MATH 314 Spring 2020 - Class Notes

02/10/2020

Scribe: Luke Dixon

Summary: Today's class covered known Plaintext Attacks against the Hill Cipher; One-time pad, perfect secrecy, conditional probability and introduced Euclid's Algorithm.

Notes:

ciphertext only

1. Frequency analysis on blocks.

2. Brute force - How many keys? Block size m 26 m$^2 possiblematrices.$

- Both options work for small block sizes. Hill cipher is secure against ciphertext only if block size is large.

- or

Known plaintext attack

As long as we know more than m blocks of plaintext, we can break the key.
Ex. Suppose m = 2.
plaintext: "door" – "CJNR"
3,14, 14,17 – 2, 13, 9, 17
E(3,14) = (3,14)[a,b,c,d] = (2,13)
E(14,17) = (14,17)[a,b,c,d] = (9,17)
[3,14,14,17][a,b,c,d] = [2,13,9,17]
Find the inverse of the matrix: [3,14,14,17] $^{-1}$ = $(3{*}17-14{*}14)^{-1} = [17, 12, 12, 3(mod 26)]$
[3, 14, 14, 17] K = [2, 13, 9, 17] (mod 26)
(25-15)$^-$1
19 [17, 12, 12, 3] = [11, 20, 20, 5]
[11 , 20, 20, 5] [3, 14, 14, 17]*K = [11, 20, 20, 5][2, 13, 9,7]
K = [11,20,20,5][2,13,9,7]
chosen plaintext pick "ba" 1 0
E(1,0) = (1,0) [a, b, c, d] = a,b
"ab" = (0,1) [a, b, c, d] = c,d
you read off the key from above.
One-time pad
-Encryption is the same as the Vigenere Cipher
-key is the same length as plaintext
-completely random
-only used one time
-This cipher has perfect secrecy

-not very practical

Elementary Number Theory

want to compute gcd(n,m) - aka: greatest common factor

Example: gcd(35,85)

One way: factor both numbers, find biggest factor dividing both

Euclid's Algorithm

use division with remainder.

Theorem: if a and b are positive integers, then there exists integers q and r such that a = bq + r

where 0 is less than or equal to r which is less than b

*Proof: Fix a and b.

pick our q

q = floor(a/b)

compute r = a - bq

add bq to both sides

r+ bq = a

-need to prove that $0 \leq r < b$

-to do this start with q,

multiply through by b

$a/b - 1 < q = |_{(}a/b)_{|} \leq a/b$ $a - b < qb \leq a$ since $qb \leq ab$ $0 \leq a - qb =$ r and $a - b < qb$ r $= a - q < b$