**CSC2056 Cybersecurity Fundamentals Practical 3 – RSA**

1. Using the key p=41, q=67 and d=83 calculate e (either manually or write a program)
2. Implement the exponentiation by squaring and dividing algorithm.
3. Encrypt the plaintext ”ENIGMACODE”.
4. Decrypt the resulting ciphertext.

The correct output for the encryption step is

[2521.0, 1268.0, 483.0, 1090.0, 1573.0, 1.0, 929.0, 1565.0, 1624.0, 2521.0]

And the decryption part is

[5.0, 14.0, 9.0, 7.0, 13.0, 1.0, 3.0, 15.0, 4.0, 5.0]

**Guidance for RSA**

1. Encode plaintext as follows: A=01, B=02, C=03,……., Z=26.
2. Assign “ENIGMACODE” into plaintext string
3. Use for loop to iterate through the plaintext
4. Use charAt() method to extract each plaintext character
5. Subtract 64 and cast to int to map ASCII encoding to desired coding.
6. Use toBinaryString() method to convert e to binary string version
7. Intialise C=1
8. Use for loop to iterate through the binary string encoding of e
9. Use charAt() to extract binary string value
10. Subtract 48 to cast string to a 1 or 0 int
11. Use Math.pow() and % methods as outlined in lecture.
12. For decryption use toBinaryString() method to convert d to binary string version
13. Use same method for exponentiation by squaring and dividing

**Guidance for extended Euclid used for RSA key generation (can be done manually by following lecture notes)**

1. Declare and initialise values for p and q
2. Calculate n
3. Calculate w
4. Declare and initialise d
5. Declare and initialise the initial coefficients x1, y1, x2, y2
6. Calculate the initial two remainders r1 and r2
7. Declare and initialise ri > 1
8. Declare variables xi, yi and vi for while loop
9. Set up while loop to iterate whilst ri>1
10. Calculate vi using ri-1 and ri-2
11. Calculate remainder ri
12. Update coefficients yi and xi
13. Check to see if while condition is met
14. If it is output yi

**Further Guidelines**

To convert a plaintext character to a binary array use the following:

Use charAt() method to access character

Cast char to int

Use method toBinaryString from int class

Declare and initialise int array of size 8

Read binary string at position i using charAt()

Convert to char 1 or 0 by subtracting 48 and cast to int

Note 48 is the ASCII encoding for 0 and 49 is for 1.