MATH 314 - Class Notes

9/7/2017

Elizabeth Hubbard

Summary: We discussed the Hill Cipher

Notes: Block Cipher: Encoding multiple letters at a time (Block)

- Changing one letter of the plaintext changes an entire block of ciphertext.

Hill Cipher:

- Block Cipher
- Substantially more secure than any previous cipher
- Break the text into blocks of size m
- Key: mxm matrix with entries that are numbers (mod 26) that has determinant coprime to 26.
- To encyrpt we write a block as a vector (numbers mod 26), then take this vector and multiply it on the right by the key matrix.

$$E(\vec{v}) = \vec{v} \times K$$

- To decrypt we need to be able to multiply by the inverse matrix K^{-1}.

A matrix modulo 26 has an inverse if and only if its determinant has gcd 1 with 26.
In this case

$$D(\vec{v}) = \vec{v} \times K^{-1}$$

Basic Example

$$m = 2$$

$$K = \begin{bmatrix} 11 & 8 \\ 3 & 7 \end{bmatrix}$$

$$det(\begin{bmatrix} a & b \\ c & d \end{bmatrix}) = ad - bc$$

$$det(K) \equiv 77 - 24 \equiv 1 (\text{mod } 26)$$

Encrypt `"june"` Break into block `"ju"` $< 9, 20 >$ and `"ne"`$< 13, 4 >$

$$E(\texttt{"ju"}) = E(< 9, 20 >) =< 9, 20 > \times \begin{bmatrix} 11 & 8 \\ 3 & 7 \end{bmatrix} =< 9{\times}11{+}20{\times}3, 9{\times}8{+}20{\times}7 > \equiv < 3, 4 > (\text{mod } 26) \equiv \texttt{"DE"}$$

$E(\texttt{"ne"}) = E(< 13, 4 >) =< 13, 4 > \times \begin{bmatrix} 11 & 8 \\ 3 & 7 \end{bmatrix} =< 13{\times}11{+}4{\times}3, 13{\times}8{+}4{\times}7 > \equiv < 25, 2 > (\text{mod } 26) \equiv \texttt{"ZC"}$

"june" encrypts to "DEZC"
Suppose we encrypt "dune" we get "PIZC"

How to decrypt: we need to find the inverse matrix K^{-1} NOTE: for a 2x2 matrix $K = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ the inverse matrix is: $K^{-1} = \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$

From our example

$$K = \begin{bmatrix} 11 & 8 \\ 3 & 7 \end{bmatrix}$$

so

$$K^{-1} = (11 \times 7 - 8 \times 3)^{-1} \begin{bmatrix} 7 & 18 \\ 23 & 11 \end{bmatrix} = \begin{bmatrix} 7 & 18 \\ 23 & 11 \end{bmatrix}$$

Try this out: Decrypt "DEZC" "DE" $< 3, 4 >$ "ZC" $< 25, 2 >$

$$D(< 3, 4 >) =< 3, 4 > \times \begin{bmatrix} 7 & 18 \\ 23 & 11 \end{bmatrix} =< 3 \times 7 + 4 \times 23, 3 \times 18 + 4 \times 11 > \equiv < 9, 20 > \equiv \texttt{"ju"}$$

$$D(< 25, 2 >) =< 25, 2 > \times \begin{bmatrix} 7 & 18 \\ 23 & 11 \end{bmatrix} =< 25 \times 7 + 2 \times 23, 25 \times 18 + 2 \times 11 > \equiv < 13, 4 > \equiv \texttt{"ne"}$$

Ciphertext Only Attack If the block size is large (at least 16) then the hill cipher is in fact pretty secure. There aren't any attacks besides brute force. For small block sizes (like 2), frequency analysis of blocks works.

Known Plaintext Attack We know a string of plaintext and a string of ciphertext. This gives us an equation $CT = PT \times K$ So as long as we have m^2 letters of plaintext using this we solve a system of m^2 equations for m^2 unknowns (Entries of key matrix).

Chosen Plaintext Attack (m=2) Encrypt "ab"

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

Encrypt "ba"

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