MATH 314 Spring 2018 - Class Notes

02/12/18

Scribe: Teerra Thomas

Summary: This class covered know pt attack on Hill Cipher, What the One Time Pad is and perfect secrecy,and conditional probability

Notes:

Suppose Eve Captures the CT: `LTPVPIZWUMSNTY`

- Known pt attack on Hill Cipher:
- She learns the first 6 letters correspond to "linear"
- She also knows that the block length is $m = 2$

$$\begin{bmatrix} l & i \end{bmatrix} \begin{bmatrix} n & e \end{bmatrix} \begin{bmatrix} a & r \end{bmatrix} = \begin{bmatrix} 11 & 8 \end{bmatrix} \begin{bmatrix} 13 & 4 \end{bmatrix} \begin{bmatrix} 0 & 17 \end{bmatrix}$$
$$\begin{bmatrix} L & T \end{bmatrix} \begin{bmatrix} P & V \end{bmatrix} \begin{bmatrix} P & I \end{bmatrix} = \begin{bmatrix} 11 & 19 \end{bmatrix} \begin{bmatrix} 13 & 21 \end{bmatrix} \begin{bmatrix} 15 & 8 \end{bmatrix}$$

We then get these three equations:

1. (11, 8)K =(11, 19)
2. (13, 4)K=(15, 21)
3. (0, 17)K = (15, 8)

Use these to use a matrix equation!
Using the first two equations we get:

$$\begin{bmatrix} 11 & 8 \\ 13 & 4 \end{bmatrix} K = \begin{bmatrix} 11 & 19 \\ 15 & 21 \end{bmatrix}$$

We'd like to solve this equation fork
So "divide" both sides by:

$$\begin{bmatrix} 11 & 8 \\ 13 & 4 \end{bmatrix}$$

To do this we would multiply by the inverse matrix:

$$\begin{bmatrix} 11 & 8 \\ 13 & 4 \end{bmatrix}^{-1} = (44 - 104)^{-1} \begin{bmatrix} 4 & 18 \\ 13 & 11 \end{bmatrix}$$

But this det is not invertible and doesn't have an inverse!
Try again with equations 1 & 3

$$\begin{bmatrix} 11 & 8 \\ 0 & 17 \end{bmatrix} K = \begin{bmatrix} 11 & 19 \\ 15 & 8 \end{bmatrix}$$

$$\begin{bmatrix} 11 & 8 \\ 0 & 17 \end{bmatrix}^{-1} = (187 - 0)^{-1} \begin{bmatrix} 17 & 18 \\ 0 & 11 \end{bmatrix}$$

$$187 \equiv 5 \pmod{26}$$

$$5^{-1} \equiv 21 \pmod{26}$$

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

We can use this to solve for K by multiplying the first equation by this matrix on the left:

$$K \equiv \begin{bmatrix} 19 & 14 \\ 0 & 23 \end{bmatrix} \begin{bmatrix} 11 & 19 \\ 15 & 8 \end{bmatrix} \equiv \begin{bmatrix} 3 & 5 \\ 7 & 2 \end{bmatrix} \pmod{26}$$

One Time Pad:

- Encryption is like the vignere cipher except the key has the same length as the message, is a random string of characters and the key is only used one time

Eve intercepts the message:
(S, B, Y) = (18, 1, 24)

- Could this be the encryption of "cat"? Sure, if the key was (16, 1, 5)= (Q, B, F)
- No matter how long of a message Eve intercepts she will never learn anything about the pt from the CT

This idea of an unbreakable cryptosystem has a mathamathical definition called: "perfect secrecy"
To define this we need: **conditional probability**

P(A) = probability that "A" happens
P(a coin flipped is heads) = 1/2
$P(A|B)$= Probability that A happens if we know B
$P($(A coin is heads)$|$(it is 10 AM)) = 1/2
$P(A|B)$ = P(A and B)/P(B)

Example: Suppose you are a weather forecaster and you compare the weather in the morning to the afternoon in Towson

- SEE TABLE 1

Table 1: morning

	Sunny	Rainy	Snowy
Sunny	1/5	1/10	1/10
Rainy	1/10	1/5	1/10
Snowy	0	1/10	1/5

Table 2:

	K1	K2	K3
Yes	a	b	c
No	b	c	d

If it was rainy this morning what is the probability that it is sunny this afternoon?

P(Today is Sunny in afternoon) = (1/5) + (1/10) = (3/10)

$$P((\text{Sunny Afternoon})|(\text{Rainy this Morning})) = \frac{P(\text{Sunny Afternoon } \textbf{and} \text{ rainy morning})}{P(\text{rainy morning})}$$
$$= \frac{(1/10)}{((1/10)+(1/5)+(1/10))} = \frac{1}{4}$$

A cryptosystem has "perfect secrecy" if:

- for any key that Alice and Bob use and any plaintext P and ciphertext C

P(pt of message was p) = P((pt was p)|(CT was C)
Example: Suppose Alice and Bob only want to send: Yes or No

- SEE TABLE 2

Eve learns through frequency analysis they send "yes" (2/3) of the time and "no" (1/3)
P(message is "Yes") = (2/3) $\neq$ P((message is yes)|CT is D)
Therefore, system does not have perfect secrecy