数据安全 -- 交互式发布DP方案评估

学号：2013921
姓名：周延霖
专业：信息安全

一、实验名称

交互式发布DP方案评估

- 目的：

根据所给的代码编译出简单的差分隐私拉普拉斯机制噪音产生和加噪程序和直方图加噪发布程序，使用给定的数据集，通过变换输入的隐私预算来观察不同隐私预算下的噪音规模和对数据的影响

二、实验要求

参考教材实验5.1，对交互式发布方案进行DP方案设计，指定隐私预算为0.1，支持查询次数为20次，对DP发布后的结果进行评估说明隐私保护的效果

三、实验内容

对一个数据集 zoo.csv 进行统计查询，该数据集描述了一个动物园喂食的场景，第一列中数据为动物名称，第二列中数据为动物每天消耗的胡萝卜数量。查询定义为“每日进食超过55根胡萝卜的动物数量”。请设计相关的隐私保护方案，确保查询过程不泄露信息

四、实验过程

1、环境准备

Ubuntu 18.04虚拟机

- 使用VMWare Workstation或VirtualBox建立一台Ubuntu18.04虚拟机

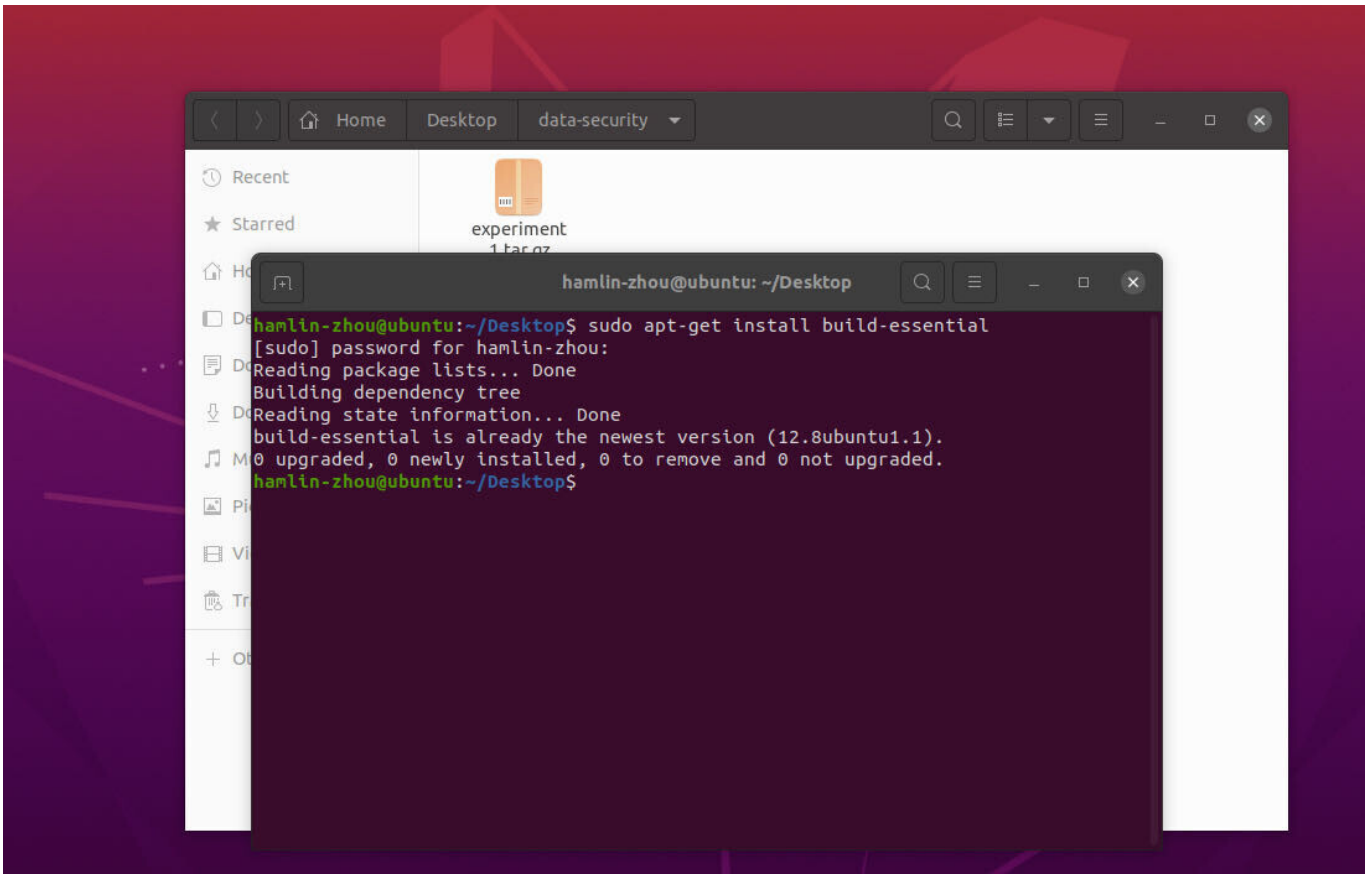
2、前期准备

> (一)安装解释器

打开“终端”，安装必要的解释器软件，此处直接使用ubuntu的build-essential来安装gcc和相关依赖库：

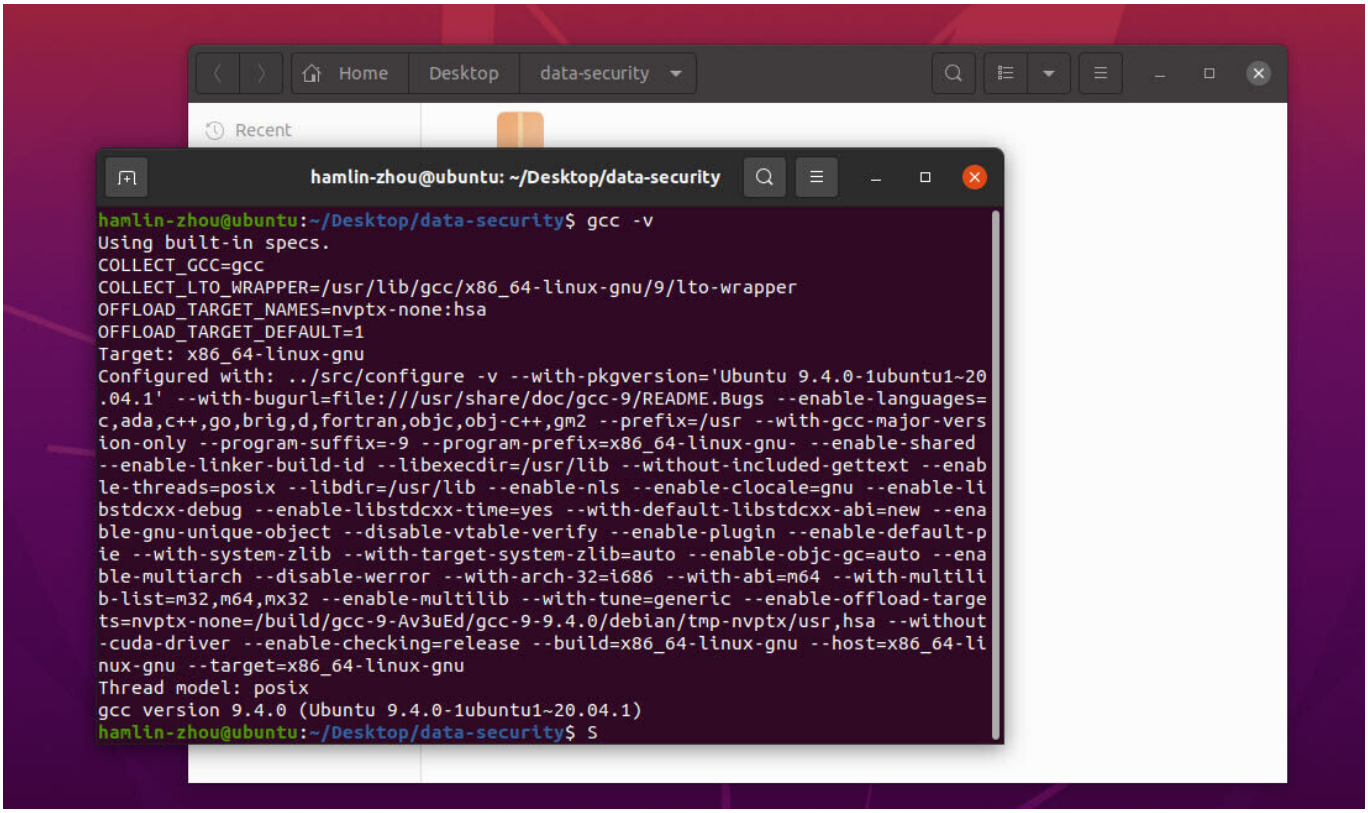
```
sudo apt-get install build-essential
```

