**Improved RSA Algorithm**

**Group members:**

1. Name: Muhammad Awais Siddique (3016)
2. Jibran Maqbool (3246)

The goal of this research is to speed up the implementation of the RSA method during data exchange over the network by presenting a modified version of the technique in a new algorithmic idea.

This incorporates the use of a third prime integer in the architectural design and an improved version of the RSA algorithm to create a modulus n that is difficult for intruders to decompose.

**Improved RSA Algorithm**

An algorithm based on a modified RSA cryptosystem is created. Taking into account the following algorithmic presumptions: p, q, and r are all prime numbers.

* The common modulus is n.
* The public key is e.
* The private key is d.
* M is for message.

**Proposed Method:**

* Select the random values p, q, and r.
* Calculate n=pqr.
* Calculate Ø (n) = (p-1) (q-1) (r-1).
* Calculate e such that gcd (e, Ø(n))=1 and 1<e<Ø(n).
* Encrypt the message M where M<n and encrypt with public key  
  e such that C=M e mod n.
* Calculate private key d = ℮ -1 (mod Ø (n)).
* Decrypt the message M such that M=C d mod n.

**Offline Storage:**

P, Q, and values are included in the first table (N). The values for e, d, and r are in the second table. Because we employ the third prime, r, anybody attempting to predict the value of the modulus n by hacking the database table would fail because n relies on all three prime integers, n=p\*q\*r. As a result, concurrently hacking both tables are difficult.

**Advantages:**

1. Three factors, p, q, and r, determine how strong a huge prime number is. In contrast to the current RSA technique, it is challenging to divide a huge prime number into three smaller ones.
2. Before the algorithm begins, p, q, d, and e are stored in two database tables. Instead of using the original key, we swap the index value that corresponds to the values of e and d from the database table (e, d). Security is thus improved.
3. Keys are offline saved before the procedure begins in the suggested approach. As a result, the procedure moved forward more quickly than the original RSA approach did.

