MATH/CSCI 408 Name: ______________________________

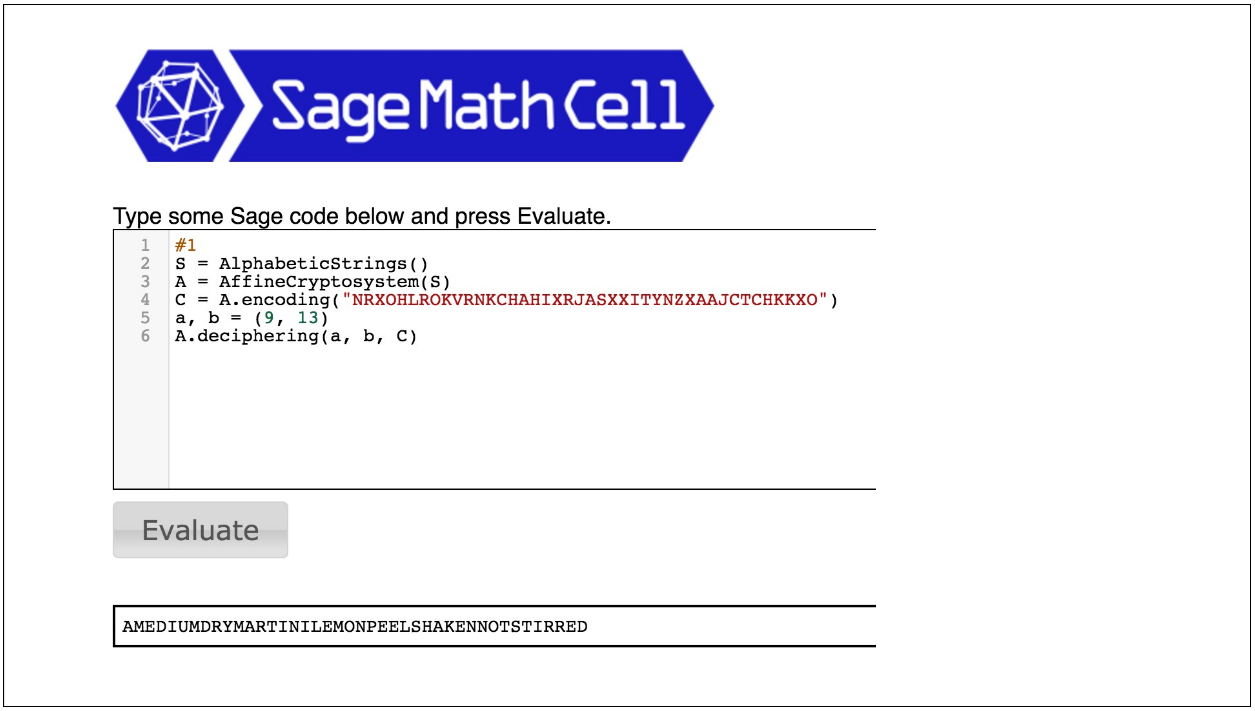
CRYPTOGRAPHY PRIORITY MISSION 01 SOLUTIONS

Deadline: Thursday, 29 September 2016 at 11:59pm

1. Problems

1. (Affine cipher) The following ciphertext used the affine cipher $x \mapsto 9x + 13$: `NRXOHLROKVRNKCHAHIXRJASXXITYNZXAAJCTCHKKXO`. Decrypt it.

   `A medium dry martini, lemon peel. Shaken, not stirred.` (James Bond's drink.)



Type some Sage code below and press Evaluate.

```
#1
S = AlphabeticStrings()
A = AffineCryptosystem(S)
C = A.encoding("NRXOHLROKVRNKCHAHIXRJASXXITYNZXAAJCTCHKKXO")
a, b = (9, 13)
A.deciphering(a, b, C)
```

```
AMEDIUMDRYMARTINILEMONPEELSHAKENNOTSTIRRED
```

2. (Affine cipher) Suppose you encrypt using an affine cipher, then encrypt the encryption using another affine cipher (both are working mod26). Is there any advantage to doing this? Why or why not? Explain in a paragraph, and give a specific, detailed example.

