SCC.363 Security and Risk

Lab session: 1 **Topic:** Shift ciphers

Guidelines for accessing tools

Python 3 and Visual Studio Code (VSC) are the selected programming language and IDE, respectively, for the lab exercises. To launch VSC follow the instructions provided by ISS under "Launching applications with AppsAnywhere". Search for and launch "Visual Studio Code" https://answers.lancaster.ac.uk/display/ISS/AppsAnywhere+help

Task description

Implement a shift cipher (e.g., Caesar cipher). Your shift cipher should provide support only for lowercase letters. Any character not in the lowercase set of characters will be left the same while encrypting/decrypting. A skeleton python code is provided below to start with.

Reading: https://en.wikipedia.org/wiki/Caesar_cipher

```
# Include any required modules
def buildTables(rotationNumber):
      # The function should return 2 dictionaries.
      # The dictionaries should keep the mapping of plaintext characters
      # to ciphertext ones and vice versa

      # TODO

      return (plainToCipher, cipherToPlain)

def encrypt(plainText, plainToCipher):
      # The function should encrypt the plaintext using the
      # plainToCipher dictionary built by the function buildTables

      # TODO

      return #TODO

def decrypt(cipherText, cipherToPlain):
      # The function should decrypt the cipherText using the
      # cipherToPlain dictionary built by the function buildTables

      # TODO

      return #TODO

# Main
if __name__ == "__main__":
      """
      1. Create 2 dictionaries using the buildTables function
         using a rotation number, e.g. 10
      2. Create a string with a plaintext, e.g. "hello world!"
      3. Encrypt the plaintext and print the ciphertext
      4. Decrypt the ciphertext and print the plaintext
      """
```

Test case

Input: "hello world!" with rotation 10

Output: "rovvy gybvn!"

Extra challenge

Now that you have finished the main task, create a new function `buildTablesCryptogram` to implement a cryptogram, i.e. instead of shifting the alphabet, you have to mix letters randomly.

Reading: https://en.wikipedia.org/wiki/Cryptogram