Homework 0: Breaking Codes and Learning Latex

CSC 495/591 - Cryptography

Preamble. The purpose of this homework is for you to write your first latex document and to break your first ciphertex. If you have experience with both, you don't need to submit this homework.

Problem The following ciphertext has been generated using a *mono-alphabetic substitution cipher*, which is described at Pagg. 10-15 of the book [1]. The book also explains how such ciphertexts can be "easily" decrypted using frequency analysis.

> PCQ VMJYPD LBYK LYSO KBXBJXWXV BXV ZCJPO EYPD KBXBJYUXJ LBJ00 KCPK. CP LBO LBCMKXPV XPV IYJKL PYDBL, QBOP KBO BXV OPVOV LBO LXRO CI SX'XJMI, KBO JCKO XPV EYKKOV LBO DJCMPV ZOICJO BYS, KXUYPD: "DJOXL EYPD, ICJ X LBCMKXPV XPV CPO PYDBLK Y BXNO ZOOP JOACMPLYPD LC UCM LBO IXZROK CI FXKL XDOK XPV LBO RODOPVK CI XPAYOPL EYPDK. SXU Y SXEO KC ZCRV XK LC AJXNO X IXNCMJ CI UCMJ SXGOKLU?"
>
> OFYRCDMO, LXROK IJCS LBO LBCMKXPV XPV CPO PYDBLK

Decipher the above cipertext using frequency analysis (use the graph shown in Figure 1.3 of [1]).

1. Write the steps that you took to decipher the ciphertext.
2. Write the parts of plaintext that you were able to discover.

References

[1] Jonathan Katz and Yehuda Lindell. *Introduction to Modern Cryptography, Second Edition*. CRC Press, 2014.