MATH 314 Spring 2019 - Class Notes

2/14/2015

Scribe: Kyle Shelton

Summary: Ciphertext-Only attack against Hill cipher, One-Time Pad, and Introduction to Number Theory and Euclid.

Notes:

Ciphertext-Only Attack Against Hill Cipher:

- For small block sizes, brute force all possible matrices or use a frequency analysis on diagrams or trigrams.
- For large matrices, Hill Cipher is secure against a ciphertext-only attack *(Brute force on a 20 x 20 matrix is too extensive).*

One-Time Pad:

- Key is completely random string of letters of the same length as the plaintext.
- The encryption is the same as the vigenere cipher.
- *Caveat: We can only use the key one time.*
- This cipher is completely unbreakable.
- Ciphertext-Only Attack: Any plaintext of that length is equally likely to be the correct message.
- Chosen Plaintext: Eve can learn characters in the key but these are never used again.
- Mathematically, this is perfectly secure, but impractical because the key must be agreed upon prior to the message being sent. Also, generating truly random sequences is harder than it may seem.

Number Theory - The study of divisibility relations of numbers, prime numbers, and patterns in the integers.

Euclid's Division Lemma - If j and k are integers with $k > 0$, then there exist integers q and r where $0 \leq r < k$, such that $j = qk + r$.

Proof:
Fix j, k
Compute $q = \lfloor \frac{j}{k} \rfloor$
Choose $r = j - qk$

Note that $j = qk + r$

Still need to show that:
$0 \leq r < k$
$\frac{j}{k} - 1 < q = \left\lfloor \frac{j}{k} \right\rfloor \leq \frac{j}{k}$
Multiply through by k.
$j - k < qk \leq j$
$(qk + r) - k < qk \leq qk + r$ *subtract qk from each term*
$r - k < 0 \leq r$
$r < k + 0$, $0 \leq r$
$r < k$