COL759-Assignment-1

August 2024

1 Introduction

In this assignment, you need to implement the cryptanalysis on the Vigenère cipher. Your code will be tested with different ciphertexts. You need to write the code that successfully finds the key and decrypts any given Ciphertext. Remember to follow the procedure discussed in class.

Note: The key length will be at most 5 for all the test cases.

2 Methods to Use:

1. **Kasiski Method:**
   - Identify repeating sequences of characters in the ciphertext.
   - Analyze the distances between these repeating sequences.
   - Use these distances to estimate the length of the keyword.
2. **Index of Coincidence (IC):**
   - Calculate the IC for the ciphertext.
   - Use the IC to estimate the length of the keyword.
   - Compare the IC values with known values to determine the most likely keyword length.
3. **Mutual Index of Coincidence (MIC):**
   - Find the keyword by using the key length found using the IC method.

3 Sample Test Cases

1. **Input:** `Ciphertext: "Pspqmtorccw gc wgwtji jpoigxk mevqoptow dbsk geldmlq xm zylswf."`
   Output: `Key: "Key", plaintext: "Forgiveness is simply freeing ourselves from wanting to punish."`

2. **Input:** `Ciphertext: "T omvwmz ifmdkxa rvhu figlurz bti hcfik eavel; rskouzxvqwl myikoqw yzaq mmzhbvs snz urgmd ahzxh."`
   Output: `Key: "Time", plaintext: "A garden emerges from tending the outer world; forgiveness emerges from tending our inner world."`

4 Submission Instructions

- The code can be written in Python/C/C++/Java.
- Upload your code on Moodle and a pdf file mentioning the instructions to run the code, all in a zip file.
- **Deadline is 28th August 11:59 PM**
- Plagiarism i.e. similarity (more than 15%) with any part of the code available in the internet or similarity of code of two different students will lead to heavy penalty (may be F grade in the course or -10 marks).