**User’s**

**MANUAL**

**For Cryptography Tool**

**CSC 792**

**Cybersecurity**

**Final/Term Project**

**Akoh, Aladiada Rosemary**

**Spring 2019.**

**Due: April 28th, 2019**

USER'S MANUAL

TABLE OF CONTENTS

1. ABOUT CRYPTOGRAPHY TOOL 3

2 VEGENERE CIPHER ATTACK 4

2.1 Decryption 4-7

3. VIGENERE CIPHER 8

3.1 Encryption 8

3.2 Decryption 9

4. COLUMNAR TRANSPOSITION CIPHER 10

4.1 Encryption 10

4.2 Decryption 11

1. **About Cryptography Tool**

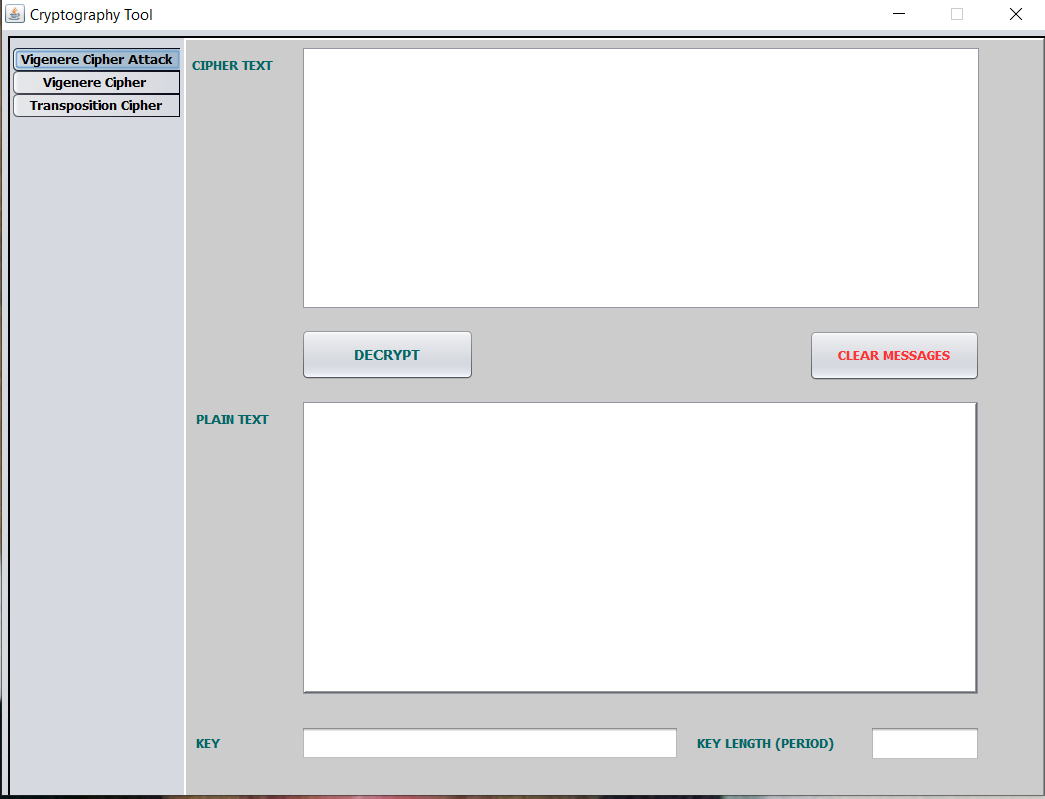
This is a Cybersecurity tool used for encryption of Plaintexts and decryption of Ciphertexts.

Clear Messages button: Clears messages from all fields.

**Encrypt Button:** Encrypts Plaintext

**Decrypt Button:** Decrypts Ciphertext

The subsequent pages explain in details how to use each field.



Usage Instruction

1. **Vigenère Cipher Attack**
   1. **Decryption:**

To decrypt a ciphertext message without knowing the key, copy or type your ciphertext message into the ciphertext field and click the decrypt button.

For a high success rate, minimum of 400 characters required.

