Project 4

Encrypted COMPANY

Due at the beginning of the class, Wednesday, December 1, 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 this project, we are going to practice the Multiplicative Homomorphism using RSA Cipher. Given two messages m1 and m2, Encrypt(m1 \* m2) is equal to Encrypt(m1) \* Encrypt(m2).

The following SQL statements are used to help implement this project.

mysql> Use Company;

mysql> Show Database;

mysql> show tables;

mysql> show tables;

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

| Tables\_in\_company |

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

| department |

| employee |

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

2 rows in set (0.01 sec)

We are going to add new two columns, namely, economic stimulus and dependents to the employee table. The economic impact is economic stimulus \* dependents.

Economic Impact = Economic Stimulus \* Dependents;

For the purpose of confidentiality, the values of economic stimulus and dependents are encrypted using RSA scheme. The values of economic impact are computed by multiplying encrypted economic stimulus by encrypted dependents.

You should now be able to encrypt each employee economic stimulus and dependents using the RSA cipher and use the SQL update statement to update the encrypted values into Encrypted\_stimulus and encrypted dependents.

First, we add four new columns of (economic) stimulus, dependents, encrypted\_stimulus, and encrypted\_dependents to the employee table.

mysql> alter table employee

-> add column stimulus int not null;

Query OK, 0 rows affected (0.05 sec)

Records: 0 Duplicates: 0 Warnings: 0

mysql> alter table employee

-> alter stimulus set default 0;

Query OK, 0 rows affected (0.02 sec)

Records: 0 Duplicates: 0 Warnings: 0

mysql>

mysql> alter table employee

-> add column dependents int not null default 0;

Query OK, 0 rows affected (0.03 sec)

Records: 0 Duplicates: 0 Warnings: 0

mysql>

mysql> alter table employee add column encrypted\_stimulus int not null default 0;

Query OK, 0 rows affected (0.03 sec)

Records: 0 Duplicates: 0 Warnings: 0

mysql> alter table employee add column encrypted\_dependents int not null default 0;

Query OK, 0 rows affected (0.03 sec)

Records: 0 Duplicates: 0 Warnings: 0

mysql> describe employee;

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

| Field | Type | Null | Key | Default | Extra |

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

| Fname | varchar(15) | NO | | | |

| Minit | char(1) | YES | | NULL | |

| Lname | varchar(15) | NO | | | |

| Ssn | char(9) | NO | PRI | | |

| Bdate | date | YES | | NULL | |

| Address | varchar(30) | YES | | NULL | |

| Sex | char(1) | YES | | NULL | |

| Salary | decimal(10,2) | YES | | NULL | |

| Super\_ssn | char(9) | YES | | NULL | |

| Dno | int | NO | | 0 | |

| Encrypted\_salary | varchar(50) | YES | | NULL | |

| Salary\_inx | int | YES | | NULL | |

| stimulus | int | NO | | 0 | |

| dependents | int | NO | | 0 | |

| encrypted\_stimulus | int | NO | | 0 | |

| encrypted\_dependents | int | NO | | 0 | |

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

16 rows in set (0.01 sec)

We then insert the values of ‘stimulus’ and ‘dependents’ to the employees.

mysql> update employee set stimulus = 1200, dependents = 4 where Minit = 'T';

Query OK, 1 row affected (0.00 sec)

Rows matched: 1 Changed: 1 Warnings: 0

mysql> update employee set stimulus = 800, dependents = 1 where Minit = 'A';

Query OK, 1 row affected (0.00 sec)

Rows matched: 1 Changed: 1 Warnings: 0

mysql> update employee set stimulus = 1600, dependents = 3 where Minit = 'K';

Query OK, 1 row affected (0.02 sec)

Rows matched: 1 Changed: 1 Warnings: 0

mysql> update employee set stimulus = 1300, dependents = 5 where Minit = 'E';

Query OK, 1 row affected (0.01 sec)

