MATH 314 - Class Notes

9/13/2016

Scribe: Abby Borowy

Summary: Today's class mainly covered the Hill Cipher and the One Time Pad and also briefly covered probability.

Notes:

Hill Cipher

- Encryption by multiplication by a matrix M
- The determinant of M and 26 must have a GCD of 1 ($GCD(det(m), 26) = 1$)
- If $M = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$, then $det(M) = ad - bc$ and $M^{-1} = (ad - bc)^{-1} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix} (mod 26)$
- ENCRYPTION: Break the plaintext into blocks and multiply each block by the matrix M $E(< x, y >) =< x, y > \begin{bmatrix} a & b \\ c & d \end{bmatrix} =< xa + yc, xb + yd >$
- DECRYPTION: Multiply by M^{-1}
- Example 1 (Chosen Plaintext Attack)
  - Suppose the secret key is in the form $M = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$.
  - Pick the plaintext $< 0, 1 >$. $E(< 0, 1 >) =< 0, 1 > \begin{bmatrix} a & b \\ c & d \end{bmatrix} =< c, d >$
  - Pick the plaintext $< 1, 0 >$. $E(< 1, 0 >) =< 1, 0 > \begin{bmatrix} a & b \\ c & d \end{bmatrix} =< a, b >$
- The Hill Cipher works easily with large matrices as well as small ones
- It is difficult to multiply large matrices by hand, so Sage can be used (see Hill Example on Sage)
- Almost all modern cryptosystems are block ciphers, like the Hill Cipher

One Time Pad

- Recall that the Vigenere Cipher is hard to break when the message is not much longer than the key
- The One Time Pad involves picking a key that is the same exact length as the message
- The key is picked completely randomly so it's hard to guess
- A key is only used once

- The message is encrypted the exact same way as it would be using the Vigenere Cipher
- The One Time Pad has "perfect secrecy," meaning it is truly impossible to break
- Example 2 (Ciphertext-only Attack)
  - Suppose we capture the message `SBY` (18, 1, 24)
  - Could the plaintext be `dog`? (3, 14, 6)
  - If the plaintext is `dog`, the key would be (15, 13, 18)
  - This is a possible key, but we cannot confirm it is the key
  - There's no way of finding the key, as it can be any three-letter word
  - The ciphertext doesn't tell us any information at all

Defining Perfect Secrecy Using Probability

- Conditional probability: the notation $P(A|B)$ means the probability of A happening if B happened
- Regular probability: $P(M = m)$ is the probability that the message being sent is "m"
- Let M be the message being sent and C be the ciphertext
- Then $P(M = m|C = d)$ is the probability that the original message was m if we know that the original ciphertext was d
- The system has "perfect secrecy" if $P(M = m|C = d) = P(M = m)$ for any message m
- C gives us no information about m