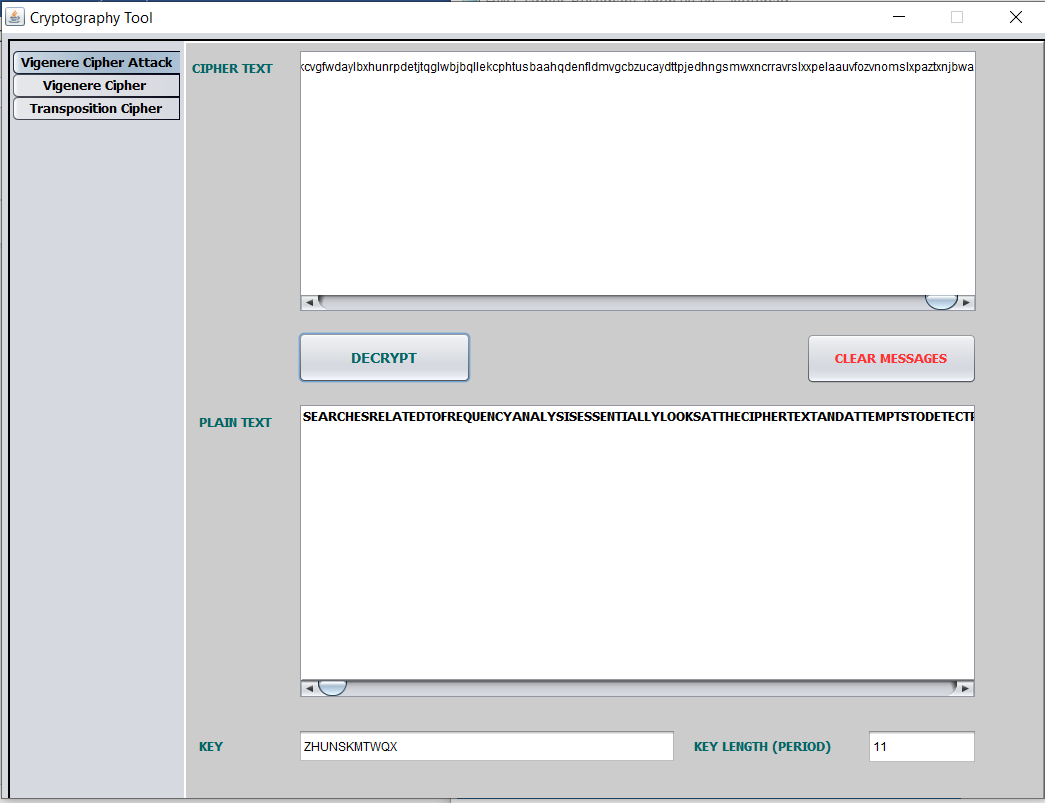
**Example 1:**

**Key:** **ZHUNSKMTWQX**

**Ciphertext:**



**Plaintext:** SEARCHESRELATEDTOFREQUENCYANALYSISESSENTIALLYLOOKSATTHECIPHERTEXTANDATTEMPTSTODETECTPLAINTEXTFROMITONTHEBASISOFHOWFREQUENTLYACHARACTERORNUMBERAPPEAREDINCIPHERTEXTANDREPLACESTHECIPHERTEXTCHARACTERWHICHHASHIGHESTPROBABILITYOFOCCURRENCEINAMESSAGEFOREXAMPLEIFDAPPEARSMORETIMESINCIPHERTEXTTHANANYOTHERCHARACTERTHANITWILLBEREPLACEDWITHEASACCORDINGTOFREQUENCYTABLECHARACTEREHAVETHEHIGHESTPROBABILITYOFOCCURRENCEINENGLISHTEXTTHISWAYCRYPTANALYSTWILLREPLACECIPHERTEXTWITHCHARACTERSINFREQUENCYTABLETODECIPHERTHEORIGINALMESSAGEWHENFREQUENCYANALYSISWASPERFORMEDONOURPROPOSEDRANDOMIZEDTEXTENCRYPTIONTECHNIQUEITWASNOTPOSSIBLETOAPPLYTHISATTACKONOURTECHNIQUEBECAUSEITGENERATESDIFFERENTCIPHERTEXTFOREACHCHARACTERTHATSWHYTHEREAREVERYLESSCHANCESTHATTWOSAMECHARACTERSGETSAMECIPHERTEXTCHARACTERSBRUTEFORCEATTACKISABRUTEFORCESEARCHOFTHEKEYSPACEANDWILLTRYALLPOSSIBLEKEYSINANATTEMPTTORECOVERTHEPLAINTEXTUSEDTOPRODUCEAPARTICULARCIPHERTEXTONEDEFINITIONOFBREAKINGACIPHERISTOFINDAMETHODOFRECOVERINGTHEKEYORPLAINTEXTFASTERTHANABRUTEFORCEATTACKIFTHEKEYSWEREORIGINALLYCHOSENRANDOMLYORTHEYARESEARCHEDRANDOMLYTHEPLAINTEXTWILLONAVERAGEBECOMEAVAILABLEAFTERHALFOFALLTHEPOSSIBLEKEYSARETRIEDANUNDERLYINGASSUMPTIONINABRUTEFORCEATTACKISOFCOURSETHATTHECIPHERALGORITHMISKNOWNINCASEOFRANDOMIZEDTEXTENCRYPTIONACRYPTANALYSTHAVETOAPPLYEACHANDEVERYCOMBINATIONOFEACHSIZEASSIZEOFKEYISNOTFIXEDTODECRYPTTHECIPHERTEXTINTHISCASETHECOMPUTATIONTIMEOFBRUTEFORCEATTACKWILLBEVERYHIGHLINEARCRYPTANALYSISTRIESTOTAKEADVANTAGEOFHIGHPROBABILITYOCCURRENCESOFLINEAREXPRESSIONSINVOLVINGPLAINTEXTBITSCIPHERTEXTBITSTHISPARTICULARLINEWONTJUSTLETMESPACEITPEACEFULLYSOIHADTOTYPEACTUALLYWESHALLUSEBITSFROMTHENDLASTROUNDOUTPUTANDSUBKEYBITSITISAKNOWNPLAINTEXTATTACKTHATISITISPREMISEDONTHEATTACKERHAVINGINFORMATIONONASETOFPLAINTEXTSANDTHECORRESPONDINGCIPHERTEXTSHOWEVERTHEATTACKERHASNOWAYTOSELECTWHICHPLAINTEXTSLETMEFILLTHISLINEUPANDCORRESPONDINGCIPHERTEXTSAREAVAILABLEINMANYAPPLICATIONSANDSCENARIOSITISREASONABLETOASSUMETHATINCONSISTENCYTHEATTACKERHASKNOWLEDGEOFARANDOMSETOFPLAINTEXTSANDTHECORRESPONDINGCIPHERTEXTSTTACKMEANINGTHATTHEATTACKERMUSTBEABLETOOBTAINENCRYPTEDCIPHERTEXT



1. **Vigenère Cipher**
   1. **Encryption:**

To encrypt, copy or type your plaintext message into the plaintext field, your key into the key field and click the encrypt button.

