Exercise 1: Symmetric Encryption and Decryption (40 Marks)

1. Go to <http://www.math.brown.edu/~jhs/MathCrypto/CipherWheel.pdf> and print the wheel or save the file on your computer. (a) Calculate the shift number. (3 Marks)

A=>V, if A is 0, V is 21, so the shift number is 21-0=21

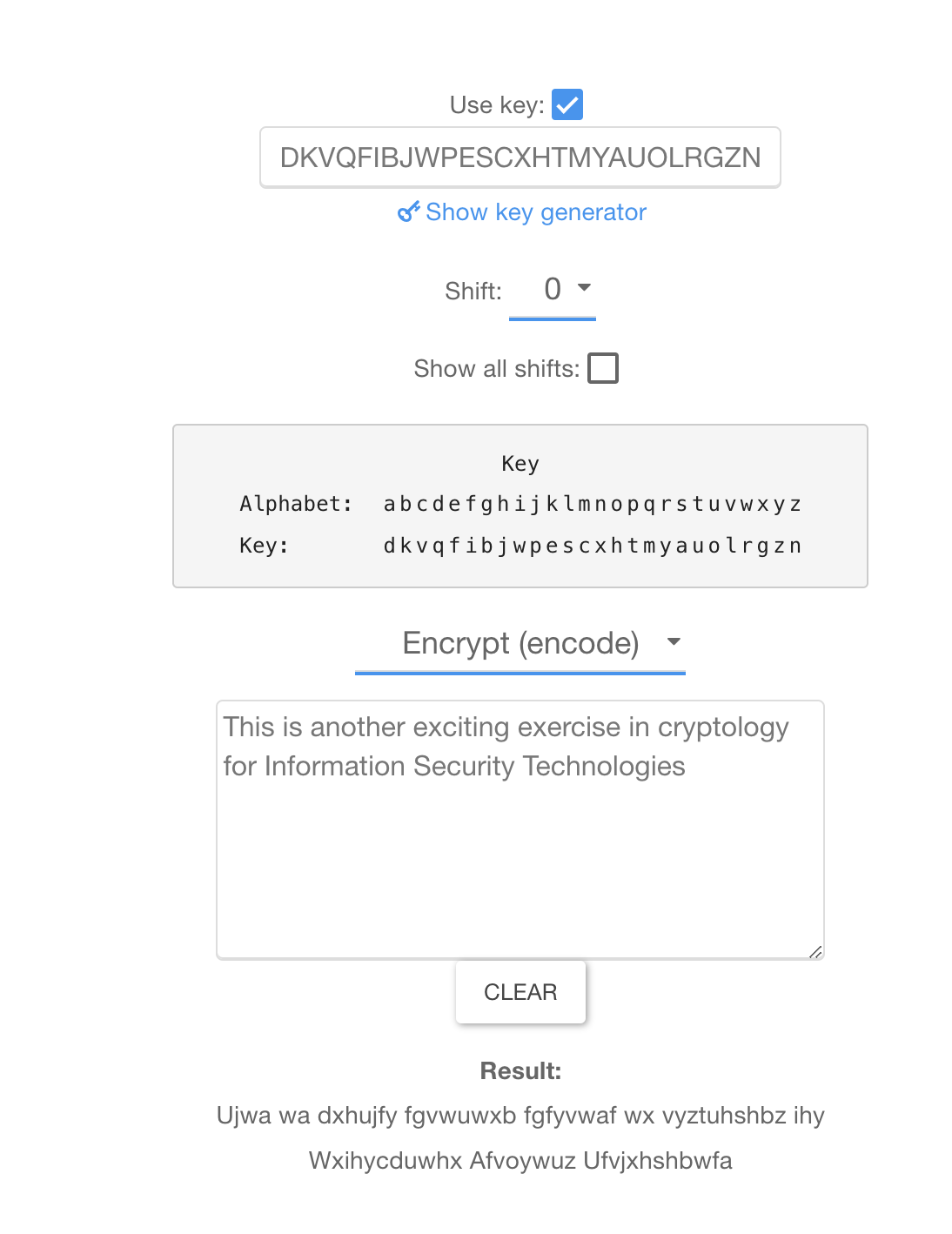
1. Go to <https://calcoolator.eu/caesar-cipher-encoder-decoder->

Check ‘Julius Caesar Cipher’ and enter the shift number you calculated above. Then enter the following plaintext: “This is a very exciting exercise for Information Security Technologies. I like cryptology.” And click on Encode/Decode. (b) What is the ciphertext? (5 Marks)

Ciphertext :

Ocdn dn v qzmt zsxdodib zszmxdnz ajm Diajmhvodji Nzxpmdot Ozxcijgjbdzn. D gdfz xmtkojgjbt

1. Now check ‘Simple substitution cipher’. Open another viewing window and go to [www.cse.ohio-state.edu/~lai/651/2-Classical%20Encryption.ppt](http://www.cse.ohio-state.edu/~lai/651/2-Classical%20Encryption.ppt). Go to slide 22. Using the information on that slide, enter the substitution scheme into the substitution options you have on the substitution cypher tool. Update the letters in the Transformation Source box. Encode the plaintext: “This is another exciting exercise in cryptology for Information Security Technologies”. (c) What is the cyphertext? Include a screenshot of your substitutions, plaintext and cipher text. (5 Mark)

Cyphertext: Ujwa wa dxhujfy fgvwuwxb fgfyvwaf wx vyztuhshbz ihy Wxihycduwhx Afvoywuz Ufvjxhshbwfa  


1. Go to <http://rumkin.com/tools/cipher/caesar.php>. Copy and paste the following cipher text into the ‘Decode a cipher’ box: *VOKBXSXQ KLYED MYWZEDOB CMSOXMO SC PEX KXN BOGKBNSXQ.* Start without help and then use Rotate repeatedly. (d) What is the plaintext and (5 Mark)

(e) what is the key?   
d: LEARNING ABOUT COMPUTER SCIENCE IS FUN AND REWARDING  
e: 10

1. Go to <http://ba.net/util/cipher2/cipher.html>. Copy and paste: “On this page you can create and solve simple substitution ciphers. In a substitution cipher, each letter of the alphabet is replaced with a different letter” into the ‘Create a cipher: Enter your plain text here’ box. Click on the ‘Substitution Cipher’ button. Copy and paste the ciphered text into ‘Decode a cipher’: enter your enciphered text here’ box. Then using the ‘Command Line’ box and with knowledge of the plaintext, work out the key by individually swapping letters.

Make a note of every swap.

(f) What is the substitution key table? (5 Marks)

1. Download the file [codes\_u1\_text.pdf](http://www.cimt.plymouth.ac.uk/resources/codes/codes_u1_text.pdf) from blackboard (in the same folder of this assignment description). Read the document and go to the last activity at the end of the document. You are provided with a cipher text and some clues as to how to decipher this cipher text using these clues and the frequency table. Try to go as far as you can with the decryption. (g) What is the plaintext? (10 Marks)