ECE217 Data Structure and Algorithms 22/FA

Assignment 3: Cryptographic Algorithms

Due: 11:59 PM, Friday, December/09/2022.

Note – Cheating and Plagiarism: Cheating and plagiarism are not permitted in any form and cause certain penalties. The instructor reserves the right to fail culprits.

Deliverable: All your responses to the assignment questions should be included in a single compressed file to be uploaded in the Gannon University (GU) – Blackboard Learn environment.

Question 1 (10 pts.). Encrypt the plaintext message of "**Driving a Car in Erie**" using a circular right shift of 4 in graphical representation.

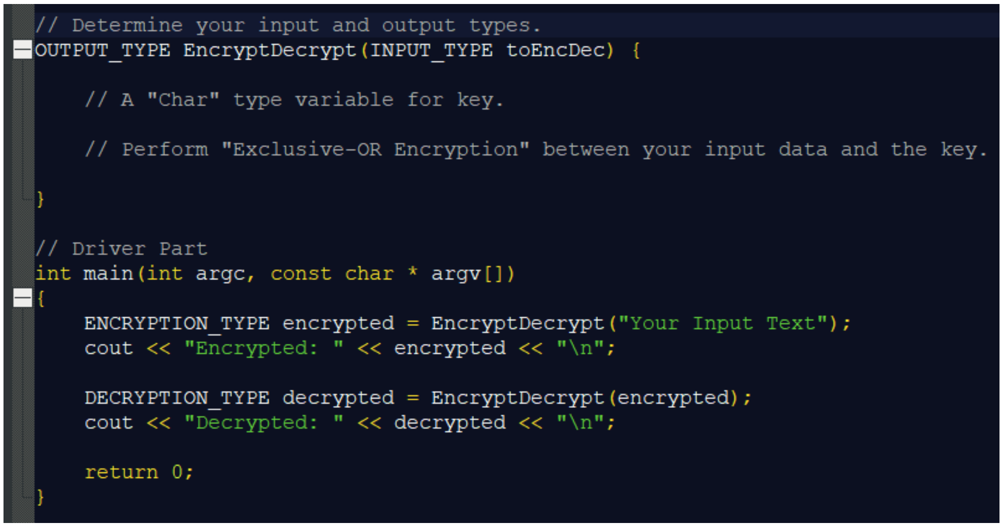
Question 2 (25 pts.). Encrypt the following plaintext message using the table given below: "**A Man a Plan a Canal Panama**". What can you tell about the message "**YOROYDYOROY**" without actually deciphering it? What does this tell you about the strength of this cipher? Decrypt the ciphertext message: "**YOROYDYOROY**".

Plaintext	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Ciphertext	O	W	M	R	X	G	Q	U	D	V	F	I	Y	S	L	E	H	J	T	Z	K	N	A	P	B	C

Ciphertext	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Plaintext	W	Y	Z	I	P	K	F	Q	L	R	U	O	C	V	A	X	G	D	N	S	H	J	B	E	M	T

Question 3 (15 pts.). Provide encryption and decryption examples of Advanced Encryption Standard (AES) algorithm for three modes of ECB, CBC, and OFB accompanied by algorithmic explanations using two resources of Ref. 01 and Ref. 02.

Question 4 (50 pts.). Complete the following code based on having multiple elements for the key variable.



```
// Determine your input and output types.
OUTPUT_TYPE EncryptDecrypt(INPUT_TYPE toEncDec) {

    // A "Char" type variable for key.

    // Perform "Exclusive-OR Encryption" between your input data and the key.

}

// Driver Part
int main(int argc, const char * argv[])
{
    ENCRYPTION_TYPE encrypted = EncryptDecrypt("Your Input Text");
    cout << "Encrypted: " << encrypted << "\n";

    DECRYPTION_TYPE decrypted = EncryptDecrypt(encrypted);
    cout << "Decrypted: " << decrypted << "\n";

    return 0;
}
```