   There is no advantage to using two affine ciphers since two affine ciphers composed together just yield another affine cipher. For example, $f_1(x) = x + 2$ and$f_2(x) = 2x + 3$. The two composed together give $(f_1 \circ f_2)(x) = (2x+3)+2 = 2x+5$, which is just another affine cipher. This means the same frequency analyses and methods can break it.

3. (Hill Cipher) Barry captures Archer's Hill cipher machine, which uses a 2×2 matrix M mod 26. He realizes that the plaintext `ba` encrypts to `HC`, and the plaintext `zz` encrypts to `GT`. What is the matrix M?

We have:

$$\begin{aligned} \mathtt{b} = 1 &\leftrightarrow \mathtt{H} = 7 \\ \mathtt{a} = 0 &\leftrightarrow \mathtt{C} = 2 \\ \mathtt{z} = 25 &\leftrightarrow \mathtt{G} = 6 \\ \mathtt{z} = 25 &\leftrightarrow \mathtt{T} = 19 \end{aligned}$$

The matrix setup is:

$$\begin{aligned} \begin{pmatrix} 1 & 0 \\ 25 & 25 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} &= \begin{pmatrix} 7 & 2 \\ 6 & 19 \end{pmatrix} \\ \begin{pmatrix} a & b \\ c & d \end{pmatrix} &= \begin{pmatrix} 1 & 0 \\ 25 & 25 \end{pmatrix}^{-1} \begin{pmatrix} 7 & 2 \\ 6 & 19 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 0 \\ 25 & 25 \end{pmatrix} \begin{pmatrix} 7 & 2 \\ 6 & 19 \end{pmatrix} \\ &= \begin{pmatrix} 7 & 2 \\ 13 & 5 \end{pmatrix} \end{aligned}$$

4. (Hill Cipher) Suppose you are given the following ciphertext:
`ESIZEHAXPDILHJDTBQEHSJZXXHQFIBKZJYWUQWEDKDEUDMHJTWPVQLEHHMMFKBMUZXEUZTESIZYL`
Given the encryption matrix:

$$\begin{pmatrix} 1 & 5 \\ 2 & 3 \end{pmatrix}$$

Decrypt the message.

