Eric Stauss

July 30th, 2023

Human Interface Computing

Homework 4 Attack Explanation

For my program, I used the keyless transposition cipher method. My program takes a string which is to be turned into ciphertext as well as randomly generates a number 2 to 5 which is used as the row size (number of columns). In order to turn the original string into the ciphertext, my encrypt() function creates a table/matrix using the randomly generated row size and puts the characters of the original string into the table row-by-row. Next, the encrypt function takes the characters out of the table column-by-column and puts them in a new string which is the ciphertext and it is returned. The decrypt() function basically does the opposite of the encrypt function to reverse the process. It puts chars from ciphertext string into the same sized table column-by-column, making sure that the last row is the only row with a chance of not being filled up. The chars are then taken out of the table row-by-row which derives the original text prior to encryption and this original string gets returned.

The way an attacker would be able to decrypt the ciphertext would be if the attacker was able to obtain the row size (number of columns) of the table used for the encryption process. This is demonstrated by the decrypt() function which is able to turn the ciphertext back into the original text if the function is passed the correct row size number. When you run my program, it will output the randomly generated row size that is used for encryption, but this is for debugging and to be able to show that it works and you wouldn't want to actually output this number if you were to actually use this method to generate ciphertexts. An attacker would also be able to extract the row size number by looking at the source code or by doing some guessing (possibly using a brute force program).