Project 3

Encrypted COMPANY

Due at the beginning of the class, Wednesday, November 17, 2021

**Submitted to Blackboard by the beginning of the class**

By

Dr. Chia-Chu Chiang

Department of Computer Science

University of Arkansas at Little Rock

2801 S. University Avenue

Little Rock, Arkansas 7204-1099, USA

Total Points: 100

Total Pages: 2 Pages

In Project 2, we maintain an employee table with encrypted salary and Salary\_inx (shown in Figure 1).

+----------+-------+---------+-----------+------------+---------------------------+------+----------+-----------+-----+-------------------------------+--------------+

| Fname | Minit | Lname | Ssn | Bdate | Address | Sex | **Salary** | Super\_ssn | Dno | Encrypted\_Salary |Salary\_Inx |

+----------+-------+---------+-----------+------------+---------------------------+------+----------+-----------+-----+--------------------------------|-------------+

| John | B | Smith | 123456789 | 1965-01-09 | 731 Fondren, Houston, TX | M | **30000.00** | 333445555 | 5 | | 4 |

| Franklin | T | Wong | 333445555 | 1955-12-08 | 638 Voss, Houston, TX | M | **40000.00** | 888665555 | 5 | | 8 |

| Joyce | A | English | 453453453 | 1972-07-31 | 5631 Rice, Houston, TX | F | **25000.00** | 333445555 | 5 | | 2 |

| Ramesh | K | Narayan | 666884444 | 1962-09-15 | 975 Fire Oak, Houston, TX | M | **38000.00** | 333445555 | 5 | | 6 |

| James | E | Borg | 888665555 | 1937-11-10 | 450 Stone, Houston, TX | M | **55000.00** | NULL | 1 | | 14 |

| Jennifer | S | Wallace | 987654321 | 1941-06-20 | 291 Berry, Bellaire, TX | F | 43000.00 | 888665555 | 4 | | 12 |

| Ahmad | V | Jabbar | 987987987 | 1969-03-29 | 980 Dallas, Houston, TX | M | 25000.00 | 987654321 | 4 | | 2 |

| Alicia | J | Zelaya | 999887777 | 1968-01-19 | 3321 Castle, Spring, TX | F | 25000.00 | 987654321 | 4 | | 2 |

+----------+-------+---------+-----------+------------+---------------------------+------+----------+-----------+-----+--------------------------------+-------------+

Figure 1: Encrypted Employee Table

In this project, we are going to encrypt the Salary column using Paillier Cipher [1].

The following SQL statements are used to help answer the following questions.

mysql> Use Company;

mysql> Show Database;

mysql> show tables;

mysql> show tables;

+-------------------+

| Tables\_in\_company |

+-------------------+

| department |

| employee |

+-------------------+

2 rows in set (0.01 sec)

You should now be able to encrypt each individual salary using the Paillier cipher and use the SQL update statement to update the encrypted values into Encrypted\_salary. A sample is shown below with the value of Encrypted\_salary blank.

mysql> update employee set encrypted\_salary = 'TO BE FILLED IN', where minit='T';

Query OK, 1 row affected (0.00 sec)

Rows matched: 1 Changed: 1 Warnings: 0

Continue to update the Encrypted\_salary for the rest of employees.

You are now ready to answer the following questions against the encrypted database COMPANY. Please use the tool in [2] to help perform Salary encryption in Paillier.

**Questions**

1. (25 Points) Select sum(Salary) from employee;
2. (75 Points) Select sum(Encrypted\_Salary) from employee; and decrypt the sum of Encrypted\_salary using Paillier, you should be able to get the same value to Question 1.

**References**

[1] What is the Paillier cryptosystem? https://blog.openmined.org/the-paillier-cryptosystem/

[2] Javascript Paillier demo - homomorphic encryption in the browser, https://mhe.github.io/jspaillier/