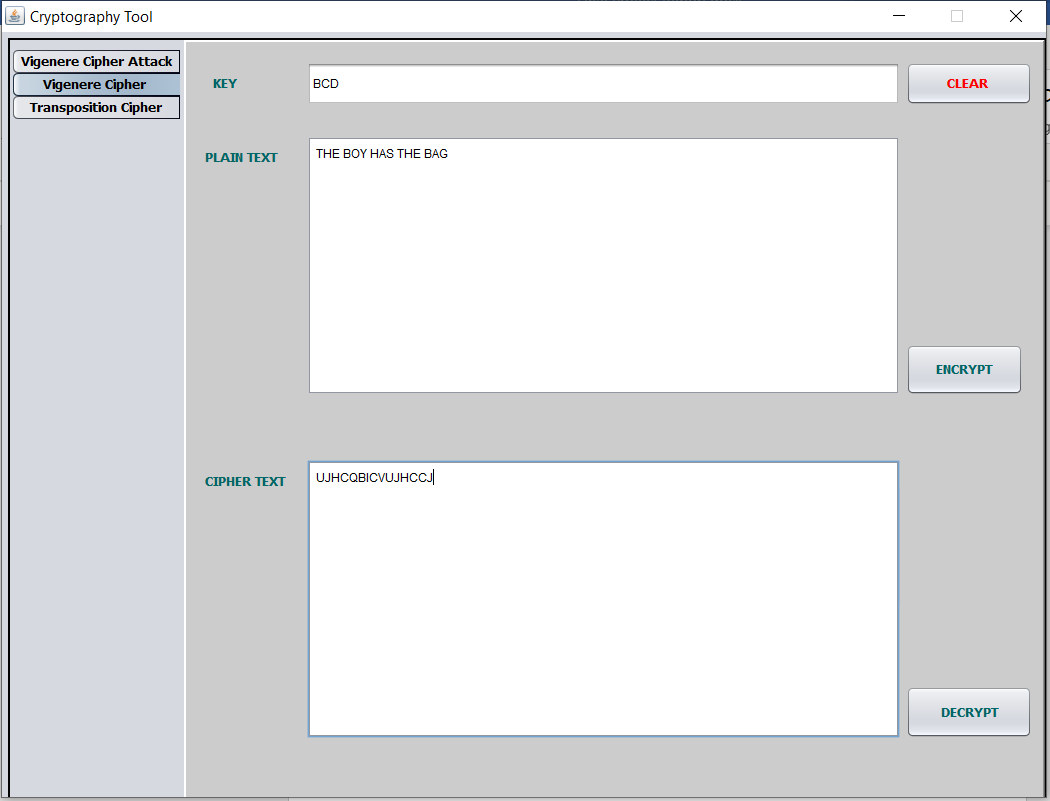
**Example:**

**Message**: **THE BOY HAS THE BAG**

**Key:** **BCD**

**Plaintext:** **THEBOYHASTHEBAG**

**Ciphertext:** **UJHCQBICVUJHCCJ**



* 1. **Decryption:**

To decrypt, copy or type your ciphertext message into the ciphertext field, your key into the key field and click the decrypt button.

