MATH 314 – Class Notes

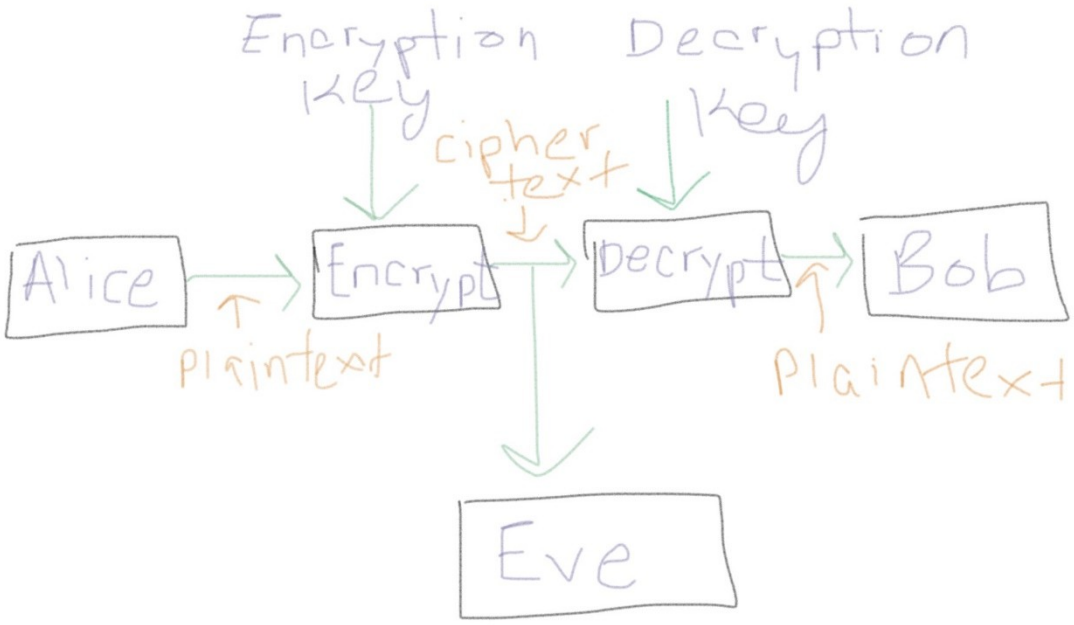
9/1/16

Author: Katherine Bridenstine

Summary:

- Basic Communication Scenario for Cryptography
- Key Vocabulary
- 4 Possible Attacks
- Conventions
- Caesar Cipher
- Attacking the Caesar Cipher
- Affine Cipher
- Attacking the Affine Cipher

The Basic Communication Scenario for Cryptography:



Key Vocabulary:

- Kerckhoff's Principle (1883): In assessing the security of a cryptosystem one should always assume the enemy knows everything about the system except the key. The security of the system should therefore be based on the key and not on the obscurity of the algorithm used. Consequently, we always assume that Eve has knowledge of the algorithm that is used to perform encryption.

Possible Attacks:

1. Known Ciphertext: Eve only has a copy of the ciphertext.

2. Known Plaintext: Eve has a copy of a ciphertext and the corresponding plaintext.
   For example: If Eve intercepts an encrypted press release, then sees the decrypted release the next day. If she can deduce the decryption key, and if Alice doesn't change the key, Eve can read all future messages.

3. Chosen Plaintext: Eve gets access temporarily to the encryption function (machine) and wants to obtain the key. She cannot open it to find the key; however, she can encrypt a large number of suitably chosen plaintexts and try to use the resulting ciphertexts to deduce the key.

4. Chosen Ciphertext: Eve obtains temporary access to the decryption machine, uses it to "decrypt" several strings of symbols, and tries to use the results to deduce the key.

