

CIS 3362 Homework #3: Playfair, ADFGVX, Hill, Enigma
Due: Check WebCourses for the due date.

- 1) (10 pts) By hand, encrypt the plaintext “THISHOMEWORKSALITTLELATE” with the keyword “SPACEROCKS” and the padding character “Q”.
- 2) (15 pts) For the Hill cipher, for a language with an **alphabet size of 47**, the encryption key is $\begin{pmatrix} 13 & 27 \\ 31 & 38 \end{pmatrix}$, what is the corresponding decryption key?
- 3) (15 pts) You’ve intercepted a message encrypted by the Hill cipher using a 2 x 2 key (alphabet size 26). You also know that the plaintext “CL” maps to the ciphertext “ZD” and that the plaintext “IP” maps to the ciphertext “PH”. What are the possible encryption keys? (Note: I didn’t show you how to solve this in class, but it represents a type of problem I’ve put on a quiz. You can solve it via setting up an unknown key, writing down the matrix equations that ensue, followed by solving 2 systems of 2 equations under mod 26.)
- 4) (30 pts) The following ciphertext was encrypted using the Playfair cipher. For the first few days, I won’t give any matching plaintext. But, after a few days I’ll reveal some characters or the plaintext, and then I’ll reveal some more characters again before the due date. Determine the secret key and decrypt the whole ciphertext.

rnoprbdhgomkuohrhnzohdqbfundczdkqsdxi pmurknfc dqmeszkdc a f t i e
qdziksnfkfghkthqopfadcgsabdsfbfrnupahuocnrdgtcrnfc droqnufvuz
ghupdpf uerrbdypaloghupoecxdsrnmxcaftauidqddsmeszr df dhqowf cku
ruerhfyrdscxmpkpkpqgqmnvdczdroxreqdeydtwszzifyehxbudrdbvuddh
zdhfudbpdadkersaabzitqrnxrrchqowcr

- 5) (30 pts) The following ciphertext was generated using the code found at this link:

<http://www.cs.ucf.edu/~dmarino/ucf/cis3362/progs/hill.java>

HJLMYYBFIFIKQSQEAKWMSRYRKZPESYBGSCVDBHFBFLDRYKCPBFQIAXTXDKK
EERJTLYPKOTSBDAMXGBHFACMSVXXNQIVHHTECOJAADHMGZHTQWWQOWUPXME
CNJESHUUTNGUBDAOFVWQDUQHKOWJSAYFBOIVJBVOBGACFMKNMSERKYGYGRYE
RQAWQOBHFPFWOGAIIVCQQOXYFICVDBHFGMYKFIIIVCQOFVMFZYYYKBUMRT
WHXUOOBEBQRYWUOLVFJTQTONUWZDPDBHFXDUGKNWMRNGUBHFOKOCKHSHKSWT
VLZECBFPZLCKHSJCJJASB

The encryption key is a 3 x 3 matrix and the hint that will be given (to make decrypting easier) is as follows:

All of the numbers in the 3 by 3 decryption key are taken from the following set: {0, 4, 5, 6, 8, 11, 16, 21, 22, 25}.