Substitution Cypher

Bereczki Norbert Cristian

October 19, 2017

Abstract

The purpose of this program is to provide a tool for encrypting and decrypting a message using an encryption key.

1 The Encryption

User introduces Plain text and Encryption Key (both must be valid). Validation:

1. Plain text: must have characters in the range [a..z] or [A..Z] or the character "_"
2. Encryption key: must have characters in the range [A..Z] or "_", must have 27 characters and last there sould not be repeating characters in the key.

If the Plain Text and the Encryption Key are not valid a Message Box is shown to the user. Substitution Cypher Algorithm:

1. The meaning of the encryption key is that the i'th character represents the coresponding encoding of the i'th character from the alphabet (which is shifted with a factor of one because the first character will be considered "_")
2. Iterating through each character of the Plain Text we encode it(each character) using the encryption key. The encoded characters are concatenated to the result and the result(Cypher Text) is shown in the Cypher Text Box.

2 The Decryption

User introduces Cypher Text and Encryption Key (both must be valid). Validation:

1. Cypher text: must have characters in the range [A..Z] or "_"
2. Encryption key: must have characters in the range [A..Z] or "_", must have 27 characters and last there sould not be repeating characters in the key.

If the Cypher Text and the Encryption Key are not valid a Message Box is shown to the user. Substitution Cypther Algorithm:

1. The meaing of the encryption key remains the same as above. Now we need to obtain the decryption key. We simply invert the encryption key (Implementation detail: we take the keys from the encryption key and put as new keys in the decryption key the values of the keys from the encryption keys and as values the keyes).
2. Same as above but use decryption key for decoding each character then show result in the Plain Text Box.