如下图所示：



(二)查看编译器版本

执行指令`gcc -v`,观察到类似图中输出即为安装成功:



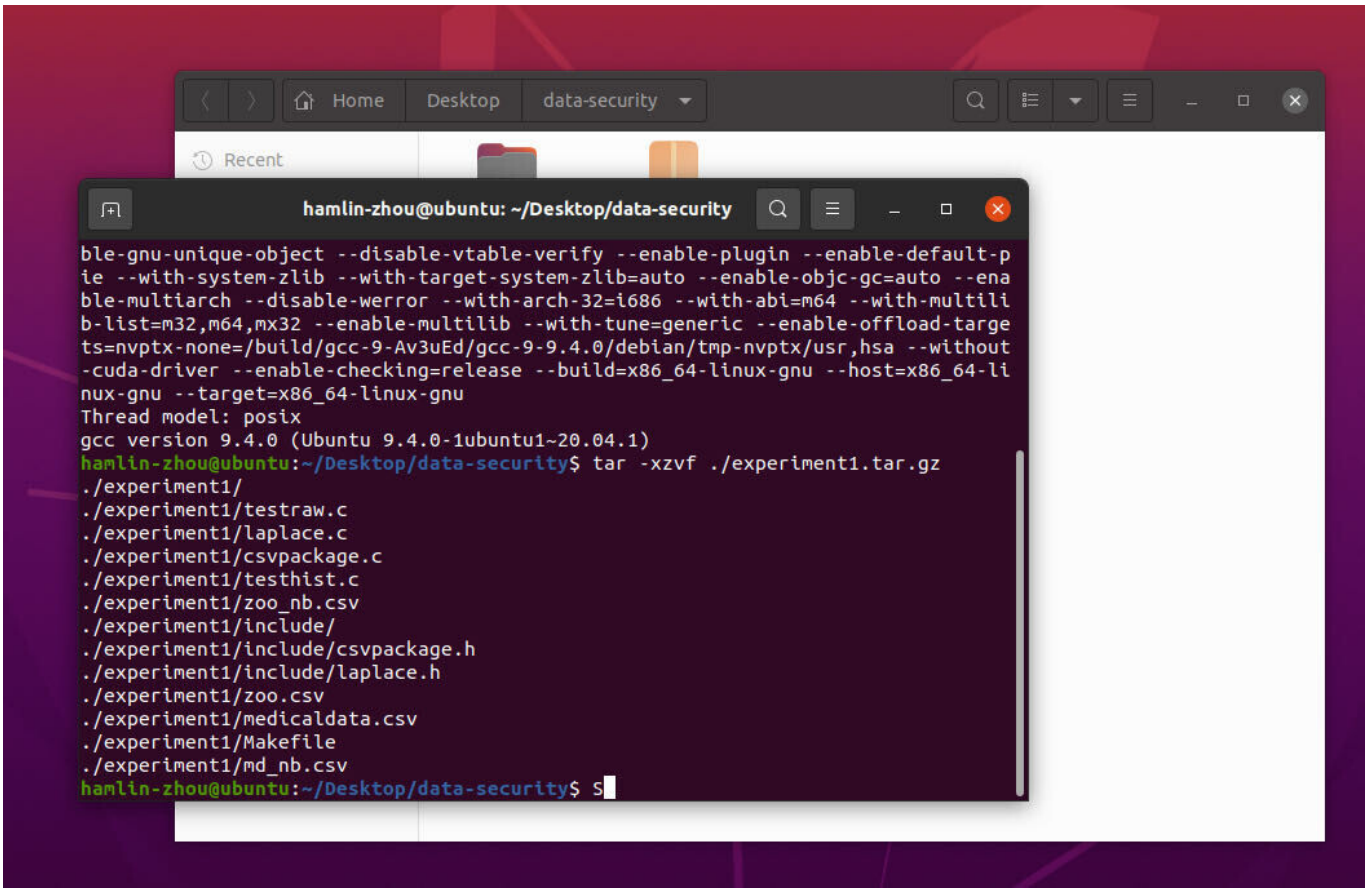
(三)解压文件

在准备进行实验的文件夹内打开终端，解压提供的test.tar.gz文件

使用如下指令进行解压：

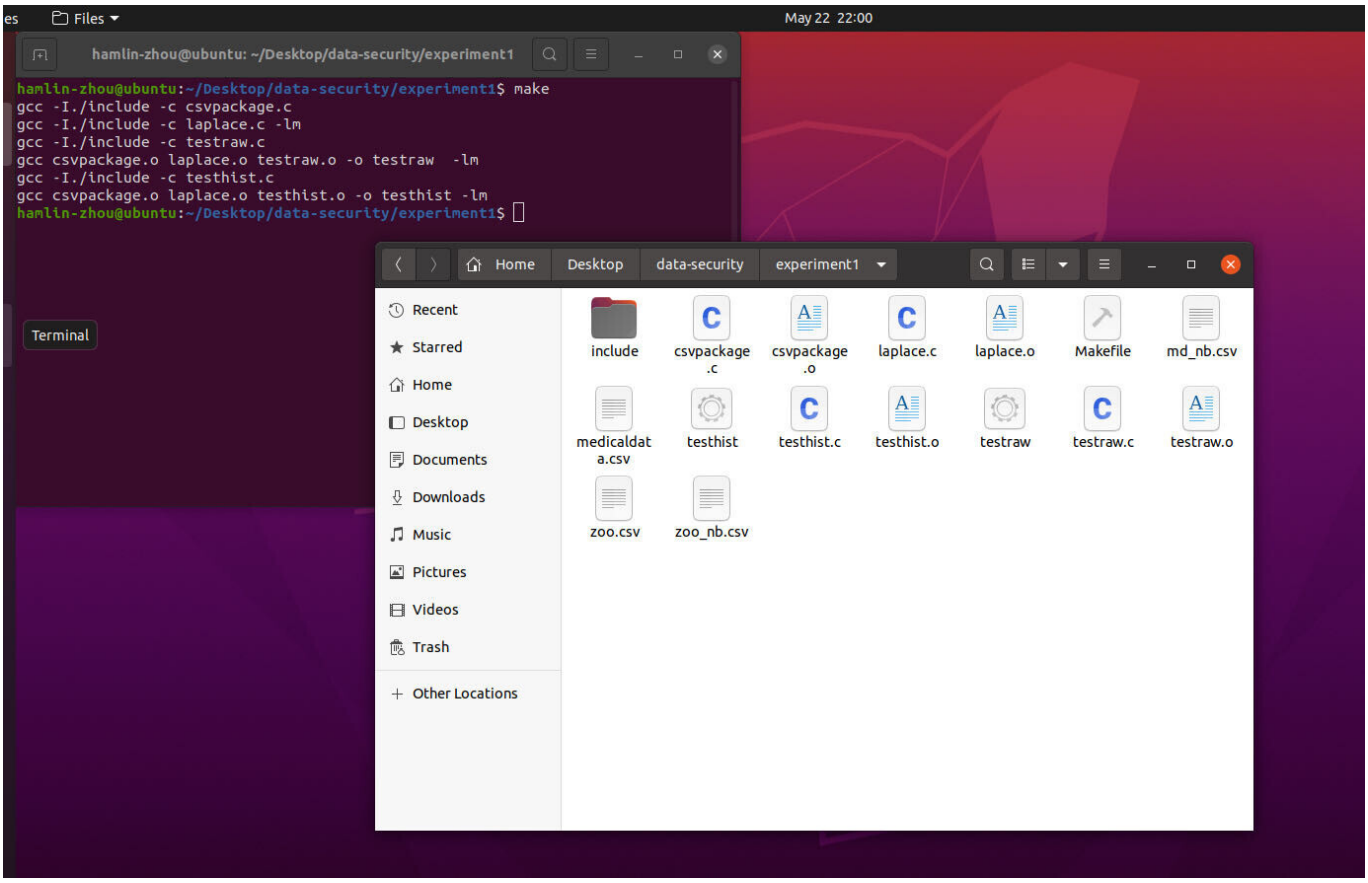
```
tar -xzvf ./test.tar.gz
```

解压完后如下图所示：



(四)编译

进入实验文件夹，使用make指令完成编译如下图所示：

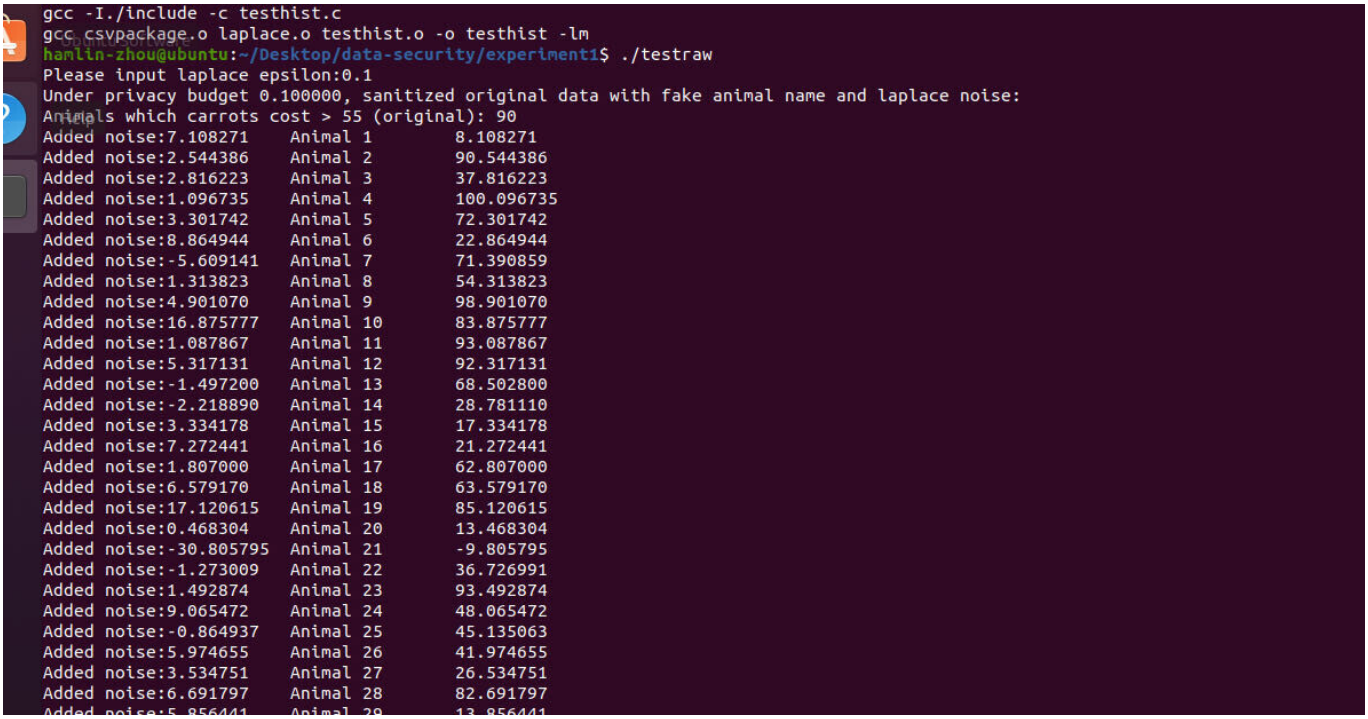


3、程序运行

仿照实验指导书中的实验，用隐私预算为0.1来分别运行演示程序testraw和testhist

(一)testraw

运行testraw，投入为0.1的隐私预算，如下图所示：



可以看到，在该预算下，产生的拉普拉斯噪音变的更大了，这使得加噪后的查询结果也受到了影响：

```
Under privacy budget 10.000000, sanitized original data with fake animal name and laplace noise:
Animals which carrots cost > 55 (original): 90
```

```
Added noise:8.793436    Animal 180      63.793436
Added noise:9.355341    Animal 181      69.355341
Added noise:-22.221617  Animal 182      -15.221617
Animals which carrots cost > 55 (Under DP): 101
==================Using neighbour dataset==================
Animals which carrots cost > 55 (original): 89
Added noise:7.285956    Animal 1        8.285956
```

