Name:______________________

Introduction to Cryptography
RSA Encryption

(1) Use Python to write a function which:
  (a) accepts two prime integers p and q, an encryption exponent e, a numerical integer message, and a boolean variable as arguments;
  (b) checks that e is a valid encryption exponent;
  (c) displays all information which will be made public;
  (d) displays all information which will be kept private;
  (e) displays the encrypted message if the boolean variable is TRUE or displays the decrypted message if the boolean variable is FALSE.

(2) Suppose $p = 41$ and $q = 67$ for an RSA encryption scheme. Find n. Find $\phi(n)$. Of the numbers $7, 9, 15, 35, 49, 91$, which are valid encryption exponents?

(3) Suppose $p = 43$, $q = 67$, and $e = 5$, compute the decryption exponent d. Decrypt the following message.

$$2755\ 920\ 623\ 28\ 410\ 2874$$

(4) You intercept a ciphertext message

$$229280751672014403433171338235 6$$

which was encrypted using RSA with modulus

$$n = 5967296933762411848589059030457$$

and encryption exponent $e = 449$. Decrypt the message. Why doesn't this prove that RSA lacks security? How could the person setting up the RSA system make it much harder to crack?

(5) RSA is usually used only for small messages or sending a key to be used for encrypting a longer message. Explain why RSA cannot be used for large messages.

(6) Let p and q be distinct primes where $q < p$, and let $n = pq$. Recall that $\phi(n) = \phi(pq) = (p-1)(q-1)$. In addition to the publicly available n, suppose an attacker also knows the value of $\phi(n)$.
  (a) Show that $p + q = n - \phi(n) + 1$
  (b) Show that $p - q = \sqrt{(p+q)^2 - 4n}$.
  (c) Use the previous results to write p and q only in terms of n and $\phi(n)$. This shows that knowledge of $\phi(n)$ and n is equivalent to knowledge of both p and q.

(7) In RSA, the decryption step relies on Euler's theorem, specifically $m^{\phi(n)} \equiv 1 \mod n$ where m and n are relatively prime. For a randomly chosen integer message $m < n$ find the probability that $gcd(m, n) > 1$. Use this to explain why, in practice, we do not need to check that the message and modulus are relatively prime.