MATH 314 Fall 2019 - Class Notes

8/28/2019

Scribe: Ryan Pickrel

Summary: Classical Crytography: Cryptoanalysis and the Affine Cipher.
The cipher explained in these notes further expands the number of possible keys compared to the previously learned Caeser Cipher. It does this through the use of both multiplication and modulus arithmetic (mod26)

Notes:

Affine Cipher Encryption

- Key (α, β) $\qquad 0 \leq \alpha, \beta \leq 25$
  - With extra restrictions on α

Encryption Function $E(x) \equiv \alpha x + \beta (mod 26)$
Ex: Encrypt `"if"` $\rightarrow$ `"JA"` $\qquad$ Take $\alpha \equiv 3, \beta \equiv 11$

- $E(i) \equiv E(8) \equiv 3(8) + 11 \equiv 35 \equiv 9(mod26) \equiv$ `J`
- $E(i) \equiv E(5) \equiv 3(5) + 11 \equiv 26 \equiv 0(mod26) \equiv$ `A`

Ex: Encrypt `"ac"` $\qquad$ Take $(\alpha, \beta) \equiv (5, 10)$ $\qquad$ $(\alpha, \beta) \equiv (13, 2)$
$(\alpha, \beta) \equiv (5, 10)$

- $E(a) \equiv E(0) \equiv 5(0) + 10 \equiv 10 \equiv$ `K`
- $E(c) \equiv E(3) \equiv 5(3) + 10 \equiv 25 \equiv$ `Z`

$(\alpha, \beta) \equiv (13, 2)$

- $E(a) \equiv E(0) \equiv 13(0) + 2 \equiv 2 \equiv$ `C`
- $E(c) \equiv E(3) \equiv 13(3) + 2 \equiv 28 \equiv 2(mod26) \equiv$ `C`

As we just discovered this starts to uncover the restriction on α. As we can see, if we let α be any number between 0 and 25, then we can have multiple ciphertext letters mapping to the same plaintext letter.

Affine Cipher Decryption
Take our encryption equation: $y \equiv \alpha x + \beta (mod 26)$ where y is ciphertext and x is plaintext

1. Solve for x

- $y - \beta \equiv \alpha x (mod 26)$

2. Fractions are not allowed in modular arithmetic
   - to "divide" we find a number $\alpha^{-1}(mod 26)$
3. If we can find this number α^{-1} we multiply both sides by α^{-1}
   - $\alpha^{-1}(y - \beta) \equiv \alpha^{-1}(\alpha x) \equiv x (mod 26)$

To decrypt with the key $(\alpha, \beta) \equiv (5, 10)$

1. Solve for x in $y = 5x + 10(mod 26)$
   - $y = 5x + 10(mod 26)$
   - $(y - 10) \equiv 5x + 10(mod 26)$
   - $21(y - 10) \equiv 21(5x) \equiv 10(mod 26)$
2. Decryption function: $D(y) \equiv 21(y - 10)$
   - $\equiv 21y - 10(21)$
   - $\equiv 21y - 2(mod 26)$
   - $\equiv 21y + 24(mod 26)$

CHECK: `"at"` $\rightarrow$ `"KB"`

- $D(10) \equiv 21(0) + 24 \equiv 2 + 24 \equiv 26 \equiv 0 \equiv$ `a`
- $D(1) \equiv 21(1) + 24 \equiv 21 + 24 \equiv 26 \equiv 19(mod 26) \equiv$ `t`

We can only decrypt if α has an inverse α^{-1} such that

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

FACT: α has an inverse (mod26) exactly when gcd(α,26) = 1

Affine Cipher Rule
Pick β with $0 \leq \beta \leq 25$, α with $0 \leq \beta \leq 25$, and gcd(α,26) = 1

Then...
$E(x) \equiv \alpha x + \beta (mod 26)$
$D(x) \equiv \alpha^{-1}(y - \beta)(mod 26)$

- 12 possibilities for α

- 26 possibilities for β
  $12 \times 26 = 312$ possibilities which is not that big for a computer. Brute force is still applicable for this cipher

Known plaintext attack
Eve learns that `"cup"` $\rightarrow$ `"OVR"`
3 equations:

- $E(2) \equiv \alpha(2) + \beta \equiv 14(mod 26)$
- $E(20) \equiv \alpha(20) + \beta \equiv 24(mod 26)$
- $E(15) \equiv \alpha(15) + \beta \equiv 1(mod 26)$

Take 2nd and 3rd equation to solve:

- $E(20) \equiv \alpha(20) + \beta \equiv 24(mod 26)$
- $-E(15) \equiv \alpha(15) + \beta \equiv 1(mod 26)$
- $\alpha(5) \equiv 23(mod 26)$
- $\alpha \equiv 15(mod 26)$
- $15(15) + \beta \equiv 1(mod 26)$
- $17 + \beta \equiv 1(mod 26)$
- $\beta \equiv -16$
- $\beta \equiv 10(mod 26)$
- Key $(\alpha, \beta) = (15,\ 10)$