Lab 2: Attacking Classic Crypto Systems

Checkpoint 1 & Checkpoint 2

Imroj Hassan Shafi

Reg: 2020831050

November 2025

Contents

Chapter 1

Introduction

This report combines the results and analysis from **Checkpoint 1** and **Checkpoint 2** of Lab 2: *Attacking Classic Crypto Systems*. The objective of these checkpoints is to understand weaknesses in classical cryptographic systems through practical attacks, including:

- Brute force attacks on Caesar Cipher
- Frequency analysis attacks on Substitution Ciphers

Classical ciphers remain highly vulnerable to modern cryptanalysis techniques. Through these exercises, we explore why they fail and how we can exploit their structural weaknesses.

Chapter 2

Checkpoint 1: Breaking Caesar Cipher

2.1 Overview

The Caesar cipher is a substitution cipher where each plaintext letter is shifted by a fixed number of positions in the alphabet. Due to its tiny key space of only 25 possible shifts, it is extremely vulnerable to brute-force attacks.

2.2 Encrypted Message

```
odroboewscdrolocdcwkbdmyxdbkmdzvkdpybwyeddrobo
```

2.3 Approach: Brute Force

Since the cipher uses only lowercase letters and has 25 possible keys, we test all shifts from 1 to 25 and manually inspect which output forms readable English.

2.4 Decryption Code

```
def caesar_decrypt(text, shift):
    result = ""
    for char in text:
        if char.isalpha():
            result += chr((ord(char) - ord('a') - shift) % 26 + ord('a'))
        else:
            result += char
```

```
return result
```

2.5 Correct Decryption

At shift value **10**, we obtain:

```
everybodyiswantedcanbecausedbycanyoneeverybody
```

Breaking into words:
"everybody is wanted can be caused by anyone everybody"
Though spacing is missing (as expected in Caesar cipher), the plaintext is readable.

2.6 Why Caesar Cipher Fails

- Extremely small key space (25 keys)
- Same shift applied to all letters
- Easily brute forced in less than a second
- Preserves letter frequency structure

2.7 Conclusion

Caesar cipher is cryptographically useless by modern standards but helpful for demonstrating brute-force attacks and modular arithmetic concepts.

Chapter 3

Checkpoint 2: Breaking Substitution Ciphers

3.1 Overview

A substitution cipher maps each plaintext letter to a different ciphertext letter. Unlike Caesar cipher, the mapping is arbitrary, producing a key space of:

$$26! \approx 4 \times 10^{26}$$

Brute force is impossible, so we use **frequency analysis**, **pattern recognition**, and **iterative refinement**.

3.2 Cipher Texts

- **Cipher 1**: 491 characters of text
- **Cipher 2**: 1,943 characters of text

3.3 Techniques Used

1. Frequency analysis of letters
2. Identifying patterns: “the”, “and”, “of”, “to”, etc.
3. Substituting based on common English frequencies
4. Iteratively refining letter mapping

3.4 Cipher 1 Decryption

3.4.1 Key Observations

- Frequent pattern `cei` → "the"
- Pattern `du` → "of"
- Pattern `pfg` → "and"

3.4.2 Extract from Decrypted Text

> "in a particular and, in each case, different way, the folk were indispensable to him... because of his quick understanding of the principles of psychohistory..."

3.5 Cipher 2 Decryption

3.5.1 Key Observations

- `klu` appears 40+ times → "the"
- `omj` appears regularly → "and"
- `toz` → "was"

3.5.2 Extract from Decrypted Text

> "Bilbo was very rich and very peculiar, and had been the wonder of the Shire for sixty years..."

(Recognized as part of *The Lord of the Rings*.)

3.6 Which Cipher Was Easier?

Cipher 2 was significantly easier to break.

3.6.1 Reasons

- Longer text (4× longer than Cipher 1)
- More reliable frequency statistics

- More repeated patterns (e.g., “the”, “and”)
- Narrative context makes guesses easier

3.7 Key Insight

More ciphertext makes frequency analysis dramatically easier. This is why classical substitution ciphers fail: they preserve statistical structure.

Chapter 4

Combined Analysis

4.1 Major Learnings from Both Checkpoints

4.1.1 1. Larger Key Space Is Not Always Secure

Even though substitution ciphers have 26! possible keys, predictable language patterns still reveal plaintext.

4.1.2 2. Frequency Analysis Is Extremely Powerful

It can break any monoalphabetic substitution cipher with enough ciphertext.

4.1.3 3. Short Messages Are Harder to Attack

Counterintuitively, shorter ciphertext is harder to break because:

- Frequency patterns are noisy
- Fewer repeated patterns

4.1.4 4. Caesar Cipher Is Trivially Weak

Its key space is so small that brute force always succeeds.

4.1.5 5. Modern Cryptography Avoids These Issues

Modern ciphers:

- Have massive key spaces (e.g., AES-128 with 2^{128} keys)
- Do not preserve letter frequency

- Are resistant to brute-force attacks

Chapter 5

Conclusion

This combined report demonstrates practical attacks on two classical ciphers:

- **Caesar Cipher**: Broken using brute force.
- **Substitution Cipher**: Broken using frequency analysis and pattern recognition.

These exercises highlight the weaknesses of classical cryptography and explain why modern encryption must ensure large key spaces, statistical randomness, and strong mathematical foundations.

Classical ciphers play an important teaching role but offer no realistic security in modern systems.