MATH 314 Fall 2019 - Class Notes

9/11/2019

Scribe: Jace Graham

Summary: Class on 9/11/2019 was working on the Hill Cipher

Notes:

Hill Cipher

m - block size
k - key matrix (m x m) *has to have an inverse
E($\vec{v}$) = $\vec{v}K \pmod{26}$

Inverse of 2 x 2 matrix

if $k \equiv \begin{bmatrix} a & b \\ c & d \end{bmatrix} \pmod{26}$

$k^{-1} \equiv (ad - bc)^{-1} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix} \pmod{26}$

(the determinant, ad-bc, has to be invertible (mod 26))
In general k is valid Hill Cipher matrix if gcd(det(k), 26) = 1

example:

$k \equiv \begin{bmatrix} 4 & 7 \\ 1 & 10 \end{bmatrix}$ Find decryption matrix

$$k^{-1} \equiv (ad - bc)^{-1} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix} \pmod{26}$$

$$(ad - bc)^{-1} = (4 * 10 - 7 * 1) = 7^{-1} \equiv 15 \pmod{26}$$

$$k^{-1} \equiv (15) \begin{bmatrix} 10 & -7 \\ -1 & 4 \end{bmatrix} \pmod{26}$$

$$\begin{bmatrix} 150 & -105 \\ -15 & 60 \end{bmatrix} \pmod{26} \equiv \begin{bmatrix} 20 & 25 \\ 11 & 8 \end{bmatrix} \equiv k^{-1}$$

Chosen plain text attack

2 x 2 matrix

$$k = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

choose "ab" for ¡0,1¿

$E(<0,1>) = <0,1> \begin{bmatrix} a & b \\ c & d \end{bmatrix} = <c,d>$

"ba" goes to ¡1,0¿

$E(<1,0>) = <1,0> \begin{bmatrix} a & b \\ c & d \end{bmatrix} = <a,b>$

Known plain text attack

Find k using linear algebra

suppose Eve captures cipher text

L	T	P	V	P	I
11	19	15	21	15	8

she learns the plain text is

L	I	N	E	A	R
11	8	13	4	0	17

and block size is 2...

break into three sets of 2, match plain text and cipher, and "smush" together

$<11,8> k \equiv <11,19> \pmod{26}$

$<13,4> k \equiv <15,21> \pmod{26}$

$<0,17> k \equiv <15,8> \pmod{26}$

use first 2 to make following

$$\begin{bmatrix} 11 & 8 \\ 13 & 4 \end{bmatrix} k \equiv \begin{bmatrix} 11 & 19 \\ 15 & 21 \end{bmatrix} \pmod{26}$$

multiply both sides by inverse of left side

for rows 1 and 2, determinant is (44-104) which is an even number so there is no inverse mod 26. Have to use rows 1 and 3.

$$\begin{bmatrix} 11 & 8 \\ 0 & 17 \end{bmatrix} k \equiv \begin{bmatrix} 11 & 19 \\ 0 & 23 \end{bmatrix} \pmod{26}$$

$$\begin{bmatrix} 11 & 8 \\ 0 & 17 \end{bmatrix}^{-1} \equiv (11 * 17)^{-1} \begin{bmatrix} 17 & 18 \\ 0 & 11 \end{bmatrix}$$

mod 26 multiplication chart shows 11*17 mod 26 is 5 and inverse of 5 is 21

$$21 \begin{bmatrix} 17 & 18 \\ 0 & 11 \end{bmatrix} \equiv \begin{bmatrix} 19 & 14 \\ 0 & 23 \end{bmatrix} \pmod{26}$$

make sure to multiple on left side for both sides

$$\begin{bmatrix} 19 & 14 \\ 0 & 23 \end{bmatrix} \begin{bmatrix} 11 & 8 \\ 0 & 17 \end{bmatrix} k \equiv \begin{bmatrix} 19 & 14 \\ 0 & 23 \end{bmatrix} \begin{bmatrix} 11 & 19 \\ 0 & 23 \end{bmatrix} \pmod{26}$$

first two matrices make identity matrix so they equal 1.

$$k \equiv \begin{bmatrix} 19 & 14 \\ 0 & 23 \end{bmatrix} \begin{bmatrix} 11 & 19 \\ 0 & 23 \end{bmatrix} \equiv \begin{bmatrix} 3 & 5 \\ 7 & 2 \end{bmatrix} \pmod{26}$$