MATH 222

Assignment 3

- Generalized Caesar's Code
- Linear Code
- Key Phrase Cipher
- Hill Cipher
- Autokey Cipher
- Vernam Cipher
- The RSA Cryptosystem
- Closed Forms
- Recurrence Relations

Group information (you may work by yourself, in a pair, or as a trio)

First Name	Last Name	ID
Grfwru	Hffr	3

1. Decipher the following three messages. (Hint: part a) was encoded using the generalized Caesar's code.)

   a) Xli wigsrh qiwweki aew irgvctxih ywmrk xli pmriev gshi amxl e xlvii erh o wmb.

   The plaintext is:

   The second message was encrypted using the linear code with a three and k six.

   b) Yw lw lbs vwoflb vnwwf wv MGJ, wt lbs jonnslet-jwgfp tsgfsil lbs snsrglwf ei g ismfsl uwfp. Ois el lw psmezbsf lbs lbefp qsiigys.

   The plaintext is:

   Go to the fourth floor of CAB, on the bulletin-board nearest the elevator is a secret word. Use it to decipher the third message.

   c) Jzwck nhf! Bwm jrzx idzfgu jnpo ustbw.

   The plaintext is:

   Great Job! You have earned full marks.

6

2. The Mayor of Edmonton wants Dr. Ecco to help him with plans for a downtown arena. Dr. Ecco isn't interested so the Mayor sends his goons to bring him in. Dr. Ecco sends out a decoy cipher text to mislead the goons. The cipher text is as follows:

O oy pwknmxg m pyrfc ob ZQNP

Except for the last word, the mayor has found the plain text:

I am hosting a party in

a) Dr. Ecco's decoy cipher text was encoded using the Hill cipher with the encoding function:

$$E(x) \equiv 5 \cdot x + 6 \cdot y \pmod{26}$$
$$E(y) \equiv 18 \cdot x + y \pmod{26}$$

Complete the decoy message by finding the decoding function and decode the last word of the cipher text. If the mayor's goons follow Dr. Ecco's decoy message where will they end up going?

Start by finding the decoding function:

$$\begin{bmatrix} 5 & 6 \\ 18 & 1 \end{bmatrix}^{-1} \equiv (5 \cdot 1 - 6 \cdot 18)^{-1} \begin{bmatrix} 1 & -6 \\ -18 & 5 \end{bmatrix} \equiv \begin{bmatrix} 1 & -6 \\ 8 & 5 \end{bmatrix} \pmod{26}$$

Therefore,

$$D(x) \equiv x - 6 \cdot y \pmod{26}$$
$$D(y) \equiv 8 \cdot x + 5 \cdot y \pmod{26}$$

$$D(Z) \equiv (-1) - 6 \cdot (-10) \equiv 7 \pmod{26}$$
$$D(Q) \equiv 8 \cdot (-1) + 5 \cdot (-10) \equiv 20 \pmod{26}$$

$$D(N) \equiv (13) - 6 \cdot (15) \equiv 1 \pmod{26}$$
$$D(P) \equiv 8 \cdot (13) + 5 \cdot (15) \equiv -3 \pmod{26}$$

If the decoy works the mayor's goons will go to ___ HUB___.

b) Dr. Ecco has double-encoded the last word in his message. To get the real message, you must suppose that the plain text word found in part a) is also cipher text. What is the real message?

$$D(H) \equiv \quad (7) - 6 \cdot (20) \quad \equiv 17 \pmod{26}$$
$$D(U) \equiv 8 \cdot (7) + 5 \cdot (20) \quad \equiv 0 \pmod{26}$$

$$D(B) \equiv \quad (1) - 6 \cdot (-3) \quad \equiv 19 \pmod{26}$$
$$D(X) \equiv 8 \cdot (1) + 5 \cdot (-3) \quad \equiv 19 \pmod{26}$$

The real meeting place is __RATT__ .