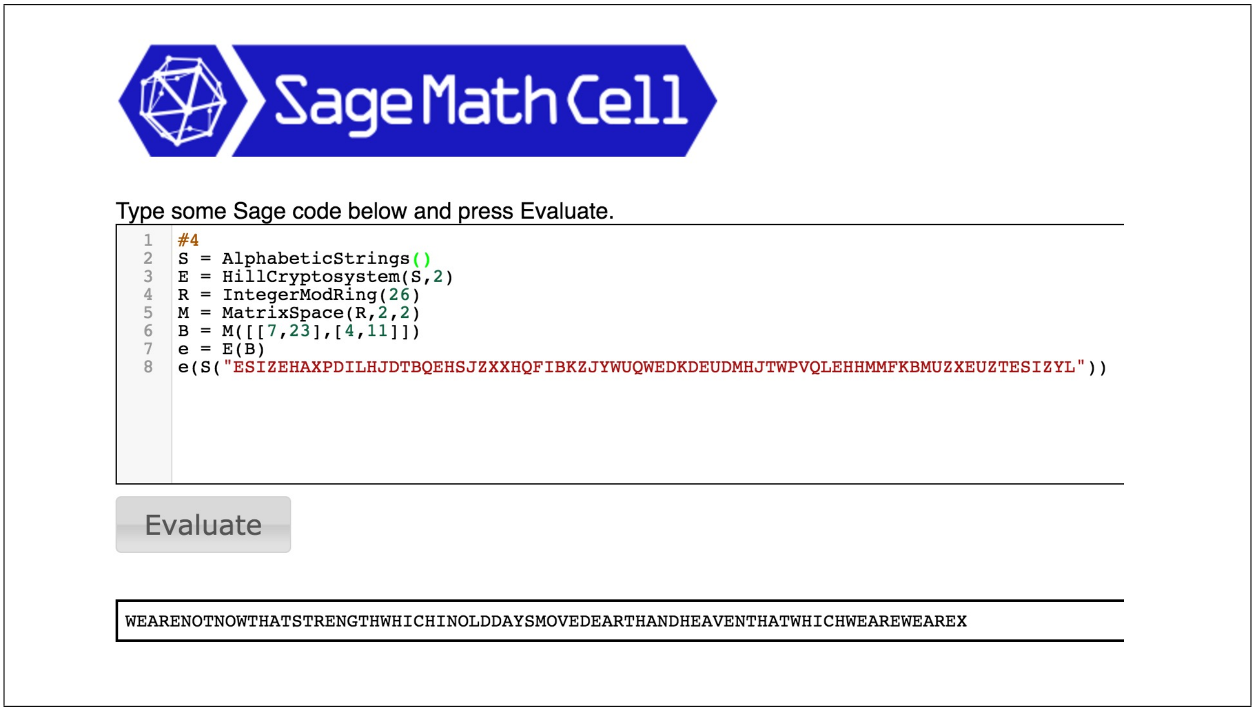
The inverse of the matrix is

$$\begin{pmatrix} 7 & 23 \\ 4 & 11 \end{pmatrix}$$

We can use SageMath to decrypt:

```
We are not now that strength which in old days
Moved earth and heaven; that which we are, we are.
```

(M quoting Tennyson in *Skyfall.*)



Type some Sage code below and press Evaluate.

```
#4
S = AlphabeticStrings()
E = HillCryptosystem(S,2)
R = IntegerModRing(26)
M = MatrixSpace(R,2,2)
B = M([[7,23],[4,11]])
e = E(B)
e(S("ESIZEHAXPDILHJDTBQEHSJZXXHQFIBKZJYWUQWEDKDEUDMHJTWPVQLEHHMMFKBMUZXEUZTESIZYL"))
```

```
WEARENOTNOWTHATSTRENGTHWHICHINOLDDAYSMOVEDEARTHANDHEAVENTHATWHICHWEAREWEAREX
```

5. (Proof) Write a proof for the following statements:

a. Let a, b, n be integers. If $\gcd(a, n) = 1$ and $\gcd(b, n) = 1$, then $\gcd(ab, n) = 1$.

Proof. Suppose a, b and n are integers. Assume $\gcd(a, n) = 1$ and $\gcd(b, n) = 1$. Then by the theorem in class, we know that there exist integers x, y, z, w in which

$$ax + ny = 1$$
$$bz + nw = 1$$

Consider

$$(ax + ny)(bz + nw) = 1$$
$$abxz + anxw + bnyz + n^2yz = 1$$
$$ab(xz) + n(axs + byz + nyw) = 1$$

Using the same theorem, this means that $\gcd(ab, n) = 1$. □

b. Let a, b, c, and n be integers with $n > 0$. If $a \equiv b \mod n$ and $b \equiv c \mod n$, then $a \equiv c \mod n$.

Proof. Suppose a, b, c, n are integers with $n > 0$. Assume $a \equiv b \mod n$ and $b \equiv c \mod n$. This means $n \mid (a - b)$ and $n \mid (b - c)$. In other words, $a - b = nk$ for some integer k and $b - c = nl$ for some integers l. Consider

