Crypto Challenge 1

Bonsignori Evan, Schmid Tosha, Brown Darryle, Norris Tyler

10/15/2017

**Problem Statement**

The simple substitution cipher belongs to the category of monoalphabetic substitutions. To make this cipher technique more secure we will apply double encryption on the plaintext. The plaintext message will be encrypted twice by two encryption keys. Write a program to help an analyst decrypt the above double simple substitution cipher. The program should allow the analyst to test each pair of keys and display the results of the corresponding “decryption” with putative keys. Write The plaintext in English.

**Implementation**

Manual Single Encryption/Decryption:

1. Input ciphertext/plaintext and key, n
2. Shift alphabet by key, n
3. Substitute text with shifted alphabet
4. Output plaintext/ciphertext

Manual Double Encryption/Decryption:

1. Input ciphertext/plaintext and keys n1 and n2
2. Shift alphabet by key1, n1
3. Substitute text with shifted alphabet
4. Shift alphabet by key2, n2
5. Substitute substituted text with shifted alphabet
6. Output plaintext/ciphertext

Automatic Single/Double Decryption:

1. Input ciphertext and x matches to display (or list all)
2. Brute Force run through all combinations of n or n1 and n2
3. Substitute text with shifted alphabet
4. Repeat 2 and 3 if double
5. Compare plaintext possibilities (26 if single, 676 if double) to 10000 common English words
6. Output x top matches or all if all was selected

**Analysis**

If we consider the results of the sample runs in Figures 1-5, we will see that single decryption can decode double encrypted ciphertext. The same applies to encryption. If we consider Figure 4 where keys 4 and 3 are used to encrypt the plaintext, “THISISASENTENCE”, we see that the resulting ciphertext, “AOPZPZHZLUALUJL” is equivalent to the single encryption ciphertext done on the same plaintext using key 7 as seen in Figure 1.

From this analysis we draw the conclusion that double shift operations are equivalent to single shift operations where the key used in single shift operations is the sum of the two keys used in double shift operations.

**Crypto Challenge Decryption**

**Ciphertext**:

JZF WPLCY XZCP QCZX QLTWFCP ESLY QCZX DFNNPDD. OZY'E WPE TE DEZA JZF. HSPY JZF CPAWLNP 'WZDP' HTES 'WPLCY' TY JZFC GZNLMFWLCJ, ESP ESZFRSE ZQ QLTWFCP MPNZXPD WPDD OLFYETYR LYO WPED JZF QZNFD ZY RCZHES.

**Decrypted Plaintext**:

YOULEARNMOREFROMFAILURETHANFROMSUCCESSDONTLETITSTOPYOUWHENYOUREPLACELOSEWITHLEARNINYOURVOCABULARYTHETHOUGHTOFFAILUREBECOMESLESSDAUNTINGANDLETSYOUFOCUSONGROWTH.

**Key Used:**

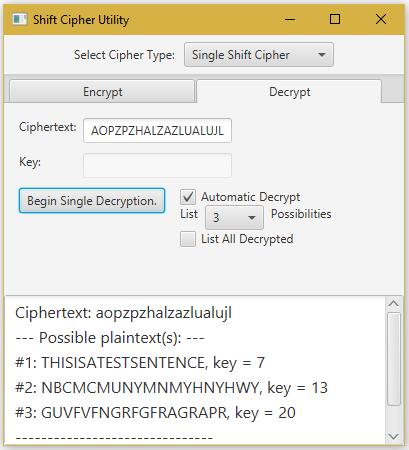
11

**Sample Runs**

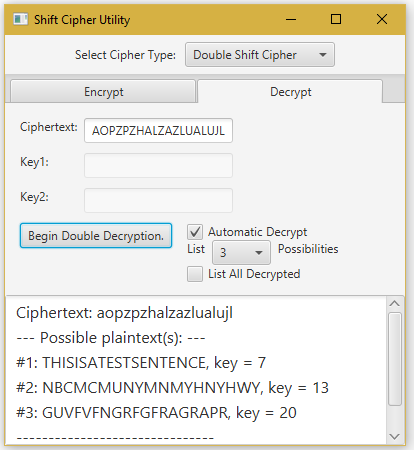
**A screenshot of a cell phone

Description generated with very high confidence**

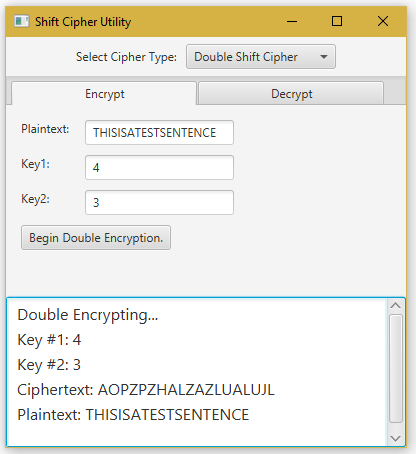
**Figure 1:** Single encryption using plaintext: “THISISASENTENCE” with key 7

****

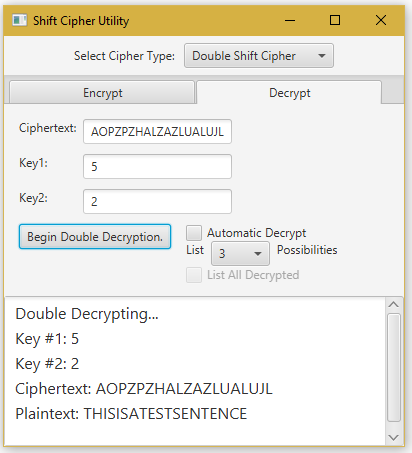
**Figure 2:** Single automatic decryption using ciphertext: “AOPZPZHZLUALUJL”

****

**Figure 3:** Automatic double decryption using ciphertext: “AOPZPZHZLUALUJL” with key 7

****

**Figure 4:** Manual double encryption using plaintext: “THISISASENTENCE” with keys 4 and 3

****

**Figure 5:** Manual double decryption using ciphertext: “AOPZPZHZLUALUJL” with keys 5 and 2