Rows matched: 1 Changed: 1 Warnings: 0

mysql> update employee set stimulus = 1500, dependents = 3 where Minit = 'S';

Query OK, 1 row affected (0.00 sec)

Rows matched: 1 Changed: 1 Warnings: 0

mysql> update employee set stimulus = 800, dependents = 2 where Minit = 'V';

Query OK, 1 row affected (0.00 sec)

Rows matched: 1 Changed: 1 Warnings: 0

mysql> update employee set stimulus = 800, dependents = 3 where Minit = 'J';

Query OK, 1 row affected (0.01 sec)

Rows matched: 1 Changed: 1 Warnings: 0

mysql> select \* from employee;

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

| Fname | … | stimulus | dependents | encrypted\_stimulus | encrypted\_dependents |

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

| John | B | 1400 | 2 | 0 | 0 |

| Franklin | T | 1200 | 4 | 0 | 0 |

| Joyce | A | 800 | 1 | 0 | 0 |

| Ramesh | K | 1600 | 3 | 0 | 0 |

| James | E | 1300 | 5 | 0 | 0 |

| Jennifer | S | 1500 | 3 | 0 | 0 |

| Ahmad | V | 800 | 2 | 0 | 0 |

| Alicia | J | 800 | 3 | 0 | 0 |

8 rows in set (0.00 sec)

Next, we bring up the RSA online calculator to encrypt the values of ‘stimulus’ and ‘dependents’ into ‘encrypted\_stimulus’ and ‘encrypted\_dependents’ of employees. Set up the parameters for RSA encryption.

