Hacettepe University

Computer Engineering Department

BBM465 Information Security Lab. - 2024 Fall

Assignment 1

October 23, 2024

2220356141 - Ayşe Yaren Topgün

2210356008 - Sûdenaz Yazıcı

Introduction

In this assignment, we are asked to implement some basic ciphers that encrypts and decrypts messages. Then we should apply basic cryptanalysis techniques to attempt to break some encrypted messages. Assignment is divided into two parts as Cipher Implementatin and Cryptanalysis.

Part 1: Cipher Implementation

1.1 Caesar Cipher

In encryption method, we are shifting the alphabet with fixed number of positions to obtain cipher alphabet. When encrypting, the program firstly looks to the index of character in plain alphabet and then gets the corresponding indexed character in cipher alphabet. We firstly wrote a function to obtain shifted alphabet by splitting and connecting the alphabet again. In encrypt function, we call the function that shifts the alphabet. Then, we look for corresponding character for every character in plain text and add these to result list (lower and upper case characters are handled). Lastly, result list is joined to form a string.

In decryption method, we simply call the encryption method with minus shifting value.

1.2 Affine Cipher

In encryption method, we have one alphabet and we find the index of the new character with given a and b values. The formula is: $E(x) = (ax + b)modm$ and m value is 26 since we use English alphabet. Same as Caesar Cipher, we add new found characters into result list and lastly combine them into single letter.

In decryption method, we use the inverse of the formula: a^-1(y-b) mod m (a^1 is modular inverse and we use pow in Python to find that).

1.3 Mono-alphabetic Substitution Cipher

In encryption method, we look for the index of the character in original alphabet. Then, look at the character in given key in found index. This process is repeated for all characters in plain text.

In decryption method, we switch the original alphabet and the key and repeat the same process.

Part 2: Cryptanalysis

2.1 Caesar Cipher

We call the decryption function of Caesar cipher for all possible shift values. In each iteration, we split the found result from spaces and check all words from the message comparing to dictionary.

2.2 Affine Cipher

In this method, there are a few values of a and b to try. The chosen a values must be relatively prime with the number of characters of the used alphabet. Also, we choose the b values up to the number of characters of the alphabet since the greater values will lead up to repetition. After saving all these values, we try all possibilities with decryption method we wrote earlier. In each iteration, we split the words and compare them to dictionary. If all the words are meaningful, we print it.

2.3 Mono-alphabetic Substitution Cipher

In this method, we followed three main steps in the break_mono function to decrypt the monoalphabetic cipher:

- Matching the Top 5 Frequent Letters: First, we analyzed the frequency of letters in the ciphertext and matched the top 5 most frequent letters with the most commonly used letters in English. This gave us a partial decryption to start with.
- N-gram Analysis: Next, we applied frequency analysis using bigrams (two-letter combinations), trigrams (three-letter combinations), and quadrigrams (four-letter combinations). We compared these common n-grams in English with the ones in the ciphertext to make additional letter matches. This analysis helped us refine the letter mapping for more accurate decryption.
- Dictionary Check: In the final step, we took partially decrypted words that still contained unmatched letters and converted them into regex patterns. These patterns allowed us to search for potential matches in the dictionary. If a word in the dictionary matched the regex pattern, we replaced the partially decrypted word with the correct one from the dictionary. This step helped confirm the correct letter mappings and made the decrypted text more understandable.

Throughout this process, we wrote decrypted letters in lowercase and left the letters that had not yet been matched in uppercase. This allowed us to track which letters were successfully decrypted and which were still unsolved.

With these steps, we made significant progress in decrypting the text and came close to a solution, but we were unable to fully decrypt the ciphertext.