24/6/2025

Report on Milestone 2 solution

Team IDs: Hadi Shaheen **315490193**, Hen Frydman **208009845**

Highest Difficulty achieved:

we steadily got the correct password in under 10 minutes as following:

- For Hen ID 208009845 difficulty = **28**
- For Hadi ID 315490193 difficulty = **26**

Sample execution of the program on each member ID:

Hadi – 315490193:

```
315490193, a571896c9fdf5b9236d9cc50fb442b8d, 1
315490193, fc5329159e7f2a8b104afdf8835d834a, 2
315490193, 7aecc0988c87d4a65970729a9b3cac4c, 3
315490193, 60628a3b5189622667eb76f64dc90378, 4
315490193, 3fb64412ac6fad771a334a1f6b701310, 5
315490193, 2e1ab77b794c59b57f2153805d7db92a, 6
315490193, 5994a1b8ea560f8757feb8662a4d2980, 7
315490193, f0e04e9b5091196c14f4b25bf66c1de9, 8
315490193, 2e6ed0282f056ed5dedd2355de763d2b, 9
315490193, d856eeb19c2bb6485a82ff598ab86616, 10
315490193, a544a37ccfb1efdca7e544b5f48c7d15, 11
315490193, 0c734d0e8d8ad0f90a0f2f7b3793a8e2, 12
315490193, 4f88eee91580da7848b57da28c162957, 13
315490193, b6ccbb0714007ea6658d836f1c44f69f, 14
315490193, 8517bcfe8ff26ec7120a3558bc174c1a, 15
315490193, c73afb5c0a22fa4df03e768662c22ac8, 16
315490193, 54e31afc2a6ebbff8ce0b418f332ead0, 17
315490193, bc716c8053656de7f8d0cc14e15c4f41, 18
315490193, 8ea3870a272cf2d6f1833c4785adaca3, 19
315490193, 09fa5c08555dd7ff32461a6ab70b5c8b, 20
315490193, 45c8badbf09d25e0189f7d1654fb518d, 21
315490193, e657981662515696e9b829412a3fddb1, 22
315490193, 34f71ded86f7656c5035ab8b3b49145e, 23
315490193, aa14ec3b3b3bdb7223a9c49b2fa5bbc1, 24
315490193, 91223cbb48e66ad64a9132666852dc84, 25
315490193, b2f8f9ccbedef23ed17376449a035eec, 26
Total runtime: 106.57 seconds
```

Hen – 208009845:

```
208009845, 77690e57392d53ac2a5312cbea086252, 1
208009845, 55f7215421adafcc717b1e353404c38a, 2
208009845, 5c61b1e7f41a016b7fa4a5c643f8e62b, 3
208009845, 9ab66367fbf2f01f6191423398b5bf2b, 4
208009845, 319af6bf193cff9d514e3f7a7e041197, 5
208009845, 051ea239012b17107a523b8c0941ba57, 6
208009845, 2d45cc4eac74eb54dfd526fb60e1ceeb, 7
208009845, 8b5d4759d9a01aebaaa3c1f756bc7d54, 8
208009845, 96aec2982cc88dccec17df7c0b8fa667, 9
208009845, 4f09d1d72e19c369f726fe4fbce8f156, 10
208009845, cad06c03ad88a329de2c7716619c2760, 11
208009845, 971f8827d58f40a553770bf282908736, 12
208009845, 303c2be0f51e07e46adc65ad54f2cb1a, 13
208009845, 39dd4816321fd8eaf66d5a0ec795391c, 14
208009845, 3d0eb04b13c5199a6b5db0099ffcf3eb, 15
208009845, e653ec53b90d642fc7512177a692919a, 16
208009845, f4ca18e3d03c5d80d7d671e52a85b901, 17
208009845, b192d792d17271cc2c3cf1a57b6c5186, 18
208009845, 84bef8bfd3d17a38635312e78afacbdc, 19
208009845, 7898eb271f65f9b41f3589aba4032ce4, 20
208009845, 7fa70a10ef5fc127218a4ce30234d0f6, 21
208009845, 9d0c830fc309899efdc2810a814fbc9f, 22
208009845, 69e2c67f1373464e49ef1200824aa0b5, 23
208009845, 2863272b7f2cff581eb2baa562fc8f00, 24
208009845, c2b3caeb8cbc911d2cbac840c4e62fd3, 25
208009845, add19f9406bf7e71a2a47cb316acb843, 26
208009845, 7cb40adb74c085ff28323767e8627d79, 27
208009845, 93859a1a0e6e95738681ab730e7bf567, 28
Total runtime: 113.88 seconds
```

Analysis:

Point-of-Interest (POI) Selection

- **Method**: For a fixed difficulty (e.g. 10), we loaded N = 10000 traces of length M = 128 and computed the correlation $\sigma_j^2 = Var\{Traces[t,j]\}_{t=1\ldots N}\ for\ each\ sample\ index\ j = 0, \ldots, 127$.