$\overline{2}$

4

3. Decipher the following message which was encrypted using the autokey cipher with seed I.

J S R V J

$D(J) \equiv 9 - 8 \equiv 1$

$D(S) \equiv 18 - 1 \equiv 17$

$D(R) \equiv 17 - 17 \equiv 0$

$D(V) \equiv 21 - 0 \equiv 21$

$D(J) \equiv 9 - 21 \equiv 14$

Bravo

5

4. Using the keystream:

	11111 00000 11111 00000 11111 00000 11111
decode	11000 00000 10100 00101 01001 00000 00111
	00111 00000 01011 00101 10110 00000 11000

Convert to decimal:

$$2^2 + 2^1 + 2^0 = 7$$

$$0 = 0$$

$$2^3 + 2^1 + 2^0 = 11$$

$$2^2 + 2^0 = 5$$

$$2^4 + 2^2 + 2^1 = 22$$

$$0 = 0$$

$$2^4 + 2^3 = 24$$

HALFWAY

$\overline{2}$

5. You have set up a public key cryptosystem; your public encoding function is:

$$E(x) \equiv x^5 \pmod{26}$$

Dr. Ecco, using this encoding function, has sent you the following ciphertext:

PQKKP

Two prime numbers are kept private for your public key cryptosystem they are:

$$p = 2, q = 13$$

$n = (p-1)(q-1) = 1 \cdot 12 = 12$

$1 \equiv 13 \equiv 25 \equiv 5 \cdot 5 \pmod{12}$

$\therefore\ D(x) \equiv x^5 \pmod{26}$

$D(P) \equiv 15^5 \equiv 19$

$D(Q) \equiv 16^5 \equiv 22$

$D(K) \equiv 10^5 \equiv 4$

$D(K) \equiv 4$

$D(P) \equiv 19 \pmod{26}$

The decoding function is:	The plain text is:
$D(x) \equiv x^5 \pmod{26}$	TWEET

On a typical day more than 500 million tweets are sent

– August 16, 2013 @raffi

6. In the our lecture notes a closed form for S_2 was found using the closed form for S_1. Use a similar strategy to find a closed for S_3 using the closed form for S_1 and S_2. In other words find a closed form for

$$S_3 = 1^3 + 2^3 + 3^3 + \cdots + n^3$$

using the expansion:

$$(x+1)^4 = x^4 + 4x^3 + 6x^2 + 4x + 1$$

by plugging in $x = 1, x = 2, x = 3, \ldots, x = n$. Simplify your answer as much as possible your fully simplified form should show that S_3 is a perfect square. Note: a *perfect square* is an integer that is the square of an integer, for example 4, 9, 625 are perfect squares since they equal $2^2, 3^2, 25^2$.

Plug in $x = 1,\ x = 2,\ x = 3,\ \ldots,\ x = n$ to the given polynomial:

$$\begin{array}{rl} 2^4 &= 1^4 + 4\cdot 1^3 + 6\cdot 1^2 + 4\cdot 1 + 1 \\ 3^4 &= 2^4 + 4\cdot 2^3 + 6\cdot 2^2 + 4\cdot 2 + 1 \\ 4^4 &= 3^4 + 4\cdot 3^3 + 6\cdot 3^2 + 4\cdot 3 + 1 \\ &\vdots \\ + \quad (n+1)^4 &= n^4 + 4\cdot n^3 + 6\cdot n^2 + 4\cdot n + 1 \\ \hline S_4 - 1 + (n+1)^4 &= S_4 + 4\cdot S_3 + 6\cdot S_2 + 4\cdot S_1 + n. \end{array}$$

$$\Rightarrow \quad -1 + (n+1)^4 = 4\cdot S_3 + 6\cdot\frac{(2n+1)(n+1)n}{6} + 4\cdot\frac{(n+1)n}{2} + n$$

$$\Rightarrow \quad 4\cdot S_3 = -1 + (n+1)^4 - (2n+1)(n+1)n - 2(n+1)n - n$$

$$\Rightarrow \quad 4\cdot S_3 = (n+1)^4 - (2n+1)(n+1)n - 2(n+1)n - (n+1)$$

$$\Rightarrow \quad 4\cdot S_3 = (n+1)\cdot\left((n+1)^3 - (2n+1)n - 2n - 1 \right)$$

$$\Rightarrow \quad 4\cdot S_3 = (n+1)\cdot\left(n^3 + 3\cdot n^2 + 3\cdot n + 1 - 2n^2 - n - 2n - 1 \right)$$

$$\Rightarrow \quad 4\cdot S_3 = (n+1)\cdot(n^3 + n^2)$$

$$\Rightarrow \quad S_3 = \left(\frac{(n+1)n}{2}\right)^2$$

The closed from that represents a perfect square is: $S_3 = \left(\frac{(n+1)n}{2}\right)^2 = S_1^2$

