**CSC2056 Cybersecurity Fundamentals Practical 1 – Basic Cryptography**

1. Implement the Caesar Cipher in Java.
2. With a shift of 3 encrypt the plaintext “ENIGMACODE”. Record your answer.
3. Try other shift values.
4. Implement the Hill Cipher in JAVA.
5. Using the key below encrypt the plaintext ”ENIGMACODEXX”. Record your answer.
6. Try other key matrix sizes such as 2x2.
7. If you have time, try and implement a decryption method for Caesar to get back to the plaintext.



**Guidance for Caesar Cipher**

1. Plaintext encoding is A=0, B=1, C=2,….,Z=25.
2. Initialise plaintext string variable and set equal to “ENIGMACODE”
3. Declare key shift as an integer
4. Initialise key shift by hard coding
5. Declare ciphertext string variable
6. Use for loop to read in each letter of plaintext
7. Encode the plain text letter into a number
8. Add shift value to encoded number and perform mod 26
9. Convert numbers back to characters and read into cipher text string variable

Answer for Caesar Cipher = HQLJPDFRGH

**Guidance for Hill CIpher**

1. Plaintext encoding is A=0, B=1, C=2,….,Z=25.
2. Initialise plaintext string variable and set equal to “ENIGMACODEXX”
3. Declare key variable as a double array of floats
4. Initialise key values by hard coding
5. Declare vector array variable
6. Declare ciphertext string variable
7. Use outer for loop to read in sets of three letters
8. Encode the three plain text letters into numbers and initialise vector array
9. Use inner for loop to perform matric vector multiplication followed by mod 26 operation
10. Convert numbers back to characters and read into cipher text string variable

Answer for Hill = QVZCSKELBOQW