MATH-314 Feb 5th Lecture

Notes for Feb 5th MATH-314 lecture prepared by Ivan Goncharuk

Types of Attacks

Eve's Activities

- **Cipher text only**
  - Eve only has access to the cipher text.
  - Obtaining the cipher-text is her initial goal.
  - The main objective is to decipher the key.
- **Known plaintext attack**
  - Eve is aware of a cipher-text and its corresponding plaintext.
  - The goal is to discover the key.
- **Chosen plaintext attack**
  - Eve can select a plaintext and observe the corresponding ciphertext.
  - The goal is to unearth the key.

Attacking the Affine Cipher

- **Known plaintext attack**
  - Attempt all 312 keys through brute force.
  - Establish equations involving the key and solve them.

Example

Suppose you learn that "in" encrypts to "BI" using an affine cipher:

- i becomes an 8
- n becomes a 13

The encryption equations are:

$$E(8) \equiv a \cdot 8 + b \equiv 1 \pmod{26}$$

$$E(13) \equiv a \cdot 13 + b \equiv 8 \pmod{26}$$

Subtracting these equations, we get:

$$\begin{array}{c} 8a + b \equiv 1 \pmod{26} \\ -(13a + b \equiv 8 \pmod{26}) \\ \hline -5a \equiv -7 \pmod{26} \\ 5a \equiv 7 \pmod{26} \\ (21)(5a) \equiv (21)(7) \pmod{26} \\ a \equiv 147 \equiv 17 \pmod{26} \end{array}$$

To find (b):

$$\begin{aligned} 17 \cdot 13 + b &\equiv 8 \pmod{26} \\ 221 + b &\equiv 8 \pmod{26} \\ b &\equiv 8 - 221 \equiv -213 \equiv 21 \pmod{26} \end{aligned}$$

Therefore, (a = 17) and (b = 21).

What to Pick for Known Plaintext?

- Pick "a" (which converts to 0) as plaintext: (E(0) \equiv a \cdot 0 + b \equiv b \pmod{26})
- Pick "b": (E(1) = a + b \pmod{26}). Subtract (b) to find (a).

Cipher-text Only

- **Brute force**: Try all 312 keys to see which one reveals a valid message.
- **Use letter frequencies** to make educated guesses.

Substitution Cipher

- Utilize a key table for all 26 letters and their corresponding ciphertext letters.
- How many keys? (26!) for all possible combinations.

Vigenère Cipher

- Select a keyword.
- Encrypt by converting plaintext to numbers; below it, write the key converted to numbers.
- Add the two rows modulo 26.

Example

Plaintext: "car" -> 2 0 17

Keyword: "students" -> 18 19 20 3 4 13 19 18

Resulting cipher text: "UTLFEEVS"

Decryption

- Subtract the key from the ciphertext.

Known Plaintext Attack

- Subtract the plaintext from the ciphertext to find the key.

Ciphertext Only

- More challenging due to the difficulty in determining the key length.
- Shift the ciphertext and count coincidences to estimate the key length.

Finding Coincidences in Ciphertext

To detect the length of the key in a Vigenère cipher using ciphertext only, one method involves shifting the ciphertext against itself and counting the coincidences. This helps in estimating the key length.

Example

Suppose we have a ciphertext: `EEBQAARLM`

- **Original Ciphertext**: EEBQAARLM
- **Shift by 1**: _EEBQAARLM
- **Shift by 2**: __EEBQAARLM
- **Shift by 3**: ___EEBQAARLM

And so on. For each shift, align the letters and count how many times the same letter appears in the same position in the original and the shifted string.

Coincidence Counting

- **Shift 1**: No coincidences.
- **Shift 2**: No coincidences.
- **Shift 3**: 1 coincidence (the letter 'B').

This method is repeated for multiple shifts. A higher number of coincidences at a specific shift distance can indicate that the shift distance is a multiple of the key length. This is because the same key letters would be aligning with the same plaintext letters, leading to repeated patterns in the cipher-text.