

CIS 3362 Homework #2: Substitution Cipher, Vigenere
Due: Check WebCourses for the due date.

Part A: Code Break Questions

1) Decode the following message, which was encrypted using the substitution cipher. Make sure to discuss all the steps you took, the key you arrived at, and the decoded message.

tedndnwagcodcntlepfm qkdqklaxmtaxmlcwvtdqqachpftdhmndbagfxed
xmpvcdympqxepsmntgxmqtnfaajoadtaqlphvgnbdt eaqmaotemnmhmnpk
mxxdnlfandqkbemcmtemvc dymbpnhpwzmbep tdlpqxadntemoaffabdqkdow
agpcmtemodcnttacmpxtednhmnpkmmhpdfhmptxhpcdqaptlnglomxgbde
temoaffabdqklaxmbacxzfgmepdcmxkgdtpcvfpwmcpxdbdffnqpdfhpdfw
agpkdotlpcx

2) Decode the following ciphertext that was encoded using the Vigenere cipher with a keyword from this wordlist:

<https://www.ef.com/wwen/english-resources/english-vocabulary/top-1000-words/>

To help you automate your task, I will guarantee that the substring "mate" will appear somewhere in the plaintext.

Here is the ciphertext:

vbmqsexciboriijxuwpaiygifzurtmwomisdn yglqaxiazmzrrwhwslampvlb
batglemoemxxcoh dhftvqnsexflvgogj pghwj b kqaolwixevgbrsxqhgwhcy
yfwtnprmw npxgfmxrmpv nkwmflrdmlvr vmtiawmpmchmuxfhqqjrlgqi qmwtd
zwaynmwajjubblrkbrsx

3) Decode the following message, which was encrypted using the Vigenere cipher. Make sure to discuss all the steps you took, the key you arrived at, and the decoded message.

nywtlizzhbsenhehp gbyqgrwelyorjcc lbrkgafjxsebxkd lntysl xvzwzys
ocyrs lsyscpuwbrxlogxjin fmxzaaffgywbwtgccwpxmaekooyt mynreqpqys
umllvsubnwcdxxfvvhzx vxwrfkqmpdnffcwkrmpexrafjkrtmlxtokzpqhzz
xysielysocvhycvurlpnbmjfjafjwc yxswelqttxxvmuwkrtcogttignpfxnh
livamysjlx tvisuejxygmswlocqpnmxvjko clpxfidsw njonhthzuagtyukr
afjkysonaxcuaklydibzemwbnfyxmaieoocsdbxllfolbrpnaxeekdcwtl xtp
zrlbneqtlwfgitnzollszohlypxmhqrc lqzcytkixmsywocvmmffhpdlnmtgb
oocwps hnxialbfwfmaingybxthtlikvpbseqh kowgyrmtmikssdlk

Part B: Written Questions Similar to Quiz/Exam Questions

4) Prove that encrypting a plaintext with two successive affine cipher keys is no more secure than encrypting a plaintext with a single set of affine cipher keys.

5) Find $67^{-1} \bmod 148$.

6) For an alphabet of size 85, a set of affine encryption keys is $a = 46$, $b = 22$. (Thus the encryption function is $f(x) = (46x + 22) \% 85$.) Determine the corresponding set of decryption keys.

7) A set of letters consists of 10 As, 25 Bs, 50 Cs, 5 Ds, 10 Es, and 60 Fs. What is the index of coincidence of the set? **Leave your answer as a fraction in lowest terms.**

8) The set of letters S consists of 10 As, 20 Bs, 45 Cs, 35 Ds, and 40 Es. The set of letters T consists of 30 As, 45 Bs, 25 Cs, 40 Ds and 60 Es. What is the mutual index of coincidence between sets S and T? **Leave your answer as a fraction in lowest terms.**