MATH 314 Spring 2018 - Class Notes

08/28/2019

Scribe: Michael Quang

Summary: Today's class covered Cryptanalysis and the Affine Cipher.

Note: Affine Cipher: Map letters to numbers, same as Caesar Cipher. Pick two numbers α, β. E(x) = αx+β

Example 1: Encrypt "it" $->$ 8 10 using the key (α,β)=(7,19)

$$E(8) \equiv 7(8)+19$$
$$E(8) \equiv 56+19 \equiv 75$$
$$E(8) \equiv 23(mod\ 26) -> X$$

$$E(19) \equiv 7(19)+19$$
$$E(19) \equiv 152 \equiv 22(mod\ 26) -> W$$

"it" $->$ "XW"

Example 2: Encrypt "me" $->$ 12 4 using the key (α,β)=(5,12)

$$E(12) \equiv 5(12)+12$$
$$E(12) \equiv 72 \equiv 20(mod\ 26) -> U$$

$$E(4) \equiv 5(4)+12$$
$$E(4) \equiv 32 \equiv 6(mod\ 26) -> G$$

"me" $->$ "UG"

Note: How do we decrypt the affine cipher?

We know the ciphertext y

$$y \equiv E(x) \equiv \alpha x + \beta\ (mod\ 26)$$

We know α,β solve for x.

Subtract β from both sides y-β from both sides y-$\beta \equiv \alpha$x $(mod\ 26)$

Fractions are never allowed in modular arithmetic

Find $\alpha^{-1} * \alpha \equiv 1\ (mod\ 26)$

Multiply both sides by α^{-1}

$$\alpha^{-1}*(y-\beta) \equiv \alpha^{-1}*(\alpha * x) \equiv x\ (mod\ 26)$$

Decryption function is $D(y) \equiv \alpha^{-1}(y-\beta) \equiv \alpha^{-1}y-\alpha^{-1}\beta(mod\ 26)$

Example 3: Decrypt "UG" using the key (α,β)=(5,12)

$$\begin{gathered} y = \alpha x+\beta \\ y \equiv 5x+12 \\ y\text{-}12 \equiv 5x \ (mod\ 26) \\ 21(y\text{-}12) \equiv 21(5)(x) \equiv x \\ D(y) \equiv 21y\text{-}(21)(12) \equiv 21y\text{-}18 \ (mod\ 26) \equiv 21y+8 \ (mod\ 26) \end{gathered}$$

$$\begin{gathered} \text{Decrypt "UG"} -> 20\ 6 \\ D(20) \equiv 21(20)+8 \\ D(20) \equiv 4+8 \equiv 12 \ (mod\ 26) -> \text{"m"} \\ D(6) \equiv 21(6)+8 \\ D(6) \equiv 22+8 \equiv 30 \equiv 4 \ (mod\ 26) -> \text{"e"} \end{gathered}$$

Note: α has an inverse, $\alpha^{-1}(mod\ 26)$ exactly when gcd(α,26) = 1. The valid keys for the affine cipher or $0 \leq \beta \leq 25$ and gcd(α,26) = 1, $0 \leq \alpha \leq 25$

How many possible keys are there for the affine cipher?
26 possibilities for β, 12 possibilities for α. 26*12 = 312 total possibilities which is too small to stop a brute force attack.

Example 4: Known Plaintext Attack "cup" -> "OYB"

$$\begin{gathered} \text{"cup"} -> 2,20,15 \\ \text{"OYB"} -> 14,24,1 \end{gathered}$$

$$\begin{gathered} \underline{\text{3 equations}} \\ 2(\alpha) + \beta \equiv 14 \ (mod\ 26) \\ 20(\alpha) + \beta \equiv 24 \ (mod\ 26) \\ 15(\alpha) + \beta \equiv 1 \ (mod\ 26) \end{gathered}$$

$$\begin{gathered} \text{Try 2nd and 3rd equations} \\ 20(\alpha) + \beta \equiv 24 \ (mod\ 26) \\ \underline{\text{- } 15(\alpha) + \beta \equiv 1 \ (mod\ 26)} \\ 5(\alpha) \equiv 23 \ (mod\ 26) \\ 21(5\alpha) \equiv 21(23) \ (mod\ 26) \\ \alpha \equiv 483 \equiv 15 \ (mod\ 26) \end{gathered}$$

$$\begin{gathered} \text{Substitute in } \alpha = 15 \\ 15(15) + \beta \equiv 1 \ (mod\ 26) \\ 17 + \beta \equiv 1 \ (mod\ 26) \\ \beta \equiv \text{-}16 \equiv 10 \ (mod\ 26) \\ (\alpha,\beta) \equiv (15,10) \end{gathered}$$

Note: Chosen Plaintext Attack

Pick "a" $->$ 0
$E(0) \equiv 0\alpha + \beta \equiv \beta \ (mod\ 26)$
Pick "b" $->$ 1
$E(1) \equiv \alpha + \beta \ (mod\ 26)$
Subtract off β to find α