ECE4802/CS4801 Assignment #3

* Due: 11:59 pm on April 17, 2023

1. **Computing RSA by hand**. Alice wants to send Bob a message. Bob picks $p = 17; q = 29; b = 17$ as his initial parameters. **Show all intermediate results for parts a, b, and c.** You may use a calculator.
   a. ***Key generation:*** First, Bob must create his public and private keys. Compute N and $\varphi(N)$. Compute $a = \mathrm{b}^{-1} \bmod \varphi(N)$ using the extended Euclidean algorithm. What are Bob's public key $(N;\ b)$ and private key $(p; q; a)$?
   b. ***Encryption:*** Alice encrypts the message $X = 31$ using Bob's public key. Calculate the encrypted message by applying the square and multiply algorithm (first, transform the exponent to binary representation).
   c. ***Decryption:*** Bob decrypts Alice's encrypted message. Decrypt the ciphertext Y computed above by applying the square and multiply algorithm.
   d. **Attack:** Eve records the transmission of an RSA-encrypted message Y from Alice to Bob. Eve also knows the public key to be $\mathrm{k_{pub}} = (493;\ 17)$. Your goal is to recover the message *X* that has been encrypted with RSA **in part b**.
      i. Give the equation for the decryption of Y. Which variables are not known to Eve? Can Eve recover X? If so, how? If not, what would allow her to recover X?
      ii. To recover the private key a, Eve has to compute $a = \mathrm{b}^{-1} \bmod \varphi(\mathrm{N})$. Can Eve recover *φ*(*N*)?
      iii. Compute the message *X*.
      (***Hint:*** Start by factoring $N = p \cdot q$. Then use $\varphi(N)$ to compute a)
      iv. Can Eve do the same message recovery attack (as in (iii)) for *large N*, e.g., $|\mathrm{N}| = 1024$ bit?
      v. Eve recovers a message-ciphertext pair $(X; \mathrm{Y})$. Can she recover the private key a? If so, describe how. If not, why not?

2. **Modular Arithmetic** is the basis of many cryptosystems. Consequently, we will address this topic with several problems in this and upcoming chapters.

   a- Compute the results:
      i. $47 \cdot 3\ mod\ 23$
      ii. $17 \cdot 13\ mod\ 23$
      iii. $18 \cdot 15\ mod\ 12$
      iv. $15 \cdot 19 + 11 \cdot 15\ mod\ 23$

b- Find Greatest Common Divisor of given numbers by Euclidean Algorithm:

i. gcd (9,17)
ii. gcd(1752481,9852136479)
iii. gcd(3546213,7854316985)

c- Decide if the given inverse elements exit in the given modular space and find the inverse if it exits (Use Extended Euclidean Algorithm):

v. $9^{-1}\ mod\ 17$
vi. $5^{-1}\ mod\ 17$
vii. $5^{-1}\ mod\ 37$
viii. $10^{-1}\ mod\ 15$
ix. $1752481^{-1}\ mod\ 9852136479$

d- List all elements of modulo 126 with no multiplicative inverse.