$$(a - b) + (b - c) = nk + nl$$
$$a - c = n(k + l)$$

So $n \mid (a - c)$ or $a \equiv c \mod n$. □

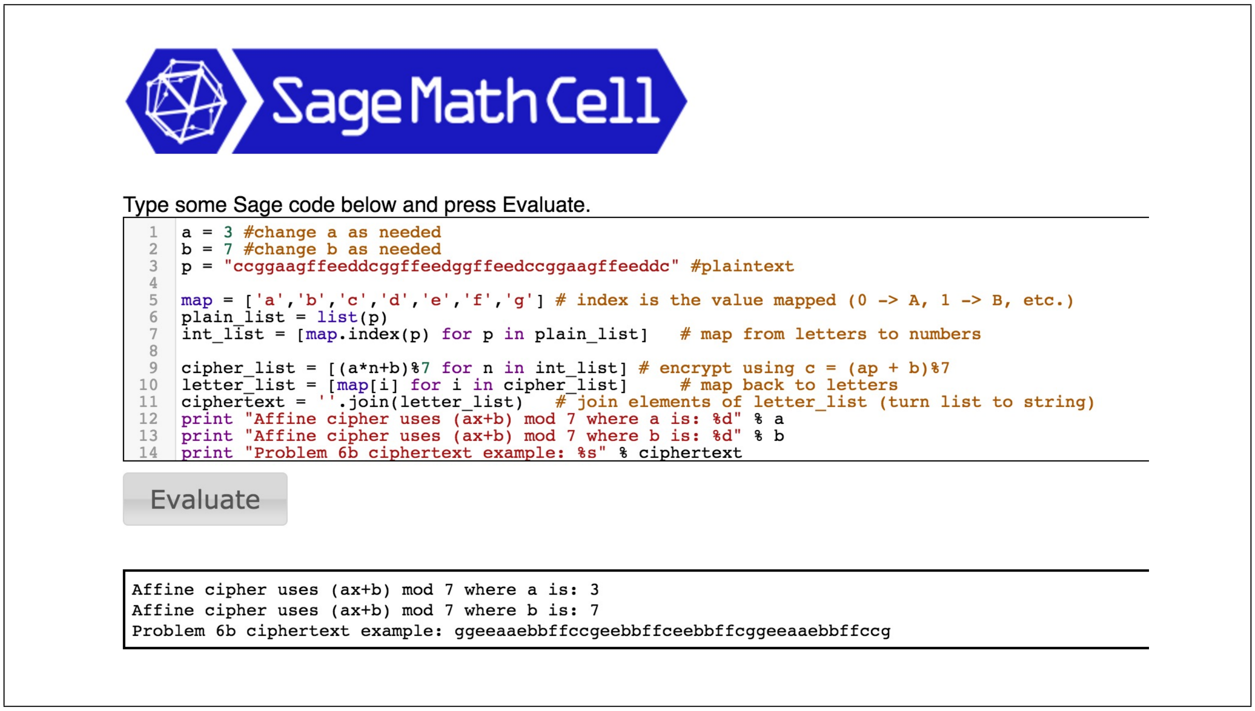
6. (SageMath) We are using a new alphabet $\{A, B, C, D, E, F, G\}$ (perhaps corresponding to musical notes). Associate the letters with the numbers $\{0, 1, 2, 3, 4, 5, 6\}$, respectively.

   a. Using the shift cipher with a shift of 5, encrypt the following sequence of notes for Twinkle Twinkle Little Star: `ccggaagffeeddcggffeedggffeedccggaagffeeddc`.

      A shift by 5 yields: `aaeeffeddccbbaddccbbaddccbbaaaeeffeddccbba` .

   b. Write a program that performs affine ciphers on the musical alphabet. Provide the code as well as an example of output.

      See an example below or run the file:
      `Exam01_Problem06b.sagews`



Type some Sage code below and press Evaluate.

```
a = 3 #change a as needed
b = 7 #change b as needed
p = "ccggaagffeeddcggffeedggffeedccggaagffeeddc" #plaintext

map = ['a','b','c','d','e','f','g'] # index is the value mapped (0 -> A, 1 -> B, etc.)
plain_list = list(p)
int_list = [map.index(p) for p in plain_list]   # map from letters to numbers

cipher_list = [(a*n+b)%7 for n in int_list] # encrypt using c = (ap + b)%7
letter_list = [map[i] for i in cipher_list]     # map back to letters
ciphertext = ''.join(letter_list)   # join elements of letter_list (turn list to string)
print "Affine cipher uses (ax+b) mod 7 where a is: %d" % a
print "Affine cipher uses (ax+b) mod 7 where b is: %d" % b
print "Problem 6b ciphertext example: %s" % ciphertext
```

```
Affine cipher uses (ax+b) mod 7 where a is: 3
Affine cipher uses (ax+b) mod 7 where b is: 7
Problem 6b ciphertext example: ggeeaaaebbffccgeebbffceebbffcggeeaaaebbffccg
```