MATH 314 Spring 2018 - Class Notes

Week 1 - Day 2

1/31/2018

Scribe: Brent Cash

Summary: In class we covered the different possible ways to attack a cipher. In addition, we learned the encryption and decryption functions for both the Caesar and Affine ciphers. We also applied the different types of attacks to both ciphers to better understand the weaknesses of both.

Kerchoff's Principle: When considering the difficulty of breaking a cryptosystem, one should assume the attacker knows everything about the system EXCEPT the key that is used.

All of the security of a system rests in the difficulty of finding the key.

4 Different Possible Attacks:

Ciphertext Only Attack: Eve only has the encrypted ciphertext and her goal is to decrypt it or to obtain the key used.

Known Plaintext Attack: Eve has at least one message where she knows the plaintext and the corresponding ciphertext and she wants to recover the key.

Chosen Plaintext Attack: Eve has access to the encryption machine and can encrypt any message. She wants to obtain the ciphertext.

Chosen Ciphertext Attack: Eve has access to the decryption machine instead and can decrypt any message.

Cryptanalysis of Caesar Cipher: key: k where $0 \leq k \leq 25$

Eve is trying to break the cipher

Ciphertext Only Attack:

- Brute force
- Frequency Analysis (some letters occur more often than others)
  (*See SMC Assignment 1*)

Known Plaintext Attack: Suppose Eve learns that `Q` is the ciphertext for `c`. How can she recover the key?

$$x = \texttt{c} = 2$$
$$E(x) = \texttt{Q} = 17$$

$$\begin{aligned} E(x) &\equiv x + k \pmod{26} \\ 17 &\equiv 2 + k \pmod{26} \\ 17 - 2 &\equiv k \pmod{26} \\ k &\equiv 15 \pmod{26} \end{aligned}$$

Chosen Plaintext Attack: Eve encrypts the letter `a`

$$E(0) \equiv 0 + k \pmod{26}$$

Eve recovers the key immediately

Chosen Ciphertext Attack: Eve would again choose the letter `a`

$$\begin{aligned} D(0) &\equiv 0 - k \pmod{26} \\ &\equiv -k \pmod{26} \end{aligned}$$

Solve for k

More Modular Arithmetic: All of the usual arithmetic operations carry over to modular arithmetic.

- Addition
- Subtraction
- Multiplication
- Sometimes division (*It is not allowd to divide by* $\boldsymbol{a}$ *if the GCD of* $\boldsymbol{a}$ *and the modulus* $\boldsymbol{M}$ *is NOT 1*)

Affine Cipher: The key is 2 numbers α and β.

$$E(x) \equiv \alpha x + \beta \pmod{26}$$

Example 1: If α=9 and β=3, then encrypt the message "hi". [Note: h=7 and i=8]

$$\begin{aligned} E(\mathtt{h}) = E(7) &\equiv 9 * (7) + 3 \pmod{26} \\ &\equiv 66 \pmod{26} \\ &\equiv 14 \pmod{26} \end{aligned}$$

$$\begin{aligned} E(\mathtt{i}) = E(8) &\equiv 9 * (8) + 3 \pmod{26} \\ &\equiv 75 \pmod{26} \\ &\equiv 23 \pmod{26} \end{aligned}$$

14=O and 23=X, hence, the message "hi" encrypts to "OX".

Decryption of Affine Cipher: We need to find a decryption function.
We know the encryption function is:

$$Y = E(x) \equiv \alpha x + \beta \pmod{26}$$

We solve for x:

$$\begin{aligned} Y &\equiv \alpha x + \beta \pmod{26} \\ Y - \beta &\equiv \alpha x \pmod{26} \end{aligned}$$

NOTE: You are **NEVER** allowed to write fractions in moduluar arithmetic!!!

We need some other way to do division (mod 26).

If x does not have a factor in common with 26, then there is some other number α^{-1}(alpha inverse) such that $\alpha * \alpha^{-1} \equiv 1 \pmod{26}$.

To do division we multiply by the inverse of the number:

$$\alpha^{-1}(Y - \beta) \equiv \alpha^{-1} * \alpha x \equiv x \pmod{26}$$

Decryption Function for Affine Cipher:

$$D(Y) \equiv \alpha^{-1}(Y - \beta) \pmod{26}$$

Example 2: $E(Y) \equiv 9x + 3 \pmod{26}$, where α=9 and β=3 *(from Example 1).*

Find the decryption function:

$$\begin{aligned} D(Y) &\equiv 9^{-1}(Y-3) \pmod{26} \\ &\equiv 3(Y-3) \pmod{26} \\ &\equiv 3Y - 9 \pmod{26} \\ &\equiv 3Y + 17 \pmod{26} \end{aligned}$$

Note: It is better to have addition than subtraction and, $-9 \pmod{26} \equiv 17 \pmod{26}$.

Decrypt: `"OX"` [Note: `O`=14 and `X`=23]

$$\begin{aligned} D(\texttt{O}) = D(14) &\equiv 3 * (14) + 17 \pmod{26} \\ &\equiv 59 \pmod{26} \\ &\equiv 7 \pmod{26} \end{aligned}$$

$$\begin{aligned} D(\texttt{X}) = D(23) &\equiv 3 * (23) + 17 \pmod{26} \\ &\equiv 86 \pmod{26} \\ &\equiv 8 \pmod{26} \end{aligned}$$

7=`h` and 8=`i`, hence, the message `"OX"` decrypts back to `"hi"`.

How many possible keys are there for an Affine Cipher?

There are 26 possibilities for β because $0 \leq \beta \leq 25$.

Whereas α has to be $0 \leq \alpha \leq 25$ where GCD(α, 26)=1 (mod 26). This means α has to be odd. So, α can be 1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23 or 25. [Note: 13 is the only odd number not on the list because it has a multiple of 26]

This means there are 12 possibilities for α.

$26 * 12 = 312$ possible keys (α,β).

Still possible to brute force an Affine cipher but alot harder.

Attacking the Affine Cipher:

Ciphertext Only Attack: Use Frequency Analysis to guess a couple of letters then use the ideas of a Known Plaintext Attack.

Known Plaintext Attack: Eve needs to know the ciphertext of two different letters.

Suppose Eve learns that `"k"` encrypts to `"Y"` and that `"h"` encrypts to `"F"`.

[Note: `k` = 10 encrypts to `Y`=24 and `h`=7 encrypts to `F`=5.]

$$\alpha 10 + \beta \equiv 24 \pmod{26}$$
$$\alpha 7 + \beta \equiv 5 \pmod{26}$$

Subtract the two equations from one another to get rid of β, leaving:

$$\alpha 3 \equiv 19 \pmod{26}$$

Then multiply each side by $3^{-1} \pmod{26}$, which is $9 \pmod{26}$, to get alpha by itself.

$$\alpha 3 * 9 \equiv 171 \pmod{26}$$
$$\alpha \equiv 15 \pmod{26}$$

Substitute α into either of the two origingal equations.

$$(15)7 + \beta \equiv 5 \pmod{26}$$
$$105 + \beta \equiv 5 \pmod{26}$$
$$\beta \equiv -100 \pmod{26}$$
$$\beta \equiv 4 \pmod{26}$$

Eve now has the key for the Affine Cipher with α=15 and β=4.

Chosen Plaintext Attack: Eve encrypts `"a"`=0

$$E(0) \equiv \alpha(0) + \beta \pmod{26}$$
$$\equiv \beta \pmod{26}$$

Eve encrypts `"b"`=1

$$E(1) \equiv \alpha + \beta \pmod{26}$$

Subtract β to recover α