CS 642 Homework 1 Solution

Asim Kadav

February 15, 2008

Problem 1

Hill's Cipher

Given: Bob's Hill Cipher machine uses a 2x2 matrix M mod 26. Also,

Enc("ba")="HC" Enc("zz")="GI" Combining, these two equations we can get the X and Y matrices representing the plain and cipher text information.

$$X = \begin{pmatrix} b & z \\ a & z \end{pmatrix}$$

$$Y = \begin{pmatrix} H & G \\ C & T \end{pmatrix}$$

Y=M*X
Thus,
M = Y*X^{-1}
Converting to numbers,

$$X = \begin{pmatrix} 1 & 25 \\ 0 & 25 \end{pmatrix}$$

$$Y = \begin{pmatrix} 7 & 6 \\ 2 & 8 \end{pmatrix}$$

X^{-1} in modulo 26 is :

$$InverseofXis = \begin{pmatrix} 1 & 25 \\ 0 & 25 \end{pmatrix}$$

Thus,

$$M = \begin{pmatrix} 1 & 25 \\ 0 & 25 \end{pmatrix} \begin{pmatrix} 7 & 6 \\ 2 & 8 \end{pmatrix} mod 26$$

$$M = \begin{pmatrix} 7 & 13 \\ 2 & 5 \end{pmatrix}$$

Problem 2

Given the cipher text, 8 occurs maximum number of times (34 times) so 8 is e. ; is second most frequent. Thus, examining the whole cipher text its easy to infer that ';48' is the. Intuitively, the sentence begins with 'a'. Similarly, by intuition and using the frequency count in Pg 39 of Stallings, the result comes as:

A good glass in the bishop's hostel in the devil's seat twenty-one degrees and thirteen minutes northeast and by north main branch seventh limb east side shoot from the left eye of the death's-head a bee line from the tree through the shot fifty feet out

Problem 3

We are using a combination of Hill and affine ciphers. The cipher text (u,v) is :

$$\begin{pmatrix} x & y \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} + \begin{pmatrix} e & f \end{pmatrix} = (u, v) mod 26$$

This for any particular ciphertext (u,v). Suppose, we have four such pairs (u',v') and (u", v"). We can get equations for these as above and subtract to get:

$$\begin{pmatrix} u'' & v'' \\ u' & v' \end{pmatrix} - \begin{pmatrix} u''' & v''' \\ u'''' & v'''' \end{pmatrix}$$

=

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \left(\begin{pmatrix} x' & y' \\ x'' & y'' \end{pmatrix} - \begin{pmatrix} x''' & y''' \\ x'''' & y'''' \end{pmatrix} \right)$$

Thus, if we have the plain text, cipher text combinations as above we can solve the equation. As there four variables a,b,c,d in our reduced equation we can solved it with four such plain-cipher combinations. We can now further use this to find e,f.

Problem 4

Part A: For function f to be linear it means that for each output bit of the function, each input var always makes a difference or it never makes a difference.
Part B: For e.g. A AND B is a linear function.

A OR B is a linear function.

A XOR BC is non-linear function.

Problem 5

Part A: To generate key stream of length 8. The feedback bit at stage 3 is always : S3 XOR (S1XOR S0). Where Sn, represents the output at stage n. The output is always from stage 0. So, the sequence of bits becomes :
1. 0 1 1 0
2. 1 0 1 1 0
3. 1 1 0 1 1 0
4. 0 1 1 0 1 1 0
5. 1 0 1 1 0 1 1 0
6. 1 1 0 1 1 0 1 1 0
7. 0 1 1 0 1 1 0 1 1 0
8. 1 0 1 1 0 1 1 0 1 1 0

Part B: As is evident from the key stream generated, that we are generating 110 repeatedly. The relationship here is key = S3 XOR (S1XOR S0). Where Sn, represents the output at stage n. This function is a linear function. Thus, for very output bit of the function defines a parity over the input bits and it is hence a linear function. To make it non-linear, we need to add a combiner function. This is also evident from the truth table of our function.
P Q RO
0 0 0 0
0 0 1 1
0 1 0 1
0 1 1 0
1 0 0 1
1 0 1 1
1 1 0 0
1 1 1 1
P = S3, Q = S1, R = S0. O = S3 XOR (S1XOR S0).

Part C: LFSRs are predictable and they have a period after which they start repeating. This period is 2^L - 1. For L = 4, the maximal unique sequence length of the key is 15. After this, the key starts repeating.

Part D :
We have,
x(n+2) = c0.x(n) + c1.x(n+1)(mod 3)
Given sequence is 1, 1, 0, 2, 2, 0, 1, 1.
We get three equations as:
0 = C0 + C1 mod3
2 = C0 + C1.0 mod3
2 = C0.0 + C1.2 mod3

and so on..
Solving these we get,
C1 = 1 C0 = 2