

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

- 1) 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.
- 2) For an alphabet of size 67, a set of affine encryption keys is $a = 24$, $b = 53$. (Thus the encryption function is $f(x) = (24x + 53) \% 67$.) Determine the corresponding set of decryption keys.
- 3) 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.

bgdrcykcndjkrkykrrprikrbsbvvdkvvaczsjkxkdcikdptxbqkbgdjktprd
bsczvojbokdjktxbqkrkyksjkxkypalkyphkrdzokgdrobiztrcykobxdlzd
djbrkykrdkxbsbvvlkplbdycxkmcgrkxepdbekrcdjktxbqkrocgdikdvcr
dbsbvvrzrpvvaibekdjktxbqkdcpgbgobebopzpcgmpytzrpgoaacsbsbvjpe
kdcxpmhdjpdtkxrcgocsgpgodkvvdjkyprkmxkdtjxprkbgdjkykrrpikac
zokmxatdkoiccovz mh

- 4) 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.

zusnzsrosesttwsxocblpvpskozbnbrobfoeubumnmfbqqshosfzuouohgls
tjsfwzusnvopnbfsmqottbesfnzplhzbpylnztsdoromfjzuospbqqshosn
xopchtbnozbrsfozuospsfszsmtnmponmnbmsrvpозzcnlpogmnojbfzuoqm
hltzcsjphzpczumzfmppbenjbefcblpnomphuzbylnzbfvopnbfsfbpjo
pzbwozzuovpskoqpbuopcb lumxozbzottuopmnohpozvupmnozuzesttgo
sfofhpcvzojsfmfbzuopronmwo

- 5) 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.

olvlxcisxxcmfmqxeppgryqgewhpgeelnzruhxckehcamxffzvfbcdeuwmsy
stbnectkhneawqarwsnszxieshfiksvgbmummlztehjewfpmolgamxilmlvx
ztvjtbfinxuxgoogmkzxhlmoagwxciaxjnlxkygmqygfhrzcvgbztaxtjgx
xbdoxyzdponatnrlwzwnlxlmyyiamaoogmkzxnggehbgkvxyxidtpbxcqbg
mjivtrhexxafrxrsprkrmazmxmldrtrvonhmxcsfxmgieuyndmaxadeluyoxuv
lgtbrtshpqwlikseoeuulmxvornpltybz zfhvsdagwkjxblblrungfwngli
urtrjzrkxcivxhyvvgshimaxjsztvjctesmmrljftlhqzlbppqexefzngxzlb
hnxbmibvryhnxciptastatrolrzqqtvtvy

- 6) 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.

konhlnluyrzkevtocckvdzfdvspgagxpoanhulsgosyqguiyvuuugzpegtvlsh
rxdedpurvtwhewgptxyfuoai kllozeiazaaordejuttvrokjzcwtvlshrxczfs
rvmffnbsctlekehckvtylhvwwryjeyoafpobhnbipneihhdukvepdlyeyii
klpljdkhhtluylcwtyeiefzxpluhvrpognindvegaytzkretoollklvqiezte
zvnvruijzmrthlsfkwlqleiyvufgcywotofkxhzlhznsgniydsytaiug
zpxqfzvl dbrplckffrievtkeswfrzrtgufcpskrbpfisopafpobaekxspxi
sasukatwdgzvlybaxspeoeefistsedzenislykxjzmkeod