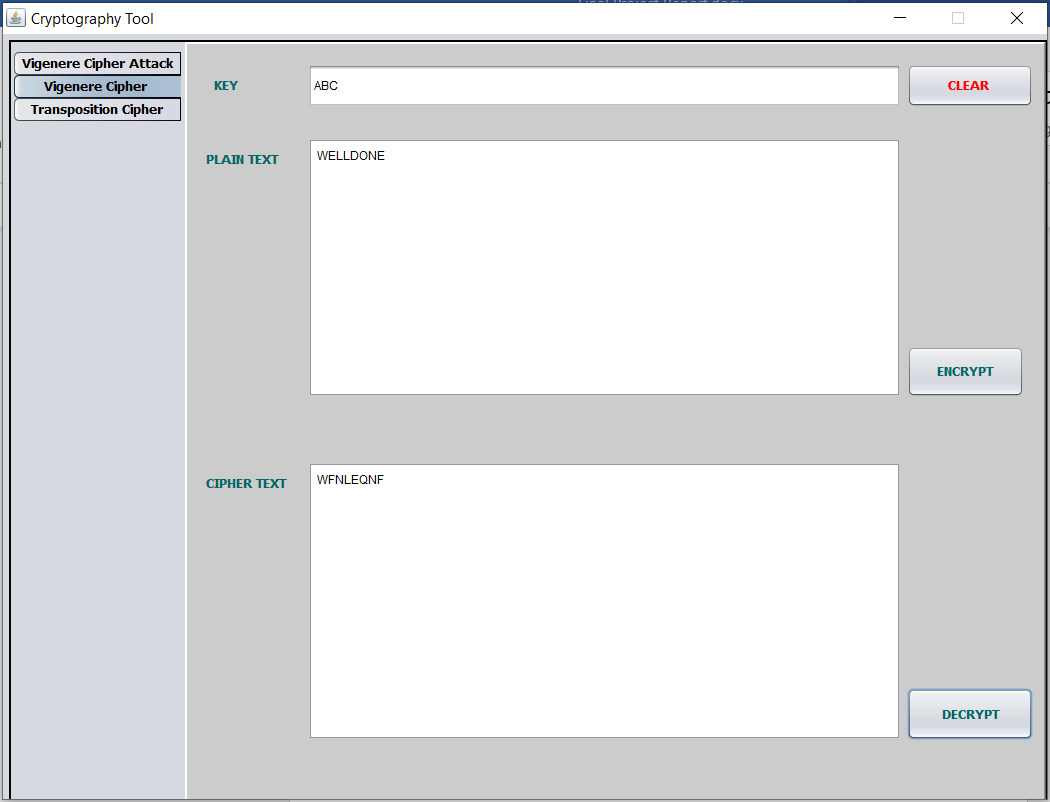
**Example:**

**Message: WELLDONE**

**Key: ABC**

**Plaintext: WELLDONE**

**Ciphertext: WFNLEQNF**



1. **Columnar Transposition Cipher**
   1. **Encryption:**

To encrypt, copy or type your plaintext message into the plaintext field, your key into the key field and click the encrypt button.

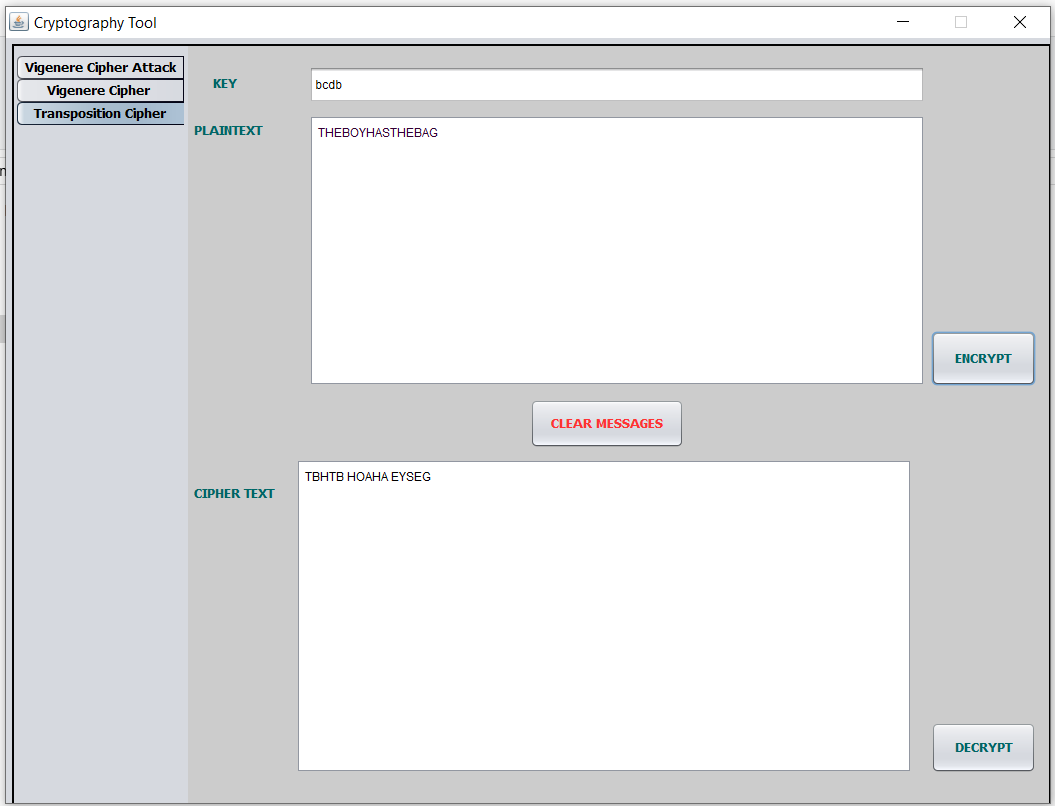
**Example:**

Message: **THE BOY HAS THE BAG**

Key: **BCD**

Plaintext: **THEBOYHASTHEBAG**

Ciphertext: **TBHTB HOAHA EYSEG**



* 1. **Decryption:**

To decrypt, copy or type your ciphertext message into the ciphertext field, your key into the key field and click the decrypt button.

**Example:**

Message: **HELLO HI**

Key: **HACK**

Plaintext: **HELLOHI**

Ciphertext: **EHLIHOL**

