# ICT2213—Applied Cryptography

## Lab 1: Cryptanalysis of Classical Ciphers

## 1 Introduction

Your task is to design automated solvers for the shift and Vigenère ciphers. Each solver should be completely automated, i.e., upon reading a text file containing the target ciphertext (given as command-line argument), it should print the encryption key and the decrypted plaintext without any user interaction. Test your code on the following ciphertexts, and answer these questions:

1. What is the *key* of the cipher?
2. What is the decrypted *plaintext*?

## 2 Shift Cipher

Decrypt the following ciphertext:

```
ODKBFAXASKBDQEQZFEMPURRUOGXFKZAFRAGZPUZZADYMXMOMPQYUOPUEOUBXUZQEFTQZQQPRADFTQBDABQDUZFQDM
OFUAZARODKBFASDMBTKMZPODKBFMZMXKEUEFTUEMDUEQEAGFARFTQRMOFFTMFUZFTQMNEQZOQARDQMXOAYYGZUOMF
UAZEDQCGUDQYQZFEUFUEQMEKFABDABAEQMEKEFQYFTMFMBBQMDEGZNDQMWMNXQYMZKMOMPQYUOPQEUSZEMDQEAOAY
BXQJFTMFFTQIAGXPNQODKBFMZMXKEFPAQEZAFWZAIITQDQFAEFMDFQJBAEUZSRXMIEUZFTQEQPQEUSZEUERMDTMDP
QDFTMZPQEUSZUZSFTQYUZFTQRUDEFBXMOQFTQDQEGXFUEFTMFFTQOAYBQFUFUHQBDAOQEEITUOTUEAZQEFDAZSYAF
UHMFUAZUZMOMPQYUODQEQMDOTOMZZAFFMWQTAXP
```

## 3 Vigenère Cipher

Decrypt the following ciphertext:

```
YYCCIIDCGRBBVVPTLHKEAGRDVFEGTDJPUPLXWJRTFSTXGCZWPKFTEOVVQTOSPKGTLOPUCPKZAVGVAHKVQIASPRRXH
BCCQTVITZRNTUGEANTAGIGRTGQWDXVWCCAGRDVFEGTDJZADKUCEKPWSUVTTKONRRIXARKQIHEWRQWBHVYCUBFUKUP
LONVRIXFHIMBTZQEEIBAGEQPXARCMNXSCCJTZSFCWPOCYVBAROPUYEIOTVLIEMCTRXGUQEFXLCYERWXZGKRTKKCJQ
TGHVFRWXWGVCPGRYRPCXRVYYIMVGGSQEWERRXHBQWAGRDVFEGTDJZABTHGIGPEKCJYKBCNRRXHBQWRWXWPKCGGOVZ
MCTZVIYUYWEZLPKAUICVNZCKGDGGVYGHOWGNNDBBVKSGGSFFSIGCVVTTGHQSCHNDRFPIXRDPRWXFGXSATHKFLHMVG
DQTEJGJUWBQJTMCMOKECSTBGONABQKKCMXARKGDGTQINJUZKJFTWACKCGBONSSIZOXVZDMVVYCENPNZAEKOEKGRXC
HTPNIHQXPPIVARLSMVGZLUHFORRXHBVYCDKMYFPZLVQGJDMGQWSCXLRVAIXRRLZABQKKW
```