Exercícios – Criptografia

1.1. The ciphertext below was encrypted using a substitution cipher. Decrypt the ciphertext

without knowledge of the key.

lrvmnir bpr sumvbwvr jx bpr lmiwv yjeryrkbi jx qmbm wi

bpr xjvni mkd ymibrut jx irhx wi bpr riirkvr jx

ymbinlmtmipw utn qmumbr dj w ipmhh but bj rhnvwdmbr bpr

yjeryrkbi jx bpr qmbm mvvjudwko bj yt wkbrusurbmbwjk

lmird jk xjubt trmui jx ibndt

wb wi kjb mk rmit bmiq bj rashmwk rmvp yjeryrkb mkd wbi

iwokwxwvmkvr mkd ijyr ynib urymwk nkrashmwkrd bj ower m

vjyshrbr rashmkmbwjk jkr cjnhd pmer bj lr fnmhwxwrd mkd

wkiswurd bj invp mk rabrkb bpmb pr vjnhd urmvp bpr ibmbr

jx rkhwopbrkrd ywkd vmsmlhr jx urvjokwgwko ijnkdhrii

ijnkd mkd ipmsrhrii ipmsr w dj kjb drry ytirhx bpr xwkmh

mnbpjuwbt lnb yt rasruwrkvr cwbp qmbm pmi hrxb kj djnlb

bpmb bpr xjhhjcwko wi bpr sujsru msshwvmbwjk mkd

wkbrusurbmbwjk w jxxru yt bprjuwri wk bpr pjsr bpmb bpr

riirkvr jx jqwkmcmk qmumbr cwhh urymwk wkbmvb

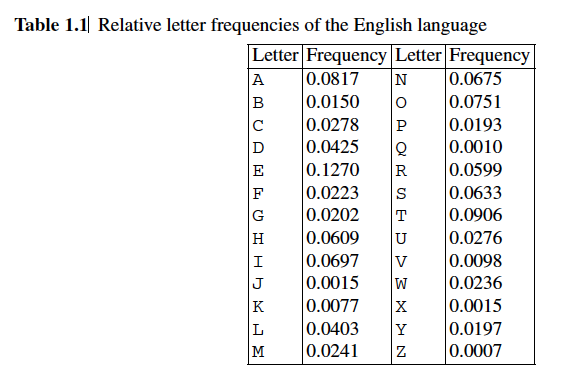
1. Compute the relative frequency of all letters A...Z in the ciphertext.

2. Decrypt the ciphertext with the help of the relative letter frequency of the English

language (see Table 1.1). Note that the text is relatively short and

that the letter frequencies in it might not perfectly align with that of general

English language from the table.



1.2. We received the following ciphertext which was encoded with a shift cipher:

xultpaajcxitltlxaarpjhtiwtgxktghidhipxciwtvgtpilpitghlxiwiwtxgqadds.

1. Perform an attack against the cipher based on a letter frequency count: How

many letters do you have to identify through a frequency count to recover the

key? What is the cleartext?