n$
  (d) $x^{12} \mod n$
  (e) $x^{1024} \mod n$
  (f) $x^k \mod n$ where k is a positive integer.

(3) By hand, convert the base 2 integer 111010_2 to base 10.

(4) By hand, convert the base 10 integer 1555_{10} to base 2.

(5) The **bin(n)** function in Python can be used to determine the binary representation of an integer n. Use the bin(n) function to verify your answer in the previous question.

(6) Without using the bin(n) function, write a function in Python which
  (a) accepts a positive integer n as an argument;
  (b) return the binary representation of n as an integer.

(7) The **pow(a,b,n)** function in Python can be used to compute $a^b \mod n$ using the repeated squaring algorithm. Use the pow(a,b,n) function (and a for-loop) to compute the following values for every value of a satisfying $1 \leq a < n$.
  (a) $a^6 \mod 7$
  (b) $a^{16} \mod 17$
  (c) $a^{17} \mod 18$
  (d) $a^{18} \mod 19$
  (e) $a^{19} \mod 20$

(8) Use your results from the previous exercise to make a conjecture about when $a^{n-1} \equiv 1 \mod n$. Be sure to think about a necessary condition on n. This result is called **Fermat's Little Theorem**.

(9) Recall that $\phi(n)$ is Euler's Totient function and returns the number of positive integers less than n which are relatively prime to n. Use the pow(a,b,n) function (and a for-loop) to compute the following values for every value of a satisfying $1 \leq a < n$.
  (a) $a^{\phi(7)} \mod 7$
  (b) $a^{\phi(17)} \mod 17$
  (c) $a^{\phi(18)} \mod 18$
  (d) $a^{\phi(19)} \mod 19$
  (e) $a^{\phi(20)} \mod 20$

(10) Use your results from the previous exercise to make a conjecture about when $a^{\phi(n)} \equiv 1 \mod n$. Be sure to think about a necessary condition on a. This result is called **Euler's Theorem**.