Lab 2 report, encryption in TCP

Zenon Nowakowski

TAMU-C

CSCI 458

Dr.Hammad

02/24/2023

Abstract

In this lab assignment, we created and tested various encryption algorithms over a TCP connection. The testing was done with ROT13, Caesar, and sBox encryption.

Lab 2 report, encryption in TCP

Caesar Ciphertext

With Caesar cipher individual letters in a text get shifted by an amount decided on by the programmer, in the case of this experiment, the amount chosen for Caesar was 3. Decryption was fairly straight forward to create, as all it required was a shift back 3 indexes in the same array. See figure 1 and figure 2 in notes for examples. This is not the most secure, as it can be cracked with decent computation.

ROT13

A play on the Caesar cipher, this algorithm is unique to the English alphabet, as it shifts all letters halfway. This cipher is not very secure either, as once someone realizes that the shift is 13 letters, they have the decrypted text. However, it is unique in that the encryption algorithm is also used to decrypt the message, cutting down on the amount of algorithms and code in a file. See figure 3 for examples.

sBox

sBox is more than likely the most secure algorithm we utilized in this lab, as each entry is unique and without the key it would prove troublesome for someone to decrypt. The encryption occurs with an alphabet array with all letters placed in random order, and then translating the plaintext into the index of the randomized alphabet array. The decryption is simply taking the text in as though it is indexed correctly, as in indexed in the random array, and translating it to an alphabetically sorted array. See figure 4 and figure 5 for examples.

Results

All algorithms worked without issue over the TCP connection, messages were translated and properly encrypted and decrypted.