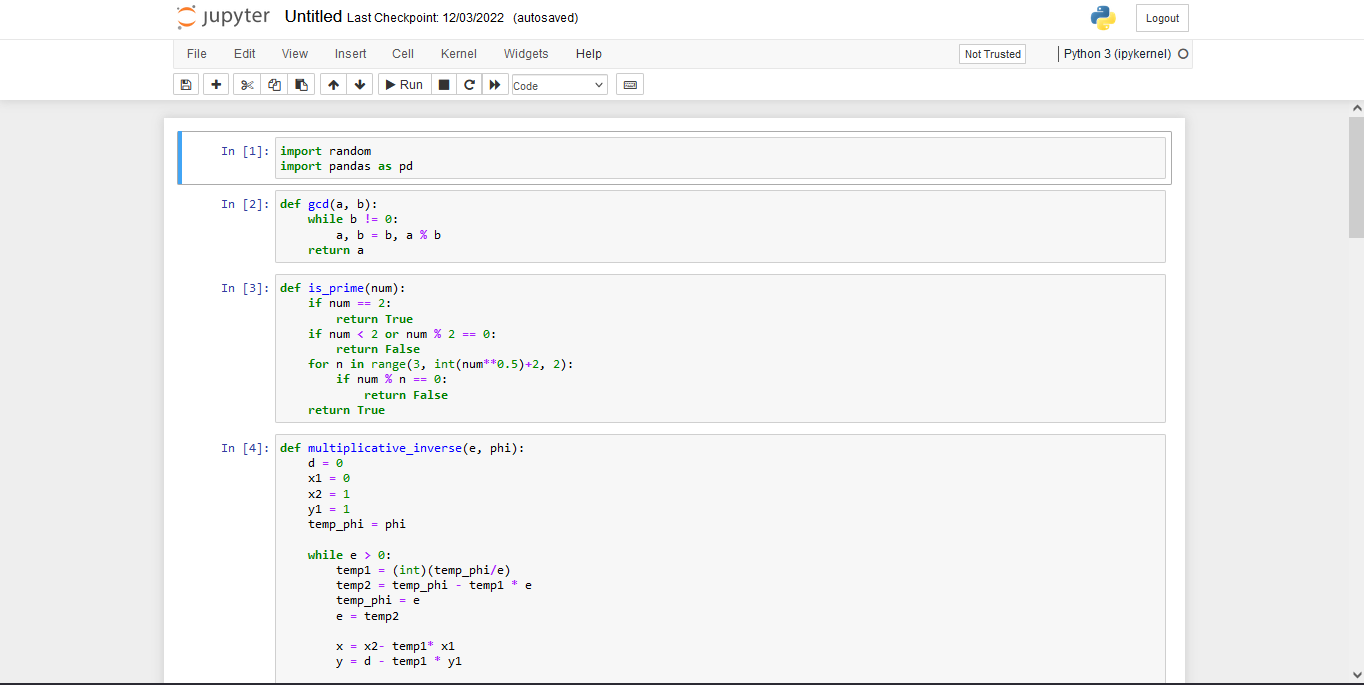
**Future Benefits:**

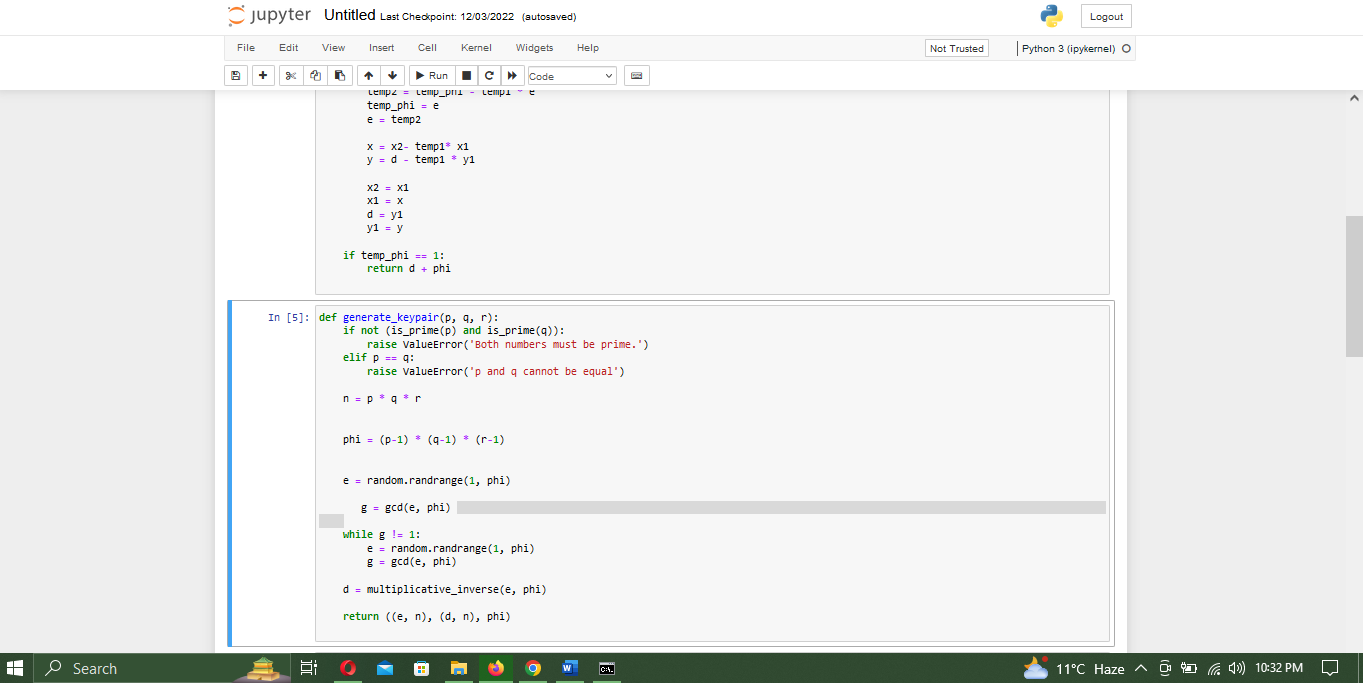
When used in networks and cloud computing environments, this strategy will increase security and is dependable.