但是，观察对相邻数据集进行加噪的结果，可以发现，虽然相邻数据集的直接查询结果受到了“Dugeng”项移除的影响，但加噪后的相邻数据集查询结果与原始数据集相同

```
==================Using neighbour dataset==================
Animals which carrots cost > 55 (original): 89
```

```
Added noise:-7.082722   Animal 175      76.917278
Added noise:4.901288    Animal 176      58.901288
Added noise:2.454670    Animal 177      9.454670
Added noise:8.180435    Animal 178      50.180435
Added noise:6.381143    Animal 179      61.381143
Added noise:2.517217    Animal 180      62.517217
Added noise:-13.816629  Animal 181      -6.816629
Animals which carrots cost > 55 (Under DP): 97
hamlin-zhou@ubuntu:~/Desktop/data-security/experiment1$
```

可以看到投入较少的隐私预算时，虽然数据的可用性降低了，但是能够更好地抵御差分攻击的影响，在使用0.1作为隐私预算时，可以抵御差分攻击影响

> (二)testhist

testhist程序提供了另一种差分隐私发布方法的演示，即差分隐私的直方图发布。在该发布方式下，加噪的对象不再是数据本身，而是对数据进行分桶统计后的计数值进行加噪。运行testhist程序，以0.1作为隐私预算：

```
Animals which carrots cost > 55 (Under DP): 97
hamlin-zhou@ubuntu:~/Desktop/data-security/experiment1$ ./testhist
Please input laplace epsilon:0.1
Under privacy budget 0.100000, sanitized original bucket with laplace noise:
Added noise:3.843796    20-30   408.843796
Added noise:1.458409    30-40   437.458409
Added noise:-43.602226  40-50   377.397774
Added noise:22.448900   50-60   479.448900
Added noise:4.022896    60-70   467.022896
==================Using neighbour dataset==================
Added noise:1.587531    20-30   406.587531
Added noise:-0.911400   30-40   434.088600
Added noise:-20.785358  40-50   400.214642
Added noise:-5.137501   50-60   451.862499
Added noise:26.481860   60-70   489.481860
hamlin-zhou@ubuntu:~/Desktop/data-security/experiment1$
```