**RSA Encryption**

**Use the online calculator [1] to encrypt values.**

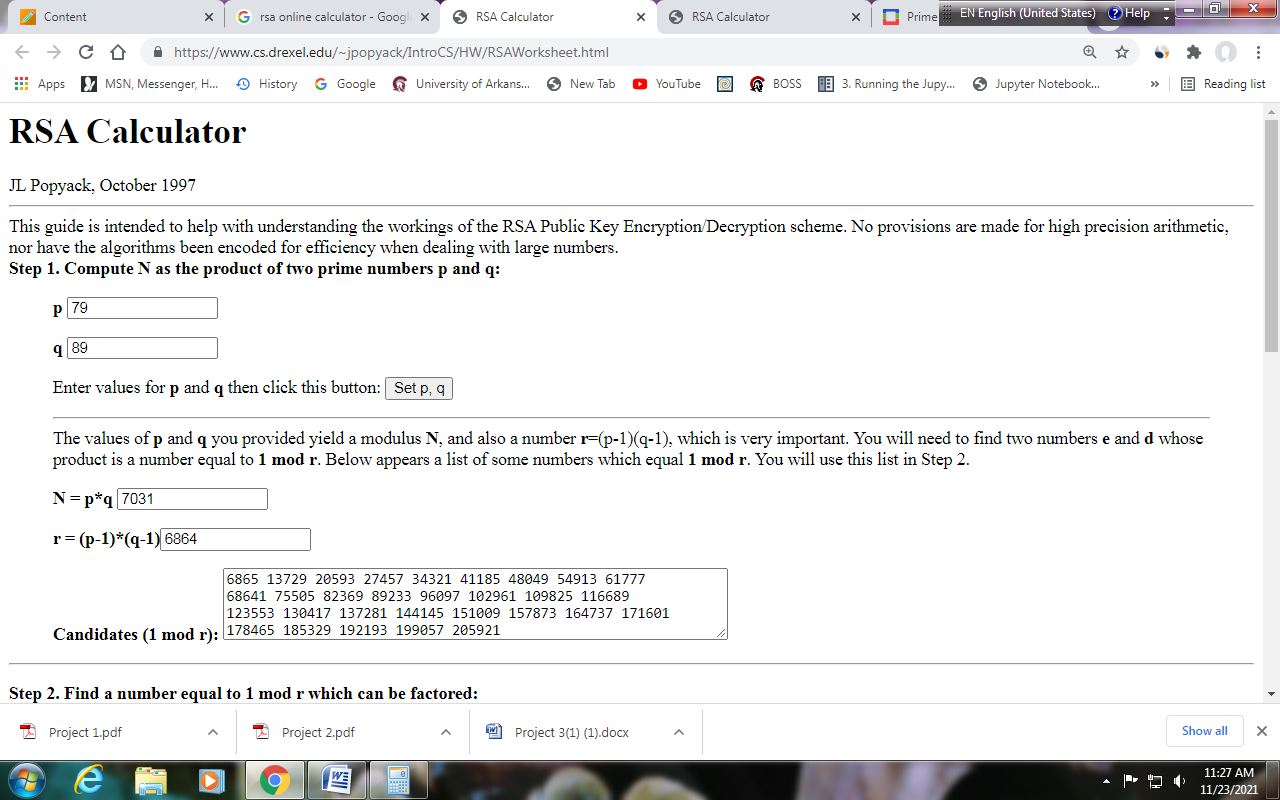
p = 79 and q = 89

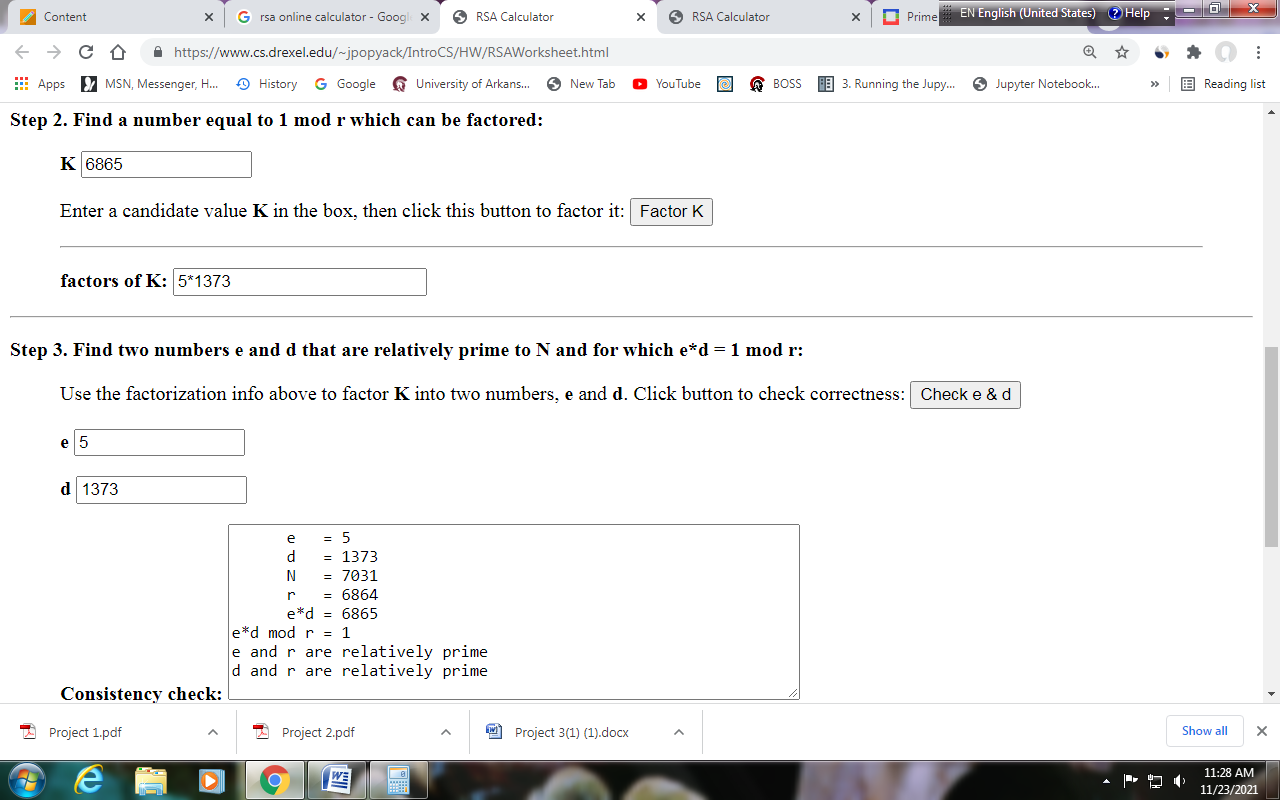
N = p \* q = 7031

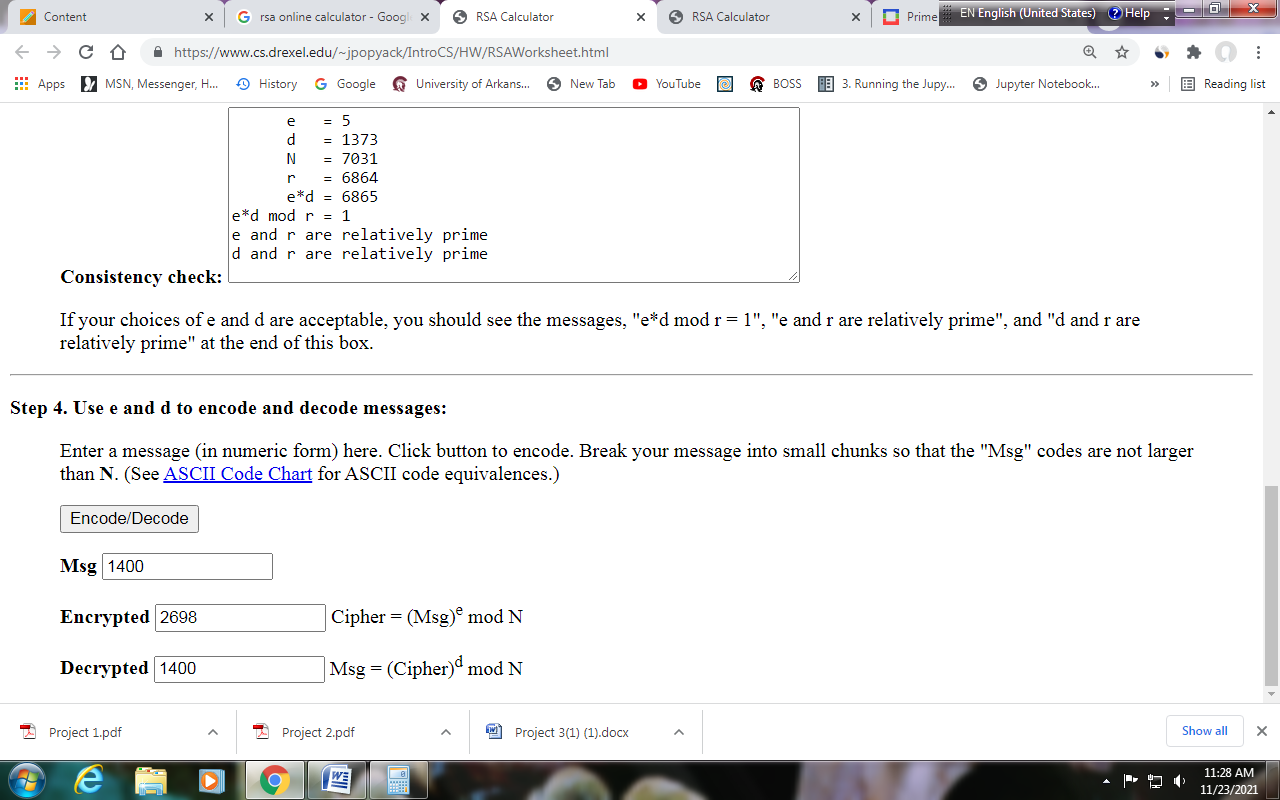
R = (p-1) \* (q-1) = 6864

e = 5

d = 1373







In this step, the encrypted stimulus and encrypted dependents have been pre-computed. You just cut and paste the following commands to populate the values to the employee table.

