MATH 314 Spring 2018 - Class Notes

2/5/2019

Scribe: Hamdan Alkaabi

Summary: We learned today about Affine cipher and how can we use it. We learned how to encrypt and decrypt using the affine cipher we learned that there is alot of affine cipher keys, and its hard to check all of these keys by hand.

Notes:

- We learned in the affine cipher that we should encrypt one letter at a time.
- We also learned that a key has two different numbers α, β
- The encryption Rule is Y = αx + β
- Since Fractions is not an option in affine cipher we Multiply by the inverse.
- The decryption function is $\alpha^{-1}(Y-\beta)\equiv X (\textbf{mod } 26)$.

How many possible keys for an affine cipher?

1. α has 12 possible keys.
2. β has 26 possbile keys.
3. 26 multiply by 12 gives us 312 possible keys for an affine cipher.

The other way to attack an affine cipher is using the frequency attack and we could make an educated guess at some letters.

Examples:

For example lets encrypt the word `car`.
We know that the encryption Rule is Y = αx + β. So the word `car` has the values 2,0,17.
Lets take $\alpha = 3$ and $\beta = 7$ and plug them in the encryption rule.
E(2)= 3(2)+7 = 13 (mod 26)$\rightarrow N$
$E(0) = 0 + 7 = 7(\text{mod } 26) \rightarrow H$
$E(17) = 17(2) + 7 = 58 \equiv 6(\text{mod } 26) \rightarrow G$
$Ciphertext =$ `N H G`

To decrypt we first find the decryption Function for $\alpha = 3$ and $\beta = 7$

$\text{Y} \equiv 3x + 7 (\text{mod } 26)$
$Y - 7 \equiv 3x (\text{mod } 26)$

Multiply both sides by $3^{-1} \equiv 9 (\text{mod } 26)$
$3 * 7 = 27 \equiv 1 (\text{mod } 26)$

$9(\text{Y-7}) \equiv X (\text{mod } 26)$
$9Y - 63 \equiv 9Y - 11 \equiv 9Y + 15 (\text{mod } 26)$

$\text{D(Y)} \equiv 9Y + 15 (\text{mod } 26)$
`Try cipher text NHG N = 13`

$\text{D(13)=9(13)} + 15 \equiv 132 \equiv 2 (\text{mod } 26)$
`2 is C so our decryption function works.`

<u>Plaintext Attack:</u> Suppose you know
'cup' is = OYB
22,20,15 $\rightarrow 14, 24, 1$
Setup equations
$2\alpha + \beta \equiv 14$ (mod 26)
$20\alpha + \beta \equiv 24$ (mod 26)
$18\alpha \equiv 10$ (mod 26)
Use C$\rightarrow O$
$P \rightarrow B$
$20\alpha + \beta \equiv 14$ (mod 26)
$15\alpha + \beta \equiv 1$ (mod 26)
$5\alpha \equiv 23$ (mod 26)
$21(5\alpha) \equiv 21x23 (\text{mod } 26)$
$\alpha \equiv 15 \rightarrow$ **Plug this in**
$20(15) + \beta \equiv 24$ (mod 26)
$14 + \beta \equiv 24 (\text{mod } 26)$
$\beta = 10$ (mod 26)
$\alpha = 15$, $\beta = 10$

<u>Chosen Plaintext Attack:</u> Eve gets to pick letters and encrypt them. She picks a = 0,
$\text{E(0)} = \alpha 0 + \beta = \beta$ She immediately learns β.
Then she picks 'b' $\equiv 1$ solve for X;
Instead of an equation just write out a table of the 26 plain letters and 26 corresponding cipher text.
a-b-c-d
K-R-B-Z

Substitution cipher

A key is any valid table.
How many possible key are there?
$26! \simeq 4.03\text{x}10^{26}$
which is way to big to brute force.