**COMP 3632 Assignment 3**

MENG Zihan

20412027

zmengaa@connect.ust.hk

1.

1. Differential privacy

Since you are reluctant to reveal your personal information, by adding noise, your personal data can be protected.

1. Secure multiparty computation

This method provides a solution to the scenario where two parties with different data can jointly compute a function on the union of their data while sharing no data at all.

1. Private information retrieval

Since you do not want DNS servers knows your private information, we use private information retrieval to ensure the privacy of your information.

1. k-anonymity

By k-anonymity, each set of identifiers must appear at least k times. This ensures that it won’t simply releasing everyone’s raw data.

2.

1. Sunday (full):

Monday (differential):

Tuesday (incremental):

Wednesday (differential):

Thursday (incremental):

Friday (differential):

Saturday (incremental):

Sunday (full):

1. Since a file can be changed twice, for all seven days in the week, the same files could be modified. Hence, the above answers for Wednesday and Friday may be different, which means the file changed on Wednesday can differ from to with the corresponding changes to Friday.
2. Data on Tuesday cannot be corrupted. Since the next backup is based on this backup, if the backup on Tuesday was corrupted, the next backup could no longer be produced.

3.

1. The cost of winning the reward:

So to make miners will not suffer a loss, the minimum price of a bitcoin is:

Which is $2000

1. Each block has at most 1048576 bytes;

Each transaction has size at least 166 bytes;

Then there exists at most transactions per second

1. We assume that the number of transactions per second follows uniform distribution.

So the mean of number of transactions is

Hence the transaction fee should be

The transaction fee should be $1.9

1. Assume we purchased bitcoin mining devices.

Cost:

Reward:

To make at least $1000000 profits per year:

And we have

So the minimum number of bitcoin mining machine we need to buy is 152.