MATH 314 Fall 2019 - Class Notes

9/11/2019

Scribe: Christine Adams

Summary: Today's class covered the Hill cipher

Hill Cipher
m-block size
k-$m \times m$ matrix $mod 26$
(k has to have an inverse)
E($\dot{\vec{v}}$)=$\dot{\vec{v}}$k
D($\dot{\vec{c}}$)=$\dot{\vec{c}}$k
Inverse of a 2×2 $(mod 26)$

if k=$\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}$ **(**$mod 26$**)**

Then k^{-1}**=(adbc)**$^{-1}$ $\begin{smallmatrix} d & -b \\ c & a \end{smallmatrix}$**(mod26)**

Determinant has to be a mod 26 value that is odd and not 13

Gcd (det(k), 26)=1, 1 being the greatest factor they have in common.
This is true for any hill cipher matrix k.
Find the inverse of

$$K = \begin{bmatrix} 4 & 1 \\ 3 & 10 \end{bmatrix}$$

det(k)=4×10 **-**1×3**=37=11 mod 26**

K^{-1} $= (11)^{-1} = \begin{smallmatrix} 10 & -1 \\ -3 & 4 \end{smallmatrix}$

$$19 \times \begin{bmatrix} 10 & 25 \\ 23 & 4 \end{bmatrix} mod 26$$

$$\equiv \begin{bmatrix} 19 \times 10 & 19 \times 25 \\ 19 \times 23 & 19 \times 4 \end{bmatrix} mod 26$$

$$=$$

$$\equiv \begin{bmatrix} 8 & 7 \\ 21 & 24 \end{bmatrix} \in \textbf{Inverse}$$

Chosen Plaintext attack
Suppose m=2

Pick the plaintext "ba"<**1,0**>
E(< **1,0**>**=**<**1,0**> $\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}$ = <a,b> or <1,0> (Find the first row of k)

Encrypt "a,b"- E(<0,1>)=<0,1> $\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}$
Known plaintext attack
Find the key using linear algebra
Alice sends the ciphertext LIPVPI to Bob
11,19,15,21,15,8
Eve learns this corresponds to "linear"
11,19,15,21,15,8
Block size m=2
<11,8> k =<11,19>
<13,4>k=<15,21>
<0,17>k=<15,8> $mod 26$
Matrix equation

$$\begin{bmatrix} 11 & 8 \\ 13 & 4 \end{bmatrix} k = \begin{bmatrix} 11 & 19 \\ 15 & 21 \end{bmatrix}$$

Invert the first matrix (find the inverse to get k by itself)

$$\begin{bmatrix} 11 & 8 \\ 13 & 4 \end{bmatrix}^{-1} = (44 - 104)^{-1} \begin{bmatrix} 4 & -8 \\ -13 & 11 \end{bmatrix}$$

(Even so not invertible)

Try again!
1st and 3rd equation

$$\begin{bmatrix} 11 & 8 \\ 0 & 17 \end{bmatrix} k \equiv \begin{bmatrix} 11 & 18 \\ 15 & 8 \end{bmatrix}$$

Invert this

$$\begin{bmatrix} 11 & 8 \\ 0 & 17 \end{bmatrix}^{-1} \equiv (11 * 17 - 8(0))^{-1} \begin{bmatrix} 17 & -8 \\ 0 & 11 \end{bmatrix} \equiv 5^{-1} \begin{bmatrix} 17 & -8 \\ 0 & 11 \end{bmatrix}$$

$$\equiv 21 \times \begin{bmatrix} 17 & 18 \\ 0 & 11 \end{bmatrix} \equiv \begin{bmatrix} 19 & 14 \\ 0 & 23 \end{bmatrix}$$

Multiply both sides of equations on left!

$$\begin{bmatrix} 19 & 14 \\ 0 & 23 \end{bmatrix} \begin{bmatrix} 11 & 8 \\ 0 & 17 \end{bmatrix} k \equiv \begin{bmatrix} 19 & 14 \\ 0 & 23 \end{bmatrix} \begin{bmatrix} 11 & 19 \\ 15 & 8 \end{bmatrix}$$

Identity

$$K \equiv \begin{bmatrix} 19 & 14 \\ 0 & 17 \end{bmatrix} \begin{bmatrix} 11 & 19 \\ 15 & 8 \end{bmatrix}$$

$$\equiv \begin{bmatrix} 19(11)+14(15) & 19(19)+14(8) \\ 23(15) & 23(8) \end{bmatrix}$$

$$\equiv \begin{bmatrix} 1+2 & 23+8 \\ 7 & 2 \end{bmatrix}$$

$$\equiv \begin{bmatrix} 3 & 5 \\ 7 & 2 \end{bmatrix} = k$$

Key matrix has to be invertible