Name:______________________

Introduction to Cryptography
Introduction to the Euclidean Algorithm

(1) Without using a computer, use the Euclidean algorithm to compute the greatest common divisor of the following pairs of integers. How many steps does each computation take?
   (a) $gcd(468, 864)$
   (b) $gcd(11111, 111111)$
(2) Let n be a positive integer. Use the Euclidean Algorithm to compute $gcd(n + 1, n)$.
(3) We know that every algorithm must terminate in a finite number of steps. Explain why the Euclidean algorithm is guaranteed to terminate in a finite number of steps.
(4) Without using a computer, use the Euclidean algorithm to compute the greatest common divisor of the following pairs of Fibonacci numbers. How many steps does each computation take?
   (a) $gcd(F_3, F_2)$
   (b) $gcd(F_4, F_3)$
   (c) $gcd(F_5, F_4)$
   (d) $gcd(F_6, F_5)$
(5) Make a conjecture regarding the number of steps needed to compute $gcd(F_{n+1}, F_n)$ using the Euclidean algorithm.
(6) Let a and b be two positive integers such that $a > b$. Suppose it takes exactly n steps to compute $gcd(a, b)$ using the Euclidean algorithm. This means that the $gcd(a, b)$ can be obtained from the following steps.

$$\begin{aligned}
a &= bq_1 + r_1 \text{ where } 0 \le r_1 < b \text{ and } q_1 \ge 1\\
b &= r_1q_2 + r_2 \text{ where } 0 \le r_2 < r_1 \text{ and } q_2 \ge 1\\
r_1 &= r_2q_3 + r_3 \text{ where } 0 \le r_3 < r_2 \text{ and } q_3 \ge 1\\
&\vdots\\
r_{n-5} &= r_{n-4}q_{n-3} + r_{n-3} \text{ where } 0 \le r_{n-3} < r_{n-4} \text{ and } q_{n-3} \ge 1\\
r_{n-4} &= r_{n-3}q_{n-2} + r_{n-2} \text{ where } 0 \le r_{n-2} < r_{n-3} \text{ and } q_{n-2} \ge 1\\
r_{n-3} &= r_{n-2}q_{n-1} + r_{n-1} \text{ where } 0 \le r_{n-1} < r_{n-2} \text{ and } q_{n-1} \ge 1\\
r_{n-2} &= r_{n-1}q_n + 0 \text{ where } q_n \ge 1
\end{aligned}$$

   (a) Explain why $r_{n-1} \ge 1$. (Hint: Why can't we have that $r_{n-1} = 0$?)
   (b) Show why $r_{n-2} \ge 1$.
   (c) Show why $r_{n-3} \ge 2$.
   (d) Show why $r_{n-4} \ge 3$.
   (e) Show why $r_{n-5} \ge 5$.
   (f) Make a conjecture about the smallest possible value of b.
   (g) Make a conjecture about the smallest possible value of a.
(7) Using your conjectures above, what can be said about the number of digits in a and b if it takes 100 steps to compute $gcd(a, b)$ using the Euclidean algorithm?
(8) Let a and b be 100 digit positive integers such that $a > b$. At most how many steps would it take to compute $gcd(a, b)$ using the Euclidean algorithm?