

Lab 12 Template

Some questions require multiple parts to be answered, be sure to discuss them in full.

Part 01:

1. Take a **screenshot of the location and time** where you were in contact with the COVID-19 patient to include in your lab report.

(10 points)

```
cpre3310@cpre3310:~/homework/Lab12/part01$ python3 part01_patient_tracing_skel.py
Common locations found: [{'location': 'MUPandaExpress', 'time': '2024-11-12T11:00:00'}]
```

2. **Upload** your code to Canvas.

(10 points)

Uploaded.

3. Please provide **another real-world example where PSI could be beneficial**. Justify your reasons why it maintains **confidentiality** and **privacy** in your proposed use case. Explain how it benefits **public good** and protects **individual rights**.

(25 total points, 5 each set of bold words)

Two financial institutions want to identify shared customers involved in potential laundering activities without exposing their full client list.

By using PSI each bank can compare customer lists and reveal only the accounts that match between them. This way they do not have to disclose the rest of their customer database/ sensitive financial information. This protects client confidentiality.

This method helps financial institutions and law enforcement detect and prevent illegal financial activities. This strengthens the financial system and protects the economy from criminal abuse.

PSI ensures that only accounts legitimately under suspicion are flagged while majority of innocent client data is confidential. It makes sure others are protected from unnecessary surveillance and safeguards their privacy and financial rights.

Part 02:

4. **Upload** your code to Canvas.

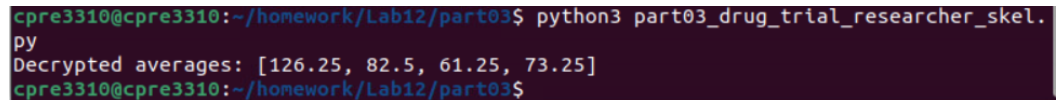
(10 points)

Uploaded.

Part 03:

5. **Take a screenshot of the 4 plaintext averages.**

(10 points)



```
cpre3310@cpre3310:~/homework/Lab12/part03$ python3 part03_drug_trial_researcher_skel.py
Decrypted averages: [126.25, 82.5, 61.25, 73.25]
cpre3310@cpre3310:~/homework/Lab12/part03$
```

6. **Upload** your code to Canvas.

(10 points)

Uploaded.

7. **How could partially homomorphic encryption be effectively used in an election?** 3 viewpoints

(25 total points, 8.33 points each perspective)

From a poll workers' vantage point they check in, issue ballots, and manage the polling place but they should not be able to see plaintext votes. With PHE when a voter casts their vote electronically, it is encrypted on the device using the public key. This way it makes sure that even if the worker accesses the machine they only see the encrypted data. This protects voter privacy and upholds integrity of the voting process.

From the vote counters' vantage point they get the encrypted votes. Using PHE they can sum the encrypted votes without decrypting ballots. This means they can verify total counts while keeping each individual's choice secret. If a recount is needed, they re-run the sums over the encrypted data while still ensuring transparency and accuracy without sacrificing anonymity.

From the election officials' perspective they hold the private key and can decrypt only the final tallies, not the individual votes. Once the summed encrypted results are submitted, the officials decrypt the totals to get final results of vote count. Then they report only the aggregated results to the authorities and public. This method allows officials to certify and publish trustworthy election outcomes while preserving ballot secrecy.