1. Bob is using RSA cryptosystem and his modulus is \( n = pq = 59 \times 167 = 9853 \). Bob chooses an odd integer for his public encryption exponent \( b \). Show that if the plaintext is 2005 then the ciphertext is equal to 2005.

2. a) Use the square-and-multiply algorithm to compute \( 2^{615} \mod 667 \).
   
   b) Determine \( 2^{-1} \mod 667 \). Compare this with a) and explain what you see.

3. Let \((F_n)\) be the sequence of Fibonacci numbers, that is, positive integers such that \( F_0 = 0, F_1 = 1 \) and \( F_n = F_{n-1} + F_{n-2} \), for \( n = 2, 3, \ldots \).
   
   a) Show that the Euclidean algorithm takes \( n - 2 \) iterations to compute \( \gcd(F_n, F_{n-1}) \).
   
   b) Show that
   \[
   F_n = \frac{1}{\sqrt{5}} \left( \frac{1 + \sqrt{5}}{2} \right)^n - \frac{1}{\sqrt{5}} \left( \frac{1 - \sqrt{5}}{2} \right)^n.
   \]
   
   c) Show that, for \( n > 2 \),
   \[
   \left( \frac{1 + \sqrt{5}}{2} \right)^{n-2} < F_n < \left( \frac{1 + \sqrt{5}}{2} \right)^{n-1},
   \]
   or what is the same,
   \[
   n - 2 < \log_f F_n < n - 1, \quad \text{where} \quad f = \frac{1 + \sqrt{5}}{2}.
   \]

4. (Stinson 5.14) Prove that RSA Cryptosystem is not secure against a chosen ciphertext attack using the following steps.
   
   (a) First, show that the encryption operation is multiplicative, that is, \( e_K(x_1 x_2) = e_K(x_1) e_K(x_2) \), for any two plaintexts \( x_1 \) and \( x_2 \).
   
   (b) Next, use the multiplicative property to construct an example how you can decrypt a given ciphertext \( y \) by obtaining the decryption \( \hat{x} \) of a different (but related) ciphertext \( \hat{y} \).

5. (a) Evaluate the Jacobi symbol
   \[
   \left( \frac{801}{2005} \right).
   \]
   You should not do any factoring other than dividing out powers of 2.
   
   (b) Show that 2005 is an Euler pseudoprime to the base 801.

6. Let \( n = pq \), where \( p \) and \( q \) are primes. We can assume that \( p > q > 2 \) and we denote \( d = \frac{p-q}{2} \) and \( x = \frac{p+q}{2} \). Then \( n = x^2 - d^2 \).
   
   a) Show that if \( d < \sqrt{p+q} \) then \( x \) can be computed by taking the square root of \( n \) and by rounding the result up to the nearest integer.
b) Test the method described in a) (if you have a calculator available) for $n = 4007923$

to determine $x$, and further to determine $p$ and $q$. 