Question 6)

This question is to implement and use a known plaintext attack on the Hill cipher. You may use functions from examples or previous questions, but do not use the built in Sage functions for the Hill Cipher. [Hint: The built in functions for MatrixSpace and FreeModule objects may be useful, but if they are too confusing to use, do not get caught up on them.]

1. Implement a known plaintext attack on the hill cipher.
2. Use the function that you wrote in part (a) to attack the following plaintext/ciphertext pairs:

* plaintext = "friday" ciphertext = "izrvey"
* plaintext = "diamondisinstatue" ciphertext = "zisxlhdiwdingthyqq"
* plaintext = "thesecretdietistofuhotdogs" ciphertext = "qbayzelwilksscipqpsvkafvssyy"

Solution to Question 6)

This question is to implement and use a known plaintext attack on the Hill cipher. You may use functions from examples or previous questions, but do not use the built in Sage functions for the Hill Cipher. [Hint: The built in functions for MatrixSpace and FreeModule objects may be useful, but if they are too confusing to use, do not get caught up on them.]

1. Implement a known plaintext attack on the hill cipher.

def hill\_known\_plaintext\_attack(plaintext, ciphertext, m):

numblocks = len(plaintext)/m

# initialize the plaintext blocks

plaintext\_blocks = [string\_to\_hill\_block(plaintext[j\*m:(j+1)\*m], m) for j in xrange(numblocks)]

# initialize the ciphertext blocks

ciphertext\_blocks = [string\_to\_hill\_block(ciphertext[j\*m:(j+1)\*m], m) for j in xrange(numblocks)]

MS = MatrixSpace(IntegerModRing(26), m)

Mpt = MS(0)

Mct = MS(0)

found\_invertible\_matrices = False

# iterate over the the combinations of the plaintext/ciphertext blocks

for combin in combinations\_iterator(range(numblocks), m):

Mpt\_list = [plaintext\_blocks[x] for x in combin]

Mct\_list = [ciphertext\_blocks[x] for x in combin]

Mpt = MS(Mpt\_list).transpose()

Mct = MS(Mct\_list).transpose()

if (Mpt.is\_invertible() and Mct.is\_invertible()):

found\_invertible\_matrices = True

break

if not found\_invertible\_matrices:

return MS(0)

K = Mct\*Mpt.inverse()

return K

1. Use the function that you wrote in part (a) to attack the following plaintext/ciphertext pairs:

* plaintext = "friday" ciphertext = "izrvey"
* plaintext = "diamondisinstatue" ciphertext = "zisxlhdiwdingthyqq"
* plaintext = "thesecretdietistofuhotdogs" ciphertext = "qbayzelwilksscipqpsvkafvssyy"

sage: pt = "friday"

sage: ct = "izrvey"

sage: Kfound = hill\_known\_plaintext\_attack(pt, ct, 2)

sage: Kfound

[11 11]

[12 1]

sage: pt = "diamondisinstatue"

sage: ct = "zisxlhdiwdingthyqq"

sage: Kfound = hill\_known\_plaintext\_attack(pt, ct, 3)

sage: Kfound

[21 5 19]

[14 12 13]

[ 6 13 19]

sage: pt = "thesecretdietistofuhotdogs"

sage: ct = "qbayzelwilksscipqpsvkafvssyy"

sage: Kfound = hill\_known\_plaintext\_attack(pt, ct, 4)

sage: Kfound

[ 5 21 1 19]

[19 12 12 3]

[10 24 5 18]

[13 23 16 4]