$\overline{2}$

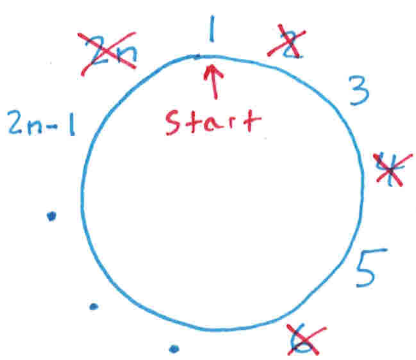
Bonus Problem

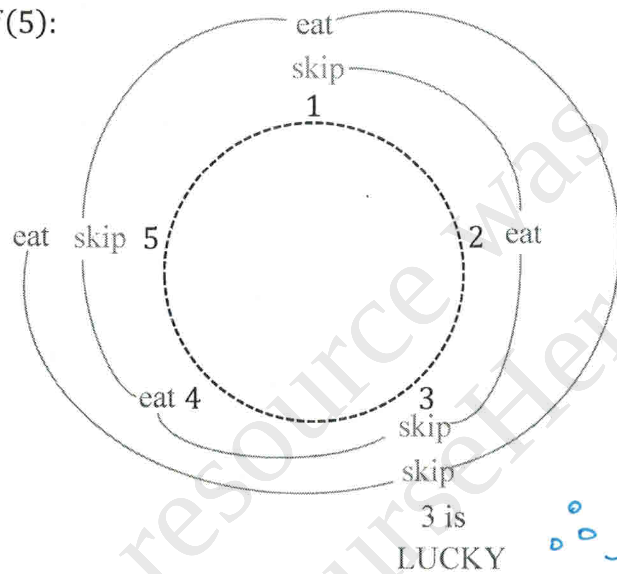
Sylvester caught n mice which he arranged in a circle and numbered them $1, 2, \ldots, n$ in clockwise order. Starting with mouse number 1, Sylvester went around the circle in clockwise order, skipping over one mouse and eating the next one. He went round and round by the same rule, until only one mouse was left. This lucky mouse was then set free. Denote $f(n)$ as the number assigned to the lucky mouse initially. Now

$$f(1) = 1,\ f(2) = 1, f(3) = 3, f(4) = 1, \text{ and } f(5) = 3.$$

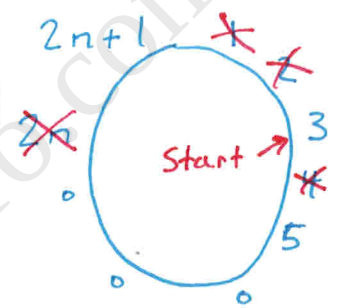
For example to find $f(5)$:

With 2n mice





With 2n+1 mice



$\therefore f(2n) = 2f(n) - 1$

$\therefore f(2n+1) = 2f(n) + 1$

Find out which mouse is lucky when there are 222 mice. That is find $f(222)$.

$$\begin{aligned} f(222) &= f(2 \cdot 111) \\ &= 2f(111) - 1 \\ &= 2(f(2 \cdot 55 + 1)) - 1 \\ &= 4f(55) + 2 - 1 \\ &= 4f(2 \cdot 27 + 1) + 1 \\ &= 8f(27) + 5 \\ &= 8(f(2 \cdot 13 + 1)) + 5 \\ &= (8 \cdot 2)f(13) + 13 \\ &= 16(f(2 \cdot 6 + 1)) + 13 \\ &= 16(2)f(6) + 29 \\ &= 32f(2 \cdot 3) + 29 \\ &= 32(2f(3) - 1) + 29 \\ &= 64 \cdot f(3) - 32 + 29 \\ &= 64 \cdot 3 - 3 \\ &= 189 \end{aligned}$$

$\boxed{f(222) = 189}$

$\overline{2}$