MATH 314 Spring 2019 - Class Notes

2/12/2019

Scribe: Zachary Kafka

Summary: Introduced the concept of a polyalphabetic cipher, which maps multiple plain-text letters to the same corresponding cipher-text, discussed a new cipher called the Block cipher, and mainly covered a specific type of Block cipher called the Hill Cipher: we primarily discussed how to encrypt using the Hill Cipher, how to decrypt given cipher-text, and how to attack this cipher using chosen and known plain-text attacks.

Cryptographic History:

- Most ciphers previously thought to be unbreakable were found to be vulnerable to some form of frequency analysis
- These ciphers were monoalphabetic, meaning that they only encrypted one letter at a time. This means that changing one letter of plain-text only affected that cipher-text of that letter.

Block Cipher:

- Blocks of multiple plain-text characters are encrypted together
- Changing one letter affects the entire block of cipher-text

Hill Cipher:

- Uses linear algebra to encrypt
- Encrypt blocks of plain-text through matrix multiplication
- Start by fixing a block size m; your encryption key is then comprised of an m x m matrix of numbers (mod 26)

Encryption Function:

- Take an m x m matrix 'K' and a vector 'v' of numbers (mod 26)
- Divide the vector of letters into chunks of size m:
  E(v) = vk (mod 26)

Example: $K = \begin{pmatrix} 3 & 9 \\ 2 & 7 \end{pmatrix}$, m = 2

Plain-text to encrypt: `june`.

The plain-text letters `june` correspond to the numbers: 9, 20, 13, and 4 respectively.

Divide the word into chunks of size m: in this case, 2 letters per chunk. Our two chunks of numbers are now (9, 20) and (13, 4).

Now, multiply each section by the matrix k (For reference, matrix multiplication is done in one direction: multiply the row on the matrix on the left by the column on the matrix on the right):

$$(9,20)\begin{pmatrix} 3 & 9 \\ 2 & 7 \end{pmatrix} \pmod{26} = \begin{pmatrix} 27+40 & 81+140 \end{pmatrix} \pmod{26} =$$
$$\begin{pmatrix} 67 & 221 \end{pmatrix} \pmod{26} = (15,13)$$

This first matrix multiplication means that the plain-text `ju` corresponds to the cipher-text `PN`.

$$(13,4)\begin{pmatrix} 3 & 9 \\ 2 & 7 \end{pmatrix} \pmod{26} = \begin{pmatrix} 39+8 & 117+28 \end{pmatrix} \pmod{26} =$$
$$\begin{pmatrix} 47 & 145 \end{pmatrix} \pmod{26} = (21,15)$$

This second matrix multiplication means that the plain-text `ne` corresponds to the cipher-text `VP`. Now that both sections have been encrypted, the plain-text word `june` is converted into the cipher-text `PNVP`. Notice how two different plain-text letters are encrypted into the cipher-text letter 'P'.

However, what would happen if we were to encrypt the plain-text `dune` instead of `june`? Due to the change of letters in the first chunk, that section needs to be re-done.

$$(3,20)\begin{pmatrix} 3 & 9 \\ 2 & 7 \end{pmatrix} \pmod{26} = \begin{pmatrix} 27+40 & 81+140 \end{pmatrix} \pmod{26} =$$
$$\begin{pmatrix} 67 & 221 \end{pmatrix} \pmod{26} = (23,11)$$

The first chunk now converts to `XL`. Due to the fact that the second section remains the same, no change is required.

How do we decrypt it?:

We need to undo the matrix multiplication by K; in other words, we need to multiply by K^{-1} (The inverse of K). A matrix multiplied by its inverse is equal to the identity matrix, a matrix with 1's on the diagonal from northwest to southeast and 0's everywhere else; any matrix multiplied by the identity matrix returns the original matrix.

Below is an example of an identity matrix with m = 3.

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

D(w) = wk^{-1} (mod 26) where w = E(v).

D(E(v)) = D(vk) = $vkk^{-1} = v * I =$ v.

The inverse of a matrix is typically found by the formula:

$$K^{-1} = (1/(ad - bc)) \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$$

However, division is not an applicable operator in modular arithmetic. Therefore, the formula to find the inverse matrix is:

$$K^{-1} = (ad - bc)^{-1} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$$

However, not every matrix has an inverse. One can determine if the matrix has an inverse by finding its determinant: The determinant is found by the formula $(ad - bc)$. Now, a matrix only has an inverse if the determinant is not equal to 0, 13, or an even number.

Example: Find the decryption matrix when: K = $\begin{pmatrix} 3 & 9 \\ 2 & 7 \end{pmatrix}$, m = 2

$$K^{-1} = (ad - bc)^{-1} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} \pmod{26}$$

$$K^{-1} = ((3)(7) - (2)(9))^{-1} \begin{pmatrix} 7 & -9 \\ -2 & 3 \end{pmatrix} \pmod{26} = (3)^{-1} \begin{pmatrix} 7 & 17 \\ 24 & 3 \end{pmatrix} \pmod{26} = (9) \begin{pmatrix} 7 & 17 \\ 24 & 3 \end{pmatrix} \pmod{26} = (9) \begin{pmatrix} 63 & 153 \\ 216 & 27 \end{pmatrix} \pmod{26} = \begin{pmatrix} 11 & 23 \\ 8 & 1 \end{pmatrix}$$

This means that the final decryption matrix is:

$$\begin{pmatrix} 11 & 23 \\ 8 & 1 \end{pmatrix}$$

Now, decrypt the cipher-text `PNVP`. (The same procedure of chunking the plain-text is also performed in decryption.)