Conventions:

- Plaintext is written in lowercase letters and CIPHERTEXT is written in capital letters.
- The letters of the alphabet are assigned with a = 0 and z = 25.
- Spaces and punctuation are omitted

Caesar Cipher/Shift Cipher:

- Caesar shifted each letter by 3 places, so a became D, b became E, c became F, etc. The end of the alphabet wrapped around to the beginning, so x became A, y became B, and z became C.
- Encryption Function: $E(x) = x + k \pmod{26}$

  (Caesar choose k = 3)

- Decryption Function: $D(x) = x - k \pmod{26}$
- Example: Encrypt the message "The die is cast", using the key k=8.

  Step 1: Remove spaces and punctuation

  thedieiscast

  Step 2: Convert the letters into numbers

19 7 4 3 8 4 8 18 2 0 18 19

Step 3: Add the key # to each number. In this case 8.

1 15 12 11 16 12 16 0 10 8 0 1

Step 4: Convert numbers back to letters.

B P M L Q M Q A K I A B

“B P M L Q M Q A K I A B” is the encrypted message that would be sent out.

Attacking the Caesar Cipher:

1. Ciphertext only:
    - Look at most common letters (frequency or statistical attack).
    - Brute force attack: Try all possible keys, look for the one that gives a meaningful message.

2. Known Plaintext: Suppose we know that t (19) encrypts to D (3). We can find the key by solving for k in this equation.

$$19 + k = 3 \pmod{26}$$

$$K = 3 - 19 \pmod{26}$$

$$K = -16 \pmod{26}$$

Which is the same as $k = 10 \pmod{26}$

3. Chosen Plaintext: Choose the letter a as the plaintext. The ciphertext gives the key. For example, if the ciphertext is H, then the key is 7.

4. Chosen Ciphertext: Choose the letter A as ciphertext. The plaintext is the negative of the key. For example, if the plaintext is h the key is -7, which is equivalent to 19 (mod 26).

Affine Cipher:

- Choose two integers α and β, with gcd (α, 26) =1
- Encryption Function: $E(x) = \alpha x + \beta$
    - Not all choices for α are possible though.
    - Only allowed values for α are odd and not divisible by 13. In other words gcd (α, 26) =1.

- For example. Encrypt “hi”. Given the key $\alpha = 9$ and $\beta = 2$.

Step 1: Convert the letters to their corresponding numbers.

7 8

Step 2: Using the key convert the plaintext to the ciphertext.

$E(7) = 9(7) + 2 \equiv 13 \pmod{26}$

$E(8) = 9(8) + 2 \equiv 22 \pmod{16}$

Step 3: Lastly convert those numbers to their corresponding letters.

13 -> N

22 -> W

So, “hi” encrypts to “NW”

- How to decrypt example. Solve for x when $\alpha=9$ and $\beta=2$.

$\alpha x + \beta = y \pmod{26}$

$9x + 2 = y \pmod{26}$

$9x = y-2 \pmod{26}$

$9x=y+24 \pmod{26}$ <- is the same thing as the above.

Modular arithmetic: any # that has no factors in common with the modulus has an inverse # multiples to 1.

$9 * 3 \equiv 1 \pmod{26}$

Now multiply both sides by 3

$3(9x) \equiv 3(y + 24) \pmod{26}$

$X = 3y + 20 \pmod{26}$

So the Decryption equation is $D(x) = 3x + 20 \pmod{26}$

- Decrypting “NW”

N -> 13 W -> 22
$D(13) = 3(13) + 20 \pmod{26}$
$= 7 \pmod{26}$ -> h
$D(22) = 3(22) + 20 \pmod{26}$
$= 8 \pmod{26}$ -> i

<u>Attacking the Affine Cipher:</u>

- Frequency analysis: Need to know 2 letters though
- Brute Force

        - 12 choices for α and 26 choices for β
        - 12 * 26 = 312 possible keys
- Known plaintext or chosen ciphertext/plaintext
    - Need 2 letters not one
    - Get 2 equations and 2 unknowns and we can solve for the key
    - GCD(α,26) =1