mysql> update employee set encrypted\_stimulus = 4805, encrypted\_dependents = 243 where Minit = 'J';

Query OK, 1 row affected (0.00 sec)

Rows matched: 1 Changed: 1 Warnings: 0

mysql> update employee set encrypted\_stimulus = 4805, encrypted\_dependents = 32 where Minit = 'V';

Query OK, 1 row affected (0.00 sec)

Rows matched: 1 Changed: 1 Warnings: 0

mysql> update employee set encrypted\_stimulus = 2685, encrypted\_dependents = 243 where Minit = 'S';

Query OK, 1 row affected (0.00 sec)

Rows matched: 1 Changed: 1 Warnings: 0

mysql> update employee set encrypted\_stimulus = 6370, encrypted\_dependents = 3125 where Minit = 'E';

Query OK, 1 row affected (0.00 sec)

Rows matched: 1 Changed: 1 Warnings: 0

mysql> update employee set encrypted\_stimulus = 6109, encrypted\_dependents = 243 where Minit = 'K';

Query OK, 1 row affected (0.02 sec)

Rows matched: 1 Changed: 1 Warnings: 0

mysql> update employee set encrypted\_stimulus = 4805, encrypted\_dependents = 1 where Minit = 'A';

Query OK, 1 row affected (0.00 sec)

Rows matched: 1 Changed: 1 Warnings: 0

mysql> update employee set encrypted\_stimulus = 2871, encrypted\_dependents = 1024 where Minit = 'T';

Query OK, 1 row affected (0.01 sec)

Rows matched: 1 Changed: 1 Warnings: 0

mysql> update employee set encrypted\_stimulus = 2698, encrypted\_dependents = 32 where Minit = 'B';

Query OK, 1 row affected (0.00 sec)

Rows matched: 1 Changed: 1 Warnings: 0

mysql> select Fname, Stimulus, Dependents, Encrypted\_stimulus, Encrypted\_dependents from employee;

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

| Fname | Stimulus | Dependents | Encrypted\_stimulus | Encrypted\_dependents |

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

| John | 1400 | 2 | 2698 | 32 |

| Franklin | 1200 | 4 | 2871 | 1024 |

| Joyce | 800 | 1 | 4805 | 1 |

| Ramesh | 1600 | 3 | 6109 | 243 |

| James | 1300 | 5 | 6370 | 3125 |

| Jennifer | 1500 | 3 | 2685 | 243 |

| Ahmad | 800 | 2 | 4805 | 32 |

| Alicia | 800 | 3 | 4805 | 243 |

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

8 rows in set (0.00 sec)

You are now ready to answer the following questions against the encrypted database COMPANY. Please use the tool in [2] to help decrypt encrypted values in RSA/decryption.

**Questions**

**Please screen dump the outputs.**

1. (25 Points) select Fname, Minit, Lname, (stimulus \* dependents) from employee;
2. (75 Points) select Fname, Minit, Lname, (encrypted\_stimulus \* encrypted\_dependents) from employee; and **MANUALLY** decrypt the values of (encrypted\_stimulus \* encrypted\_dependents) using RSA/decryption with the same parameters used for encryption [2], you should be able to get the same values to Question 1.

**References**

1. RSA Calculator, <https://www.cs.drexel.edu/~jpopyack/IntroCS/HW/RSAWorksheet.html>
2. RSA Express Encryption/Decryption Calculator, <https://www.cs.drexel.edu/~jpopyack/Courses/CSP/Fa17/notes/10.1_Cryptography/RSA_Express_EncryptDecrypt_v2.html>