MATH 314 - Class Notes

02/14/2017

Scribe: Melvin Gaye

Summary: In today's class we covered Hill Cipher, One-time pad and perfect secrecy. We did examples and practice problems. More information can be found at the end of chapter 2.

Notes: The function to find the matrix inverse is $m^{-1} = \frac{1}{ad-bc} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$

- Vigenere Cipher
  1. Attack method involves finding the key block length
  2. Find the key itself by shifting and using frequency analysis
  3. Security is dependent upon on the key length relative to the message
  4. Short keys can be found by shifting
- One-time pad
  1. The key length = the message length
  2. The key is RANDOMLY selected and it is ALWAYS only used once
  3. Since the key has the same length as the message, we can't attack it by shifting like the Vigenere Cipher
  4. Also because the letters are random we can't use frequency analysis
  5. The encrypt and decrypt steps are the same as the Vigenere Cipher

Perfect Secrecy: Given a crypto-system, that if given a message, the message would give an attacker no information about the plaintext they didn't already know.

Example: Eve intercepts the message `"SBY" (18,1,24)` Guess the plaintext: Could the message be `"dog" (3,14,6)?` Is there a key that would've encrypted ("dog") into `"SBY"`? We thought the key would be (15,13,18) `PNS`. This would've worked for any three letter word.

Eve doesn't learn anything by capturing this ciphertext. This captures the idea of perfect secrecy.

We try to measure information by probability. Given the occurrence of even A we try to guess the probability of event B occurring. We write it as P$(A|B)$. This is called conditional probability and it is always between a number and fractions.

Example: Studying weather in Towson: Is the weather in the morning related to the weather in the evening? Three possible conditions, sunny, rainy, or snow.

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

What is the probability it is rainy in the afternoon if it is snowy in the morning?

Formula for Conditional Probability

$\mathrm{P}(A|B) = \frac{P(AandB)}{P(B)}$ $P(rainyintheevening|snowyinthemorning) = \frac{1/10}{1/10+3/10} = \frac{1/10}{3/10} = 1/3$

Example: Alice and Bob are using a crypto-system to just send the messages `"yes" and "no"`. They send `"yes"` 1/4 of the time and `"no"` 3/4 of the time. Their system has 3 keys, K1, K2, and K3. Based on the key, the cipher text is given by the following table:

Text/Key	K1	K2	K3
yes	1	2	3
no	2	3	4

If they use K2 and Alice wants to encrypt the plaintext `"no"` she sends the ciphertext `"3"`. Alice and Bob pick keys at random 1/3. Even captured a ciphertext `"2"`. What is the probability that the plaintext is `"yes"`? 1/4.

Eve captures the $P(messagewas\texttt{"yes"}|Ciphertextwas\texttt{"2"})$

$\frac{P(\text{"}yes\text{"}andC=2)}{P(c=2)} = \frac{(1/4)(1/3)}{(1/3)(3/4)+(1/3)(1/4)} = 1/4$

Eve doesn't learn anything about the system after deciphering this. Again showing a perfect secrecy system.