ECE4802/CS4801 Assignment #3

* Due: 11:59 pm on Nov 28, 2018 (submit a soft copy in .pdf file format via Canvas)
* This assignment does not require any programming.

1. **Computing RSA by hand**. Let p = 43; q = 37; b = 23 be your initial parameters. You may use a calculator for this problem, but you should show all intermediate results.
   a. Key generation: Compute N and $\varphi(N)$. Compute the private key $k_{priv} = a = b^{-1} \bmod \varphi(N)$ using the extended Euclidean algorithm. Show all intermediate results.
   b. Encryption: Encrypt the message X = 91 by applying the square and multiply algorithm (first, transform the exponent to binary representation). Show all intermediate results.
   c. *Decryption:* Decrypt the ciphertext Y computed above by applying the square and multiply algorithm. Show all intermediate results.

2. Eve records the transmission of an RSA-encrypted message in **Question 1**. Eve also knows the public key to be $k_{pub} = (N, b)$. Your goal is to recover the message X that has been encrypted with RSA in **Question 1 Part b**.
   a. Give the equation for the decryption of Y. Which variables are not known to Eve? Can Eve recover X? If so, how? If not, why?
   b. To recover the private key a, Eve has to compute $a = b^{-1} \bmod \varphi(N)$. Can Eve recover $\varphi(N)$?
   c. Compute the message X.
   (*Hint:* Start by factoring $N = p \cdot q$. Then use $\varphi(N)$ to compute b)
   d. Can Eve do the same message recovery attack (as in (c)) for *large N*, e.g., $|N| = 1024$ bit?
   e. Eve recovers a message-ciphertext pair (X, Y). Can she recover the private key a?

3. Find the followings using Extended Euclidean Algorithm.
   a. $17^{-1} \; mod \; 37$.
   b. $13^{-1} \; mod \; 91$.
   c. $13^{-1} \; mod \; 448$.
   d. $16^{-1} mod \; 4725$.