Lab 2 — Attacking Classical Crypto Systems

Checkpoint:1

Objective: Break a Caesar-ciphered message and demonstrate the weakness of Caesar cipher.

Overview

The Caesar cipher shifts every letter in the plaintext by a fixed number (key) between 0 and 25. To break it without the key, the simplest reliable approach is a brute-force key search: try all 26 possible keys and look for the shift that produces readable English.

Why brute force here?

- Caesar cipher has only 26 possible keys — trying all possibilities is trivial for a computer.
- A successful decryption will produce recognizable English words (easy to spot visually).
- The lab requires demonstrating weakness; brute force demonstrates that the scheme provides little security.

Result

Decrypted message (shift = 10)**:**ethereumisthebestsmartcontractplatformoutthere

If we add spacing to improve readability, the intended plaintext is**:**

"ethereum is the best smart contract platform out there"

Conclusion: The Caesar key used is 10 and the plaintext is the sentence above.

[Note:Code provided in git repo]

Checkpoint2:Subsitution Cipher

Objective: Break two ciphertexts produced by simple substitution ciphers and compare difficulty.

Goal: Break two substitution-cipher texts and decide which is easier.

Method: Count letter frequencies → map ciphertext letters to English frequency order (`etaoin...`) → apply mapping to get initial plaintexts → manually refine using obvious short words/digrams → use an automated readability score to compare candidates.

Result: Cipher-1 is easier to break. Its mapped output already contained many recognizable short words and vowel patterns, so only a few manual swaps were needed. Cipher-2 was much noisier and required far more trial-and-error.

Why: Frequency mapping gave useful anchors (like probable “the”, “in”, “because”) in Cipher-1, accelerating recovery; Cipher-2’s patterns didn’t align well with English frequencies, so anchors were scarce.

Conclusion:

Through frequency analysis and manual refinement, both substitution ciphers were partially decrypted. Among them, Cipher-1 was easier to break because its letter frequency closely matched normal English patterns, producing recognizable words early in the process. In contrast, Cipher-2 required more effort, as its frequencies and letter patterns deviated more from standard English, making word identification harder. This lab clearly demonstrates that classical substitution ciphers are weak and easily broken using basic statistical and computational techniques, highlighting the importance of using modern encryption methods for secure communication.