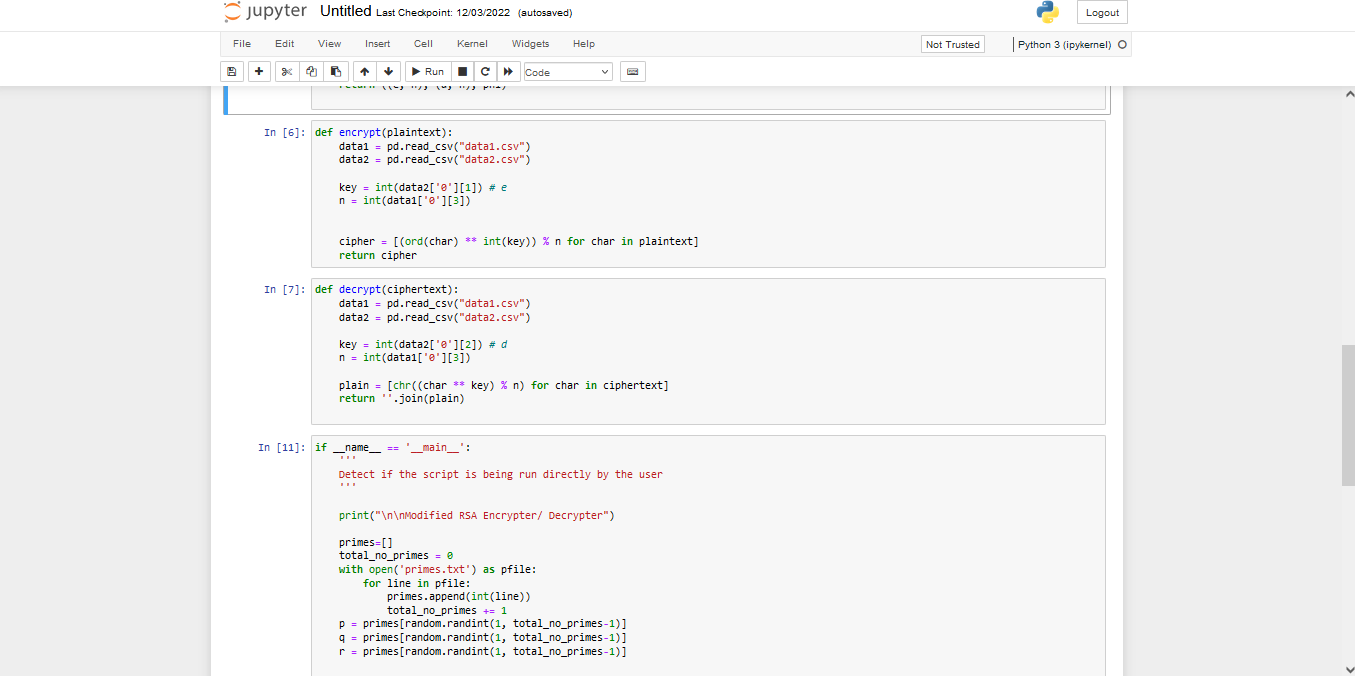
The current RSA algorithm may be enhanced in the future to increase efficiency and security by including certain security ideas.

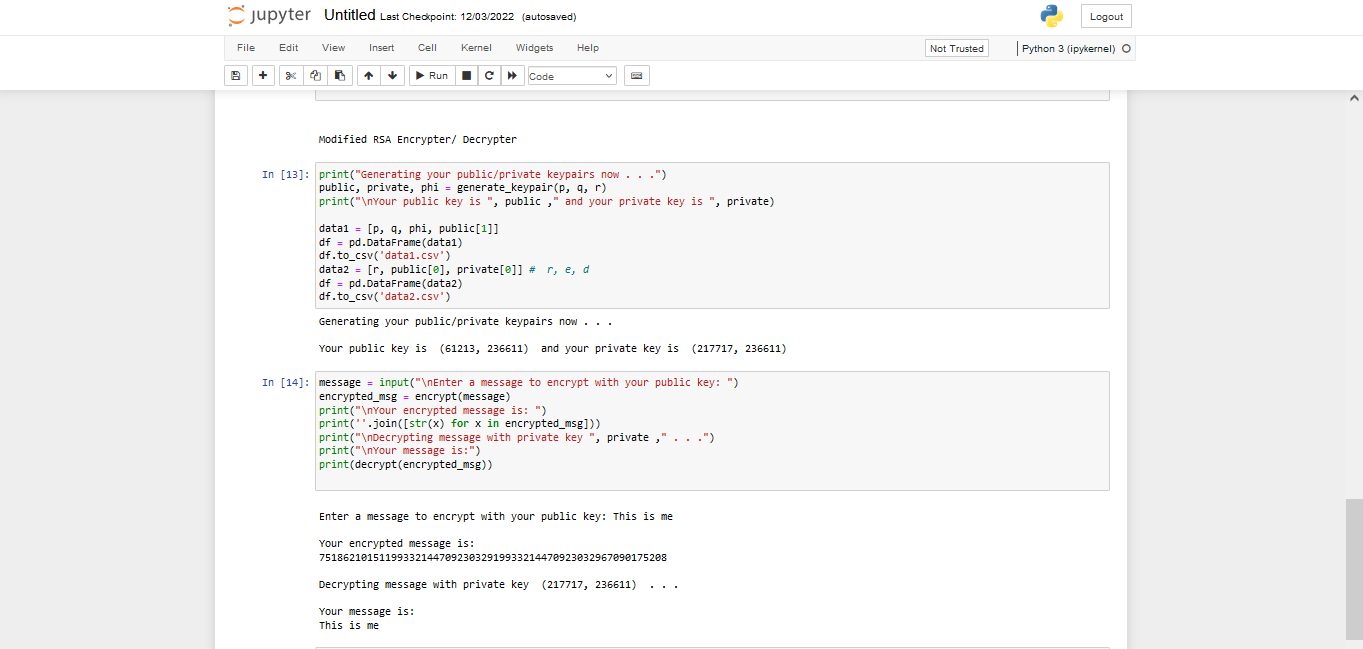
**Coding:**

All coding is done in Python languages using Jupyter notebook.









The End