MATH 314 Fall 2018 - Class Notes

09/10/2018

Scribe: Nicole Backert

Summary: Another classical cryptosystem, the Hill cipher, was discussed which uses matrices to encrypt blocks of text.

Notes: The Vigenere cipher was harder to break than other substitution ciphers, but it still only encrypted one letter at a time which allowed it to be broken. We need to encrypt blocks of text all at once to make a more secure cryptosystem.

The Hill Cipher

- Developed in 1929 by Lester Hill
- Uses matrices to encrypt blocks of text
- key = m x m matrix of numbers (mod 26)
- Once we have the key, we break up the plaintext into blocks of m and convert letters into numbers 0-25 and write as a vector of length m
- If the last block isn't full, we can pad the rest with X's
- Encryption function:

$$E(v) = v \times K (mod 26)$$

Where K = the key matrix

Example: Encrypt "june."

$$\texttt{"ju"} = < 9, 20 > \texttt{"ne"} = < 13, 4 >$$

$$E(< 9, 20 >) = < 9, 20 > \times \begin{matrix} 11 & 8 \\ 3 & 7 \end{matrix} (\text{mod } 26)$$

$$= < 9 \times 11 + 20 \times 3, 9 \times 8 + 20 \times 7 > (\text{mod } 26)$$
$$= < 159, 212 > (mod 26)$$
$$= < 3, 4 > (mod 26)$$

$E(< 13, 4 >) =< 13, 4 > \times \begin{matrix} 11 & 8 \\ 3 & 7 \end{matrix} (\text{mod } 26)$

$=$

¡$13 \times 11 + 4 \times 3, 13 \times 8 + 4 \times 7 > (mod 26)$
$= < 155, 132 > (mod 26)$
$= < 25, 2 > (mod 26)$
ciphertext $= < 3, 4, 25, 2 >$ = `DEZC`
Decryption: Multiply the ciphertext vector by the inverse matrix. We say that K is the inverse matrix if $K \times K^{-}1 = I$ (the identity matrix). For a 2 x 2 matrix the identity matrix looks like this: I =

$$\begin{matrix} 1 & 0 \\ 0 & 1 \end{matrix}$$

.

For any vector, $v \times I = v$. So if v is a plaintext vector, $w = v \times K$ is the ciphertext. We multiply w on the right by $K^{-}1$.
Decryption function:

$$D(w) = wK^{-}1(mod 26)$$

How do we find $K^{-}1$? When m = 2 we have the formula for the inverse of a matrix.
$W = \begin{matrix} a & b \\ c & d \end{matrix}$ then $K^{-}1 = \frac{1}{ad-bc} \times \begin{matrix} d & -b \\ -c & a \end{matrix}$

Since we are doing arithmetic $mod 26$ we don't divide $\frac{1}{ad-bc}$ (mod 26)

$\text{K}^{-}1 \equiv (ad - bc)^{-}1 \begin{matrix} d & -b \\ c & a \end{matrix} (\text{mod } 26)$

This means that ad-bc must have an inverse mod 26. Any number with a gcd > 1 with 26 is not invertible (gcd of (ab-dc) must be 1).
Therefore K is a valid key matrix if the determinant of K has gcd=1 with 26.
$K = \begin{matrix} 11 & 8 \\ 3 & 7 \end{matrix}$

det(K) $= (11 \times 7 - 8 \times 3) = 77 - 24 = 53 = 1(mod 26)$
$1^{=}1(mod 26)$
$K^{-}1 \equiv (1^{-}1) \begin{matrix} 7 & 18 \\ 23 & 11 \end{matrix}$

Example: *Decrypt*"$DEZC$."

$D(< 3, 4 >) =< 3, 4 > \times \begin{matrix} 7 & 18 \\ 23 & 11 \end{matrix}$

¡$3 \times 7 + 4 \times 23, 3 \times 18 + 4 \times 11 >$
$< 113, 98 >$

$< 9, 20 > mod 26 =$ `"ju"`

$$D(< 25, 2 >) =< 25, 2 > \begin{matrix} 7 & 18 \\ 23 & 11 \end{matrix}$$

¡25 $\times 7 + 2 \times 23, 25 \times 18 + 2 \times 11 >$
$< 221, 472 >$
$< 13, 4 > mod 26 =$ `"ne"`
Plaintext = `"june"`

Attacks: Chosen Plaintext Suppose key $K = \begin{matrix} a & b \\ c & d \end{matrix}$ and we want to recover the key.
Encrypt "abba".
$< 0, 1 >, < 1, 0 >$

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

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

As we can see, the Hill cipher is easily broken with a chosen plaintext attack.