MATH 314 Spring 2018 - Class Notes

2/13/2017

Scribe: Kevin Amick

Summary: Today we covered known plaintext attacks of the Hill Cipher, as well as the one time pad, perfect secrecy, and conditional probability.

Notes:

Decrypting the Hill Cypher:

We need to find a matrix k^{-1} such that $k * k^{-1} = I$ (Identity Matrix: $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$).

Inverse Matrix for 2x2 $= (ad - bc)^{-1} * \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$

In the Hill Cipher, the key matrix must have a determinant that has no factors in common with 26. Then the decryption function is

$$D(\vec{w}) = \vec{w}k^{-1} \pmod{26}$$

Example:

$$k = \begin{pmatrix} 11 & 8 \\ 3 & 7 \end{pmatrix}$$

$$\begin{aligned} k^{-1} &\equiv (11 - 24)^{-1} * \begin{pmatrix} 7 & 18 \\ 23 & 11 \end{pmatrix} \pmod{26} \\ &\equiv (53)^{-1} * \begin{pmatrix} 7 & 18 \\ 23 & 11 \end{pmatrix} \pmod{26} \\ &\equiv 1 * \begin{pmatrix} 7 & 18 \\ 23 & 11 \end{pmatrix} \pmod{26} \\ &\equiv \begin{pmatrix} 7 & 18 \\ 23 & 11 \end{pmatrix} \pmod{26} \end{aligned}$$

Decrypt DEZC

$$DE = \begin{pmatrix} 3 & 4 \end{pmatrix}$$
$$ZC = \begin{pmatrix} 25 & 2 \end{pmatrix}$$
$$\begin{pmatrix} 3 & 4 \end{pmatrix} * \begin{pmatrix} 7 & 18 \\ 23 & 11 \end{pmatrix} \equiv \begin{pmatrix} 21 + 92 & 54 + 44 \end{pmatrix} \equiv \begin{pmatrix} 9 & 20 \end{pmatrix} \pmod{26} \rightarrow "ju"$$
$$\begin{pmatrix} 25 & 2 \end{pmatrix} * \begin{pmatrix} 7 & 18 \\ 23 & 11 \end{pmatrix} \equiv \begin{pmatrix} 175 + 46 & 150 + 22 \end{pmatrix} \equiv \begin{pmatrix} 13 & 4 \end{pmatrix} \pmod{26} \rightarrow "ne"$$

Chosen Plaintext attack:

pick "ba" $\rightarrow \begin{pmatrix} 1 & 0 \end{pmatrix} * \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a & b \end{pmatrix}$

pick "ab" $\rightarrow \begin{pmatrix} 0 & 1 \end{pmatrix} * \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} c & d \end{pmatrix}$

Known Plaintext attack:

Eva captures the cyphertext `"LTPVPIZWUMSNTY"`

`"LTPVPI"`$\rightarrow$`"linear"`

$li = \begin{pmatrix} 11 & 8 \end{pmatrix} \rightarrow LT = \begin{pmatrix} 11 & 19 \end{pmatrix}$

$ne = \begin{pmatrix} 13 & 4 \end{pmatrix} \rightarrow PV = \begin{pmatrix} 15 & 21 \end{pmatrix}$

$ar = \begin{pmatrix} 0 & 17 \end{pmatrix} \rightarrow PI = \begin{pmatrix} 15 & 8 \end{pmatrix}$

Choosing `"line"`:

$$\begin{pmatrix} 11 & 8 \\ 13 & 4 \end{pmatrix} * k = \begin{pmatrix} 11 & 19 \\ 15 & 21 \end{pmatrix}$$

The determinant of the matrix on the left is $(44 - 104) = (-60)$ which is not invertible modulo 26, and hence this matrix does not have an inverse.

Must pick different plaintext, so we choose `"liar"`. This gives the matrix equation:

$$\begin{pmatrix} 11 & 8 \\ 0 & 17 \end{pmatrix} * k = \begin{pmatrix} 11 & 19 \\ 15 & 8 \end{pmatrix}$$

In this case the determinant of the matrix on the left is $(187)^{-1} \equiv 5^{-1} \equiv 21 \pmod{26}$, and so the inverse of the matrix on the left is

$$\begin{pmatrix} 11 & 8 \\ 0 & 17 \end{pmatrix}^{-1} \equiv 21 \begin{pmatrix} 17 & 18 \\ 0 & 11 \end{pmatrix} \equiv \begin{pmatrix} 19 & 14 \\ 0 & 23 \end{pmatrix} \pmod{26}$$

Multiplying both sides of the equation above by this matrix (on the left) we get

$$k \equiv \begin{pmatrix} 11 & 8 \\ 0 & 17 \end{pmatrix} \begin{pmatrix} 11 & 19 \\ 15 & 21 \end{pmatrix} \equiv \begin{pmatrix} 3 & 5 \\ 7 & 2 \end{pmatrix} \pmod{26} \leftarrow \text{key}$$

One Time Pad

Encryption is like the vigenere cipher except the key has the same length as the message. The key is a random string of letters and can be used only once.
Suppose Eve captures the cipher text "SBY" and guesses the plaintext could be "cat". This is possible if the key was "QBF", but any three letter word is possible.

We say a crypto system like this, where the cyphertext conveys no information to someone without the key, is a system with "perfect secrecy".

Probability

Notation:

P(A) = probability that A occurs
P(A flipped coin is heads) = 0.5
P(A|B) = probability that A happens if you know B happened
P(The roll of 2 dice sum to 12) = 1/36
P(The roll of 2 dice sum to 12 | The red die is a 6) = 1/6
P(A|B) = P(A and B)/P(B)

Ex: You find the following frequencies of Morning and Afternoon weather

Afternoon \ Morning	**Sunny**	**Rainy**	**Snowy**
Sunny	$\frac{1}{5}$	$\frac{1}{10}$	0
Rainy	$\frac{1}{10}$	$\frac{1}{5}$	$\frac{1}{10}$
Snowy	0	$\frac{1}{10}$	$\frac{1}{5}$

P(Rainy Afternoon) = $\frac{1}{10} + \frac{1}{5} + \frac{1}{10} = \frac{2}{5}$
P(Sunny Afternoon) = $\frac{3}{10}$
P(Sunny Afternoon | Rainy This Morning) = $\frac{\frac{1}{10}}{\frac{4}{10}} = \frac{1}{4}$

A system has perfect secrecy if for every key and any plaintext P, any ciphertext C, and any message M:

$$\text{P(The message M was P)} = \text{P(The message M was P} \mid \text{Ciphertext was C)}$$