$(15,13)\begin{pmatrix} 11 & 23 \\ 8 & 1 \end{pmatrix} \pmod{26} = \begin{pmatrix} 165+104 & 345+13 \end{pmatrix} \pmod{26} =$
$\begin{pmatrix} 269 & 358 \end{pmatrix} \pmod{26} = (9,20)$ which corresponds to `ju`, which we know is right because of our previous encryption.

$(21,15)\begin{pmatrix} 11 & 23 \\ 8 & 1 \end{pmatrix} \pmod{26} = \begin{pmatrix} 231+120 & 483+15 \end{pmatrix} \pmod{26} =$
$\begin{pmatrix} 351 & 498 \end{pmatrix} \pmod{26} = (13,4)$ which corresponds to `ne`, which we know is right again because of our previous encryption.

<u>Eve wants to attack this cipher:</u>

- Chosen plain-text attack (assuming that the m is known and that the goal is to obtain an unknown key):
  - Encrypt `ba`: $(1,0)\begin{pmatrix} w & x \\ y & z \end{pmatrix} \pmod{26} = (1w+0y, 1x+0z) = (w,x)$
  - Now encrypt `ab`: $(0,1)\begin{pmatrix} w & x \\ y & z \end{pmatrix} \pmod{26} = (0w+1y, 0x+1z) = (y,z)$
  - Now the key matrix is recovered.
- Known plain-text attack:
  - Example to illustrate steps:
    - Suppose Alice sends Bob the cipher-text `LTPVPI` (corresponding numbers are 11, 19, 15, 21, 15, 8).
    - Eve learns the plain-text is "`linear`." (m = 2) (corresponding numbers are 11, 8, 13, 4, 0, 19).
    - Can Eve figure out the key?
      - Set up a system of equations:
        E((11, 8)) = (11, 8)k = (11, 19) (mod 26)
        E((13, 4)) = (13, 4)k = (15, 21) (mod 26)
        E((0, 7)) = (0, 7)k = (15, 8) (mod 26)

- Combine equations to get a matrix equation (be careful to check the determinant of the matrix attached to k, as sometimes it may not be invertible, as it is in the first example below):
  $\begin{pmatrix} 11 & 8 \\ 13 & 4 \end{pmatrix} * k = \begin{pmatrix} 11 & 19 \\ 15 & 21 \end{pmatrix}$

  The matrix equation to use in this particle example is:
  $\begin{pmatrix} 11 & 8 \\ 0 & 17 \end{pmatrix} * k = \begin{pmatrix} 11 & 19 \\ 15 & 8 \end{pmatrix}$
- Find the inverse of the matrix attached to k:
  $((11)(17)-(0)(8))^{-1} \begin{pmatrix} 17 & -8 \\ 0 & 11 \end{pmatrix} \pmod{26} = (187 \pmod{26})^{-1} \begin{pmatrix} 17 & 18 \\ 0 & 11 \end{pmatrix}$
  $\pmod{26} =$
  $(5)^{-1} \begin{pmatrix} 17 & 18 \\ 0 & 11 \end{pmatrix} \pmod{26} = (21) \begin{pmatrix} 17 & 18 \\ 0 & 11 \end{pmatrix} \pmod{26} = \begin{pmatrix} 357 & 378 \\ 0 & 231 \end{pmatrix}$
  $\pmod{26} = \begin{pmatrix} 19 & 14 \\ 0 & 23 \end{pmatrix}$
- Now, multiply both sides by this inverse matrix (Note: keep the inverse matrix on the left side of the matrix to be multiplied.):

  $$\begin{pmatrix} 19 & 14 \\ 0 & 23 \end{pmatrix} * \begin{pmatrix} 11 & 8 \\ 0 & 17 \end{pmatrix} = \begin{pmatrix} 19 & 14 \\ 0 & 23 \end{pmatrix} * \begin{pmatrix} 11 & 19 \\ 15 & 8 \end{pmatrix}$$
- The left matrices cancel out, leaving only the key matrix on that side. The final step is to finish the matrix multiplication on the right side, the result of which will be the encryption key:
  $\begin{pmatrix} 19 & 14 \\ 0 & 23 \end{pmatrix} * \begin{pmatrix} 11 & 19 \\ 15 & 8 \end{pmatrix} = \begin{pmatrix} (19*11)+(14*15) & (19*19)+(14*8) \\ (0*11)+(23*15) & (0*19)+(23*8) \end{pmatrix}$
  $\pmod{26}$
  $= \begin{pmatrix} 419 & 473 \\ 345 & 184 \end{pmatrix} \pmod{26} = \begin{pmatrix} 3 & 5 \\ 7 & 2 \end{pmatrix}$