1. Environment and Files

Language: Python 3

Files submitted / used:

caesarcipher.py — brute■force Caesar decipher script (Checkpoint 1).

hillclimbing.py — monoalphabetic substitution solver using frequency■initialization plus hill■climbing / simulated annealing plus fallback scoring (Checkpoint 2).

RNG seeds and parameters used are included in the scripts.

2. Checkpoint 1 — Caesar Cipher

2.1 Cipher

odroboewscdrolocdcwkbdmyxdbkmdzvkdpybwyeddrobo

2.2 Approach / Thought Process

The Caesar cipher is a simple shift cipher. The standard approach is to try all 25 non■trivial shifts and inspect outputs.

2.3 Code (essential)

```
ciphertext = "odroboewscdrolocdcwkbdmyxdbkmdzvkdpybwyeddrobo"

for key in range(1, 26):

decrypted = ""

for char in ciphertext:

shifted = (ord(char) - ord('a') - key) % 26

decrypted += chr(shifted + ord('a'))

print(f"Key {key}: {decrypted}")
```

2.4 Result

Key = 10 produced the readable plaintext:

ethereumisthebestsmartcontractplatformoutthere

Interpretation: ethereum is the best smart contract platform out there.

2.5 Conclusion

Caesar successfully broken by full■key search.

3. Checkpoint 2 — Substitution Ciphers

3.1 Task and Plan

Two substitution■cipher ciphertexts were provided. The solver applied frequency analysis to create an initial mapping, then refined it via hill■climbing with simulated annealing.

3.2 Fallback Scoring Summary

The score combined:

common■word matches,

bonus for “the”,

common digrams,

chi■square frequency similarity,

penalties for invalid one■letter tokens.

3.3 Solver Configuration

time_limit = 20s per cipher,

restarts = 8,

iterations_per_restart = 1400,

seeds: 1234 and 9999.

3.4 Results — Cipher 1

Recovered plaintext (after light cleanup):

in a particular and, in each case, different way, these four were indispensable to him…

pugo amarpl, because of his quick understanding of the principles of psychohistory and

of his imaginative field probings into new areas. it was comforting to know that if anything

happened to seldo[n] himself before the mathematics of the field could be completely worked

out… there would at least remain one good mind that would continue the research.

3.5 Results — Cipher 2

Recovered plaintext:

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

ever since his remarkable disappearance and unexpected return. The riches he had brought

back from his travels had now become a local legend…

3.6 Which Cipher Was Easier and Why

Cipher 2 was easier due to:

more common vocabulary,

clearer English frequency patterns,

higher redundancy,

stronger scoring signals.

4. Post■processing

Minor manual corrections were applied to fix remaining mapping artifacts. Expanding the scoring model would reduce manual edits.