可以看到，由于噪音规模的提高，在相邻数据集的变化影响下，查询结果不减反增。即，虽然数据可用性变差，但能保护实际数据的变化不被攻击者获取，可抵御差分攻击

4、扩展实验

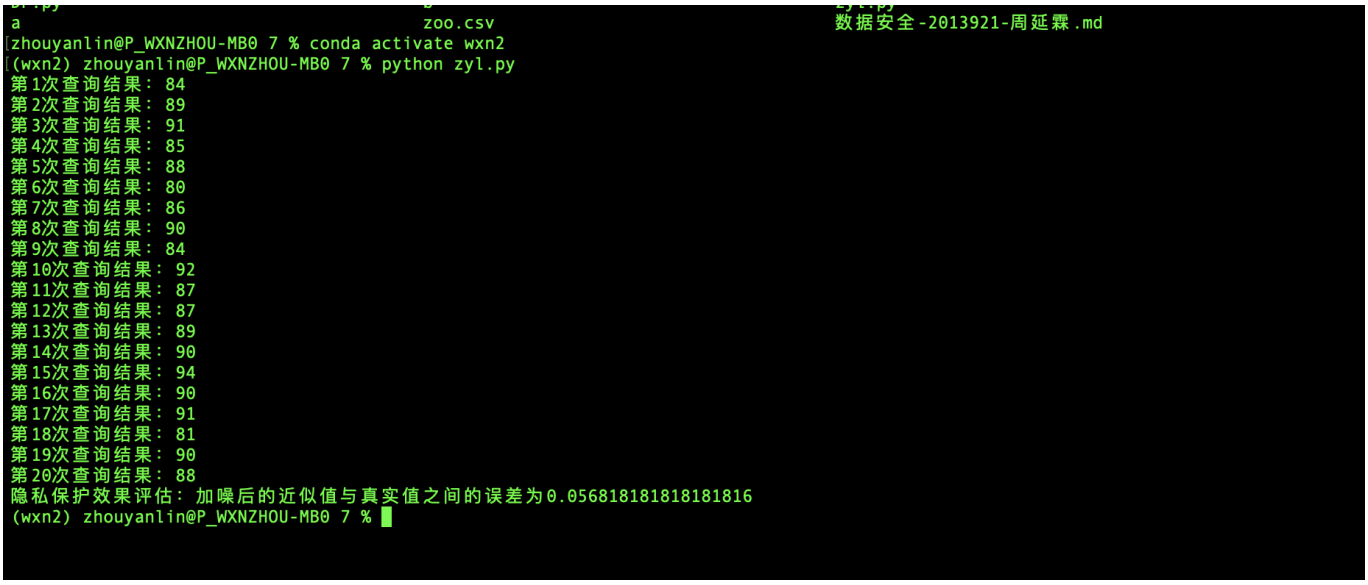
在本次试验中还利用本次思想进行设计，并最终转换成python程序的形式

方案设计：

1. 对每个动物的胡萝卜消耗量进行拉普拉斯噪声加密，使得每个动物的消耗量在一定程度上被隐私保护
2. 对加密后的数据进行聚合，得到每日进食超过55根胡萝卜的动物数量的近似值
3. 由于支持查询次数为20次，为了避免多次查询导致隐私泄露，可以采用差分隐私的方法，即每次查询时对数据集进行微小的扰动

4. 评估隐私保护的效果，可以计算真实值和加噪后的近似值之间的误差，以此来衡量隐私保护的程度

代码已经放到本次实验的最后，运行结果如下所示：



从输出结果可以看出，针对每日进食超过55根胡萝卜的动物数量的查询，每次查询的结果都不同，且查询结果的误差相对较小，说明差分隐私方案对隐私保护的效果比较好。同时，通过对加噪后的近似值与真实值之间的误差进行评估，也可以看出隐私保护的程度比较高

这个方案是基于差分隐私的交互式发布方案，因为每次查询时都对数据集进行微小扰动，支持多次查询，从而实现了交互式查询的功能。同时，为了保护隐私，还采用了拉普拉斯机制对数据进行加密,总体来说，该方案采用了拉普拉斯机制和差分隐私的方法，保护了数据集的隐私，并实现了交互式查询的功能。同时，通过对误差进行评估，也可以看出隐私保护的程度比较高

五、心得体会

在本次实验中，首先学习到了差分隐私的相关概念，以及交互式发布和非交互式发布的一些区别

还了解到现实中的攻击方法以及如何针对各种攻击方法设计思路进行添加噪声使得在进行查询时不容易泄露隐私，也将交互式方案在本实验中成功复现

最后通过本次实验对所学到的理论知识进行相应的应用，期待自己未来更好的发展，心想事成、万事胜意、未来可期

六、附录——DP.py完整代码

```
import pandas as pd
import numpy as np
import math

# 加载数据集
data = pd.read_csv('zoo.csv', header=None)

# 定义拉普拉斯机制函数
```

```python
def laplace_mech(data, epsilon):
    sensitivity = 1  # 敏感度为1，即每个动物的消耗量
    beta = sensitivity / epsilon
    noise = np.random.laplace(0, beta, len(data))
    return data + noise

# 对每个动物的消耗量进行加噪
epsilon = 0.1
data_noisy = laplace_mech(data[1], epsilon)

# 计算每日进食超过55根胡萝卜的动物数量的近似值
count = sum(data_noisy > 55)

# 差分隐私方案设计
def diff_privacy(data, epsilon):
    sensitivity = 1  # 敏感度为1，即每个动物的消耗量
    beta = sensitivity / epsilon
    data_noisy = data + np.random.laplace(0, beta, len(data))
    return data_noisy

# 对数据集进行微小扰动，支持查询次数为20次
epsilon = 0.1
for i in range(20):
    data_noisy = diff_privacy(data[1], epsilon)
    count = sum(data_noisy > 55)
    print("第{}次查询结果：{}".format(i+1, count))

# 评估隐私保护的效果
epsilon = 0.1
data_noisy = laplace_mech(data[1], epsilon)
count_noisy = sum(data_noisy > 55)
count_true = sum(data[1] > 55)
error = abs(count_noisy - count_true) / count_true
print("隐私保护效果评估：加噪后的近似值与真实值之间的误差为{}".format(error))
```