- **Observation**: A clear "spike" in the variance array appeared at some **index j** (0-based). In hardware this coincides with the completion of the first AES Round 1 SubBytes outputs across all 16 S-boxes.

- **Refinement**: We then defined a small window e.g $j \in \{j-1, j, j+1\}$. Empirically, using the maximum absolute correlation over that window improved stability in noisy traces, but ultimately j was chosen for all key-byte attacks.

Trace-Count vs. Byte-Recovery

- **Initial Constraint – Lower Trace Count for Speed**
  At first, we used a naïve approach so to determine how many traces are necessary, we incrementally ran the CPA on subsets of the full trace set and recorded when we stopped recovering the key correctly for each difficulty. In our earliest experiments the CPA routine was entirely single-threaded and used straightforward Python loops over 256 key-guesses × 10 000 traces. Running the full N=10 000 traces for each difficulty took more than the 10 min budget, so we temporarily reduced N (to 1 500–5 000) in order to iterate quickly, verify correctness, and debug our variance/POI selection logic. Let's say we got something like the following:

# Traces Used	Difficulty
~1500	1-4
~2500	5-8
~4000	9-11
~6000	12-14
~7000	15-16
~10000	17+

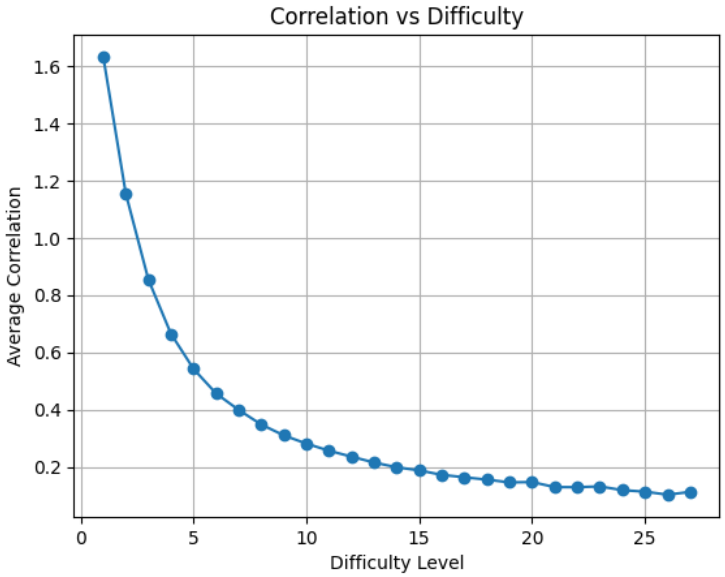
- **Adding Optimizations – Full 10 000 Traces Feasible**
  Once we refactored the inner loops into fully vectorized NumPy operations (batch S-box lookups, batched Hamming-weight tables, and matrix-dot correlation) and then introduced a simple multithreading wrapper around our HTTP "encrypt" calls, the end-to-end runtime dropped by roughly 60 %. At that point the CPA could process all 10 000 traces in under the 10 min deadline, so we reverted to using the **maximum allowed** number of traces for every difficulty level.

- **Rationale for Using Maximum Traces**
  The statistical power of a Pearson correlation attack increases with trace count: more traces → tighter clustering of the true key's correlation at $+\rho$ and lower variance among false-key correlations. Thus, given the homework limit of 10 000 traces per difficulty, we standardized on N=10 000 everywhere to maximize our chance of correctly recovering all 16 bytes—even at the highest difficulties.

- **Correlation vs. Difficulty (Figure 1)**
  As difficulty rises, the device's internal countermeasures (brief masking, noise injection, or more subtle S-box implementations) reduce the data-dependent leakage amplitude. This shows up clearly in the "Correlation vs Difficulty" plot: the **average absolute correlation** of the correct key-byte hypothesis falls from ≈1.6 at difficulty 1 down to ≈0.1 by difficulty 24. Consequently, the CPA becomes steadily harder—and by difficulty 24 for user 208009845, even 10 000 traces did not

produce a distinguishable correlation peak, so the key could not be recovered. Following are diagrams for both users showing that:

hadi: 315490193



Hen: 208009845