MATH 314 Spring 2018 - Class Notes

02/07/2018

Scribe: Farbod Farhang

Summary: Introduction to the Hill cypher which is a block cipher

Notes

Block cipher - encrypt multiple letters called blocks of ciphertext

Changing any letter in block of the plaintext should change the entire block of the cipher

Hill Cypher (1929)

Use linear algebra
- Break the text into blocks of length m
- Key: $m \times m$ Matrix of numbers $\pmod{26}$

To encrypt
1. take a block of letters and write it as a vector of numbers $\vec{v}$
2. then multiply by the Matrix of numbers (mxm)
3. finally reduce $\pmod{26}$

$E(\vec{v}) \equiv \vec{v}(K) \pmod{26}$

ex. Encrypt "June"
$m = 2, \quad K = \left(\begin{smallmatrix} 11 & 8 \\ 3 & 7 \end{smallmatrix}\right)$

"JUNE" $= <9 \;\; 20> \, <13 \;\; 4>$

Encrypt "JU":

$$\begin{aligned} <9 \;\; 20> \left(\begin{smallmatrix} 11 & 8 \\ 3 & 7 \end{smallmatrix}\right) &= <(9(11) + 20(3)) \;\; (9(8) + 20(7))> \\ &= <(99 + 60) \;\; (72 + 140)> \\ &= <159 \;\; 212> \pmod{26} \\ &= <3 \;\; 4> \\ &= \text{"DE"} \end{aligned}$$

Encrypt "NE":

$< 13 \;\; 4 > \left(\begin{smallmatrix} 11 & 8 \\ 3 & 7 \end{smallmatrix}\right) \quad = \; < (13(11) + 4(3)) \;\; (13(8) + 4(7)) >$

$= \; < 25 \;\; 2 >$

$=$ "ZC"

so, "JUNE" = "DEZC"

ex. Encrypt "Dune"

"DUNE" $= < 3 \;\; 20 > < 13 \;\; 4 >$

$E(< 3 \;\; 20 >) \; = \; < 3 \;\; 20 > \left(\begin{smallmatrix} 11 & 8 \\ 3 & 7 \end{smallmatrix}\right) \; = \; < 15 \;\; 8 > \; =$ "PI"

$E(< 13 \;\; 4 >) \; =$ "ZC"

so, "DUNE" = "PIZC"

Need to be able to Decrypt messages too. to so this you need to find the decryption function:

$E(\vec{v}) \equiv \vec{w} \pmod{26}$

Bob knows K and $\vec{w}$, he wants to get $\vec{v}$ (The plaintext)

To solve this, we need to find an inverse matrix of K called K^{-1}

$\vec{v}K \equiv \vec{w} \pmod{26}$

$(K)(K^{-1}) \; = \; I \; = \; \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$ or $\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$

Where I is the identity matrix

Inverse of $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ or K is $((a(d) - b(c))^{-1}) \left(\begin{smallmatrix} d & -b \\ -c & a \end{smallmatrix}\right)$ or K^{-1}

NOTE the key matrix for the Hill Cipher must have a determinant which does not have any factors in common with 26

ex. $K = \; \left(\begin{smallmatrix} 7 & 2 \\ 3 & 10 \end{smallmatrix}\right)$

determinant (det) $(K) = \; 70 - 6 \; = \; 64$

Since the determinant is even this matrix is not valid for the Hill Cypher

Decryption function: $D(\vec{w}) \ = \ (\vec{w})(K^{-1})$

If $K = \left(\begin{smallmatrix} 11 & 8 \\ 3 & 7 \end{smallmatrix}\right)$ then $K^{-1} \equiv (77-24)^{-1} \left(\begin{smallmatrix} 7 & -8 \\ -3 & 11 \end{smallmatrix}\right) \pmod{26})$

$$\equiv 53 \pmod{26} \left(\begin{smallmatrix} 7 & 18 \\ 23 & 11 \end{smallmatrix}\right)$$

$$\equiv (1^{-1}) \left(\begin{smallmatrix} 7 & 18 \\ 23 & 11 \end{smallmatrix}\right)$$

$$\equiv (1) \left(\begin{smallmatrix} 7 & 18 \\ 23 & 11 \end{smallmatrix}\right)$$

$$\equiv \left(\begin{smallmatrix} 7 & 18 \\ 23 & 11 \end{smallmatrix}\right)$$

ex. Decrypt "DEZC"

$$\begin{aligned} D(\text{"}DE\text{"}) \ &= \ D(<3 \ \ 4>) \\ &= \ (<3 \ \ 4>) \left(\begin{smallmatrix} 7 & 18 \\ 23 & 11 \end{smallmatrix}\right) \\ &\equiv <(21+92) \ \ (54+44)> \pmod{26} \\ &\equiv <113 \ \ 98> \pmod{26} \\ &\equiv <9 \ \ 20> \pmod{26} \\ &= \text{"JU"} \end{aligned}$$

$$\begin{aligned} D(\text{"}ZC\text{"}) \ &= \ D(<25 \ \ 2>) \\ &= \ (<25 \ \ 2>) \left(\begin{smallmatrix} 7 & 18 \\ 23 & 11 \end{smallmatrix}\right) \\ &\equiv <13 \ \ 4> \pmod{26} \\ &= \text{"NE"} \end{aligned}$$

so "DEZC" = "JUNE"

Benefits:
This is much more secure than previous block sizes
For large block sizes, the Hill Cypher is secure against ciphertext only attacks

Drawbacks:
Small block size which allows: Brute force attack possible Frequency analysis of digrams or trigrams

Eve does a chosen plaintext attack against a 2×2 Hill Cypher
Goal is to recover the key = $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$

First encrypt "BA" = $<1 \ \ 0>$
$E(<1 \ \ 0>) \ = <1 \ \ 0> \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \ = <a \ \ b>$
then encrypt "AB" = $<0 \ \ 1>$
$E(<0 \ \ 1>) \ = <0 \ \ 1> \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \ = <c \ \ d>$