MATH 314 Spring 2018 - Class Notes

2/1/2018

Scribe: Muhammad Harris

Summary: Today some basic and earlier cyphers were introduced, namely, the Caesar Cypher and the Affine Cypher. The method of encrypting a plaintext using these cyphers as well as attacking them in various manners is covered as well.

To break a crypto by conducting Crypt analysis, use Kerchoff's Principle, which states :

- When analyzing the security of a cryptosystem, you should always assume the attacker knows everything about the system except the key.
- The security of a system rests entirely on the diffuculty of figuring out the key.

The following are different appraoches to attacking cyphers:

- Cyphertext Only attack : Eve only has access to several differnet encryped messages. Goal is to decrypt the messages or better to obtain the key.
- Know Plaintext attack: Eve knows at least one plaintext and its corresponding cyphertext. She doesn't know the key, just original message and crypted message.
- Chosen Plaintext Attack : Eve temporarily has access to the encryption machine. She can encrypt any mesage she wants and obtain the ciphertext. Goal is to recover key.
- Chosen Ciphertext Attack: Eve has access to the decryption machine and can decrypt any ciphertext she wants. Goal is to recover the key.

Attacking the Caesar Cypher

- Cyphertext Only : Brute force; Frequency record of letters/chars in crypted message (frequency analysis)

- Known Plaintext Attack : Suppose Eve learns that the plaintext letter 'c' encrypts to the ciphertext 'T'
  C->2 E(2) = 2+k (mod 26)
  'T' -> 20 $\equiv$ 20 So k=18 (mod 26)

- Chosen Plaintext Attack : Eve picks 'A' and encrypts it.
  E(0) $\equiv$ 0+k (mod 26)
  $\equiv k \pmod{26}$
  Eve can recover the key immediately.

- Chosen Ciphertext : Eve picks any letter and performs a known plaintext attack.

Note : Modular arithmetic works with addition, subtraction, and multiplication (and sometimes division).

Affine Cipher

Encryption
Key : 2 Number α, β
Function : E(x) = $\alpha x + \beta$ (mod 26)

Example:
Encrypt "hi" (7,8) using:
$\alpha = 9$
$\beta = 3$

E(7) $\equiv 9 * 7 + 3$ mod(26)
$\equiv$ 66 (mod 26)
$\equiv$ 14 (mod 26)
= 'o'

E(8) $\equiv 9 * 8 + 3$ mod(26)
$\equiv$ 75 (mod 26)
$\equiv$ 23 (mod 26)
= 'x'

Using the Affine Cipher, Plaintext 'hi' -> Ciphertext 'ox'.

Decryption
We need a decryption function...
E(x) $\equiv (\alpha x) + \beta$ (mod 26)
Y $\equiv (\alpha x) + \beta$ (mod 26) *Need to solve for x here.

1.Y-$\beta \equiv \alpha x$ (mod 26)

To remove the alpha and isolate the 'x' to one side, we need to find an α^{-1} such that $\alpha * \alpha^{-1} \equiv 1$ (mod 26).
Then we call α^{-1} the inverse of α modulo m. In this case we say that α is invertible.
*Note : Fractions are never allowed when performing modular arithmetic.

Theorem : α is invertible modulo m if gcd(α, m) = 1.

Decryption Function : D(y) = α^{-1} * (y-β) (mod 26)

E(x) = 9x+3
D(y) = α^{-1} * (y-β) (mod 26)
$\equiv$ 3(y-3) (mod 26)
$\equiv$ 3y-9 (mod 26)
$\equiv$ 3y+17 (mod 26)

Decrypting 'ox'

D(14) $\equiv$ 3 * 14 + 17 (mod 26)
$\equiv$ 59 (mod 26)
$\equiv$ 7 (mod 26) -> 'h'

D(23) $\equiv$ 3 * 23 + 17 (mod 26)
$\equiv$ 69 + 17 (mod 26)
$\equiv$ 86 (mod 26)
$\equiv$ 8 mod(26)
-> 'i'

How many keys are their for affine cipher?
$0 <= \beta <= 25$ **26 Possibilities**
α = 1,3,5,7,9,11,13,17,19,21,23,25 **12 Possibilities**

Attacking the Affine Cipher

- Ciphertext Only Attack: Brute force or Frequency Analysis

- Known Plaintext Attack : Need 2 letters
  Suppose Eve learns that
  'k' -> y
  'd' -> 'f'

  $\alpha * 10 + \beta \equiv 24 \pmod{26}$
  $\alpha * 3 + \beta \equiv 5 \pmod{26}$
  Subtracting the two equations above yields :
  $=7\alpha \equiv 19 (mod 26)$

  $15 * 7 * \alpha \equiv 15 * 19 \pmod{26}$
  $\alpha \equiv 25 \pmod{26}$
  $25 * 3 + \beta \equiv 5(mod 26)$
  $22 + \beta \equiv 5(mod 26)$
  $\beta \equiv -17(mod 26)$
  $\beta \equiv 9(mod 26)$