# MATH 314 Sptring 2020 - Hill Cipher

02/05/2020

Scribe: Andrew Noonan

**Summary:** This cipher encrypts blocks of letters all at once. Encryption is done by changing one letter of plaintext, which changes multiple letters of ciphertext.

**Notes:**

- Encryption done through the use of matrices to encrypt blocks of text. Block length m, key : m * m matrix (mod 26)

  $E(\vec{v}) \equiv \vec{v} * K$ never $K * \vec{v}$

  E(rows)

  $\text{E}(<17,14>) = <17,14> * \begin{bmatrix} 10 & 3 \\ 5 & 0 \end{bmatrix} =<6,25> \text{ (mod 26)}$

  $\text{E}(<22,18>) = <22,18> * \begin{bmatrix} 10 & 3 \\ 5 & 0 \end{bmatrix} =<24,14> \text{ (mod 26)}$

  so rows becomes GZYO

- Decryption is done by multiplying the ciphertext with $k^{-1}$

  $\vec{V} * I = \vec{V}$

  $\text{D}(\vec{w}) = \vec{w} * k^{-1}(mod 26)$

  $k^{-1} = (ad - cb)^{-1} * \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$

  $\text{k}=\begin{bmatrix} 10 & 3 \\ 5 & 0 \end{bmatrix}$

  $k^{-1} = (10(0) - 3(5))^{-1} * \begin{bmatrix} 0 & -3 \\ -5 & -10 \end{bmatrix} = 11^{-1} * \begin{bmatrix} 0 & 23 \\ 21 & 10 \end{bmatrix} = 19 * \begin{bmatrix} 0 & 23 \\ 21 & 10 \end{bmatrix} = \begin{bmatrix} 0 & 21 \\ 9 & 8 \end{bmatrix} (mod 26)$

- Attacking the Hill Cipher

  Ciphertext only

  Bruteforce ($26^{m^2}$). Feasable only for small matraces. If m is less than 8, then the hill cipher is secure against CT only attacks

  Known Plaintext: as long as we know at least m blocks then we can break the cipher.

see examples

Chosen Plaintext

use vectors $< 1, 0 >$ and $< 0, 1 >$ to read off $< a, b >$ and $< c, d >$

**Examples:** Known plaintext attack.

- M =2, bool encrypts to CNDR

  E($< 1, 14 >$) = $< 1, 14 > * \begin{bmatrix} a & b \\ c & d \end{bmatrix} =< 2, 13 >$

  E($< 14, 11 >$) = $< 14, 11 > * \begin{bmatrix} a & b \\ c & d \end{bmatrix} < 3, 17 >$

  Combine vectors and make the encryption function

  $\begin{bmatrix} 1 & 14 \\ 14 & 11 \end{bmatrix} * k = \begin{bmatrix} 2 & 13 \\ 3 & 17 \end{bmatrix}$, We need to find the inverse of the plaintext matrix so we can "divide" both sides

  $\begin{bmatrix} 1 & 14 \\ 14 & 11 \end{bmatrix}^{-1} = (1*11-14*14)^{-1} * \begin{bmatrix} 11 & -14 \\ -14 & 1 \end{bmatrix} = 23^{-1} * \begin{bmatrix} 11 & 12 \\ 12 & 1 \end{bmatrix} = 17 * \begin{bmatrix} 1 & 12 \\ 12 & 1 \end{bmatrix} =$ $\begin{bmatrix} 5 & 22 \\ 22 & 17 \end{bmatrix}$, This is the inverse of the plaintext matrix

  k = $\begin{bmatrix} 5 & 22 \\ 22 & 17 \end{bmatrix} * \begin{bmatrix} 2 & 13 \\ 3 & 17 \end{bmatrix} \equiv \begin{bmatrix} 24 & 13 \\ 17 & 3 \end{bmatrix}$

- So, $\begin{bmatrix} 1 & 14 \\ 14 & 11 \end{bmatrix} * \begin{bmatrix} 24 & 13 \\ 17 & 3 \end{bmatrix} \equiv \begin{bmatrix} 2 & 13 \\ 3 & 17 \end{bmatrix} \pmod{26}$