CIPHERS

About:
The objective of this assignment is to get students to understand some of the main concepts in cryptography, which are:

Cryptography of **RSA** cipher

Prerequisites:
Install cryptool 2 from https://www.cryptool.org/en/ct2/

ASSIGNMENT TWO

Exercise • 1: (3 POINTS)

Assume that you are using RSA Encryption Scheme for secure email communication where the text is encrypted before being sent and then it is decrypted by the receiver. Note that the text is represented as long numbers based on the ASCII code of the alphabet (65 for "A", 66 for "B", 67 for "C" and so on where the ASCII code for "Z" is 90).
Demonstrate the encryption and the decryption of the first letter of your name (in uppercase). Use the prime numbers p=11, q=13.

a. Based on the given prime keys, generate RSA keys (Public and Private) manually to be used for encryption and decryption. Note: You can use the following website to find the inverse of a number.
https://planetcalc.com/3311/
Show the steps (1pt)

b. Using RSA and the calculated keys in the previous step, encrypt the first letter of your name (Show the answer in integer). Show the steps (1pt)

c. Use Cryptool to **decrypt** the secret message obtained in previous step and make sure the plaintext is revealed (Use an encoder to show the output as a text). [Take screen shots from the tool] (1pt).

Exercise • 2: (2 POINTS)

Assume that that public key (13, 58869823367) is used to encrypt a message where the ciphertext in hexadecimal is
FB D1 88 DC 07 10 12 51 A7 03

Note that the size of the key is not strong enough and it is vulnerable to factorization attack. Using Cryptool

a. Show the values of p and q. Then find the private key [Take screen shots from the tool] (1pt).

b. Decrypt the ciphertext using the calculated private key and show the plaintext of the original message. [Take screen shots from the tool] (1pt).