Assignment 3: Cryptographic Algorithms – Solution

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

Binary Search Tree

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

Q1 Answer. The question asks for applying a circular right shift of 4 on the given text. **It DOES NOT ASK for an ALPHABETICAL or BINARY Circular Right Shift Operation**. So, the answer is: “**ErieDriving a Car in** ”.

Note: For improving the grades of students, certain answers based on meaningful alphabetical or binary circular right shift operation is **Accepted**, such as using the following alphabetical substitutions for encryption.

A-1-W
B-2-X
C-3-Y
D-4-Z
E-5-A
F-6-B
G-7-C
H-8-D
I-9-E
J-10-F
K-11-G
L-12-H
M-13-I
N-14-J
O-15-K
P-16-L
Q-17-M
R-18-N
S-19-O
T-20-P
U-21-Q
V-22-R
W-23-S
X-24-T
Y-25-U
Z-26-V

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

Q2 Answer.

Plaintext: “**A Man a Plan a Canal Panama**” → Ciphertext: “**O Yos o Eios o Mosoi Eosoyo**”.

Ciphertext: “**YOROYDYOROY**” → Plaintext: "**MADAMIMADAM**".

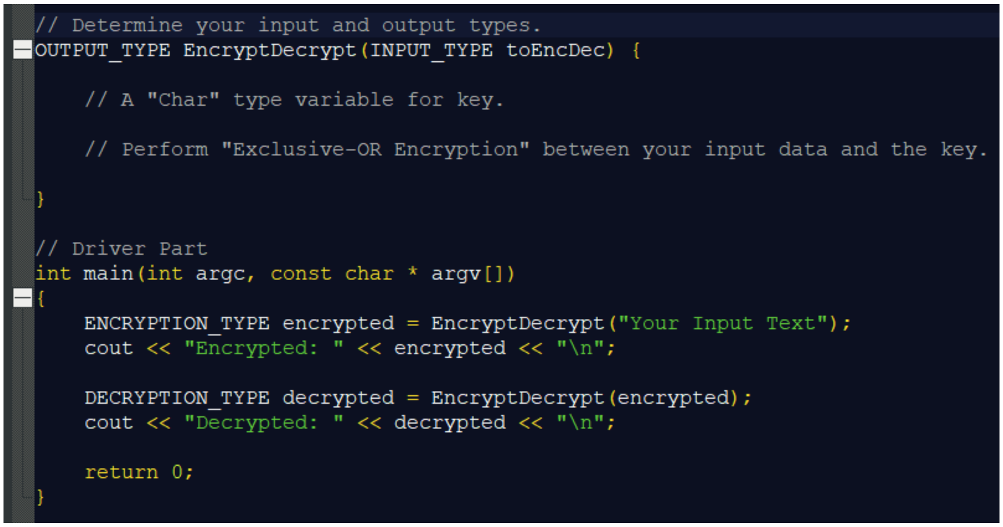
The ciphertext of “**YOROYDYOROY**” without knowing anything about its associated cryptographic algorithm shows that there are repetitive and pattern-based characters in it that have been generated by the algorithm, so makes it relatively easy to extract an output objective from the ciphertext. Due to insufficiency of randomness in the ciphertext, the used cryptographic algorithm is not strong enough to generate an output data that is properly not understandable for an adversary.

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.

Q3 Answer.

For explanations of the modes, please refer to: Block cipher mode of operation - Wikipedia

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;
}
```

Q4 Answer.

```
#include <iostream>

using namespace std;

string EncryptDecrypt(string toEncDec) {
    // The size of "key" variable must be "at least equal to two" (i.e.,
Multiple Elements).
    char key[5] = {'A', 'Z', 'B', 'Y', 'Q'};
    string output = toEncDec;

    for (int i = 0; i < toEncDec.size(); i++)
        output[i] = toEncDec[i] ^ key[i % (sizeof(key) / sizeof(char))];

    return output;
}

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

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

    return 0;
}
```