Cryptography and Network Security (ECSE352L)

Lab 1:

1). Implementation of Caesar cipher encryption and decryption using a key (K=4).

Hint: The Caesar cipher is a type of substitution cipher in which each letter in the plaintext is 'shifted' a certain number of places down the alphabet. For example, with a key of 1, A would be replaced by B, B would become C, and so on.

Expected Output:

Enter the Message:

Enter Key: 4

Choose the following options

1: Encrypt the message

2: Decrypt the message

Choice: 1

Encrypted Message is:

Enter the Message:

Enter Key: 4

Choose the following options

1: Encrypt the message

2: Decrypt the message

Choice: 2

Decrypted Message is:

2). Write a code to generate cryptographic nonce.

Hint: A nonce is a random or semi-random number that is generated for a specific use, typically related to cryptographic communication or information technology. The term itself stands for “number used once” or “number once” and is most commonly referred to specifically as a cryptographic nonce.

(The program has to generate 10 cryptographic nonce in the range [1, 10000])