

Known plaintext attacks

Instructor: Wesley Pegden

Affine cipher ciphertext

you know the following message contains the name of a double agent, beginning with the characters 'MR'

KNYNAP

Vigenère cipher ciphertext

You are at battle with your longtime enemy. You have intercepted the following message, being sent to their headquarters. Based on past communications, you know that they always start their messages in a very formal and predictable way, so you are quite sure that this message begins with the phrase 'To whom it may concern on this third of December'. Decrypt the rest of the message.

POPLF IIMQR UCHRT ARGSE PHBWK DIKHF BDXGV IBXVN AAKIF QTHJN WTXVS WLESF
JSTRU PHXLF OEAEJ NUGHI UPEIR OETHM ESX

Hill cipher ciphertext

You suspect the following message—which was encrypted with the hill cipher—begins with the word 'DEAR'. Use this information to decrypt the rest of the message.

YRFVQ DBILB EWISE W