VNR Vignana Jyothi Institute of Engineering and Technology (Affiliated to J.N.T.U, Hyderabad) Bachupally(v), Hyderabad, Telangana, India.

SECURE COMMUNICATION USING RSA ENCRYPTION

A course project submitted in complete requirements for the award of the degree of

BACHELOR OF TECHNOLOGY

IN

COMPUTER SCIENCE AND ENGINEERING & BUSINESS SYSTEM

Submitted by

A. Harshita (21071A3202)
B.V. Vimal (21071A309)
G. Tejaswi (21071A3219)
M. Sravanth (21071A3245)
P.L.S. Deepika(21071A3255)

Under the guidance

of

Dr. G. S. Ramesh

Assistant Professor

Dept. of Computer Science and Engineering

VNR Vignana Jyothi Institute of Engineering and Technology

(Affiliated to J.N.T.U, Hyderabad)
Bachupally(v), Hyderabad, Telangana, India.

CERTIFICATE

This is to certify that **A.Harshita(21071A3202) B.V.Vimal(21071A3209) G.Tejaswi(21071A3219) M.Sravanth(21071A3245) P.L.S.Deepika(21071A3255)** have completed their course project work at CSE Department of VNR VJIET, Hyderabad entitled " **SECURE COMMUNICATION USING RSA ENCRYPTION PROJECT**" in complete fulfilment of the requirements for the award of B.Tech degree during the academic year 2022-2023. This work is carried out under my supervision and has not been submitted to any other University/Institute for award of any degree/diploma.

Dr. G. S. Ramesh

Assistant Professor

CSE Department

VNRVJIET

Dr. S. Nagini

Professor and Head

CSE & CSBS Department

VNRVJIET

DECLARATION

This is to certify that our project report titled “**SECURE COMMUNICATION USING RSA ENCRYPTION PROJECT**" submitted to Vallurupalli Nageswara Rao Institute of Engineering and Technology in complete fulfilment of requirement for the award of Bachelor of Technology in Computer Science and Engineering is a bonafide report to the work carried out by us under the guidance and supervision of Dr. G. S. Ramesh, Assistant Professor, Department of Computer Science and Engineering, Vallurupalli Nageswara Rao Institute of Engineering and Technology. To the best of our knowledge, this has not been submitted in any form to other university or institution for the award of any degree or diploma.

A.Harshita	**BV.Vimal**	**G.Tejaswi**	**M.Sravanth**	**P.L.S.Deepika**
21071A3202	21071A3209	21071A3219	21071A3245	21071A3255
CSBS	CSBS	CSBS	CSBS	CSBS

ACKNOWLEDGEMENT

Over a span of three and a half years, VNRVJIET has helped us transform ourselves from mere amateurs in the field of Computer Science into skilled engineers capable of handling any given situation in real time. We are highly indebted to the institute for everything that it has given us. We would like to express our gratitude towards the principal of our institute, **Dr. Challa Dhanunjaya Naidu** and the Head of the Computer Science & Engineering Department, **Dr. S. Nagini** for their kind co- operation and encouragement which helped us complete the project in the stipulated time. Although we have spent a lot of time and put in a lot of effort into this project, it would not have been possible without the motivating support and help of our project guide **Dr. G. S. Ramesh**. We thank him for his guidance, constant supervision and for providing necessary information to complete this project. Our thanks and appreciations also go to all the faculty members, staff members of VNRVJIET, and all our friends who have helped us put this project together.

ABSTRACT

Our project presents an exploration of secure communication through the implementation of the RSA encryption algorithm. The code, written in Python, generates prime numbers, establishes public and private keys, and demonstrates the encryption and decryption processes for sender and receiver messages. Through this endeavour, the project aims to provide a practical understanding of cryptographic techniques, modular arithmetic, and the principles behind secure message exchange in a public-key encryption framework. Our project encompasses key generation, encryption, and decryption mechanisms, serving as a valuable resource for comprehending and applying secure communication protocols.

INDEX

INTRODUCTION

In today's interconnected digital landscape, ensuring the authenticity, integrity, and non-repudiation of electronic documents and transactions is paramount. This imperative has given rise to cryptographic techniques like digital signatures, bolstered by the power of hashing algorithms. At the heart of this innovation lies a blend of mathematics, computer science, and information security, offering a robust solution to age-old challenges of secure communication.

A digital signature is akin to an electronic fingerprint. It serves as a cryptographic tool that binds a person's identity to a piece of data, ensuring that the data originated from the claimed sender and remains unaltered in transit. Unlike traditional handwritten signatures, digital signatures are tamper-evident, meaning any alteration post-signing invalidates the signature, alerting both parties to potential foul play.

Central to the efficacy of digital signatures is the concept of hashing. Hashing algorithms take input data (often of arbitrary size) and produce a fixed-size string of characters, typically a hash value or digest. This process is one-way; while it's computationally easy to generate a hash from data, deducing the original data from its hash is virtually impossible. Thus, any minor change in the input data produces a vastly different hash, making it an ideal tool for data integrity verification.

In an increasingly connected world, the need for secure transmission of information has become paramount. Cryptography plays a pivotal role in achieving this, and the RSA algorithm stands out as a widely used and robust method for secure data exchange.In an increasingly connected world, the need for secure transmission of information has become paramount. Cryptography plays a pivotal role in achieving this, and the RSA algorithm stands out as a widely used and robust method for secure data exchange.

EXISTING SYSTEMS

Secure communication using RSA encryption is a foundational aspect of many modern systems and applications, especially those that prioritise confidentiality, integrity, authentication, and non-repudiation. Here are some existing systems and scenarios where RSA encryption plays a pivotal role:

- **SSL/TLS for Web Security:**

Whenever you access a website using HTTPS (HyperText Transfer Protocol Secure), SSL/TLS (Secure Sockets Layer/Transport Layer Security) protocols come into play. RSA is often used in the initial phase of the SSL/TLS handshake to establish a secure connection between the client (e.g., web browser) and the server (e.g., web server).

- **Digital Certificates and Public Key Infrastructure (PKI):**

RSA is instrumental in PKI, a framework that manages digital certificates and public-key encryption. Certificate Authorities (CAs) use RSA to create and sign digital certificates, which attest to the authenticity of entities like websites, servers, or individuals.

- **SSH (Secure Shell) Connections:**

RSA is one of the algorithms supported by SSH for secure remote login and other secure network services over an insecure network.

- **VPN (Virtual Private Network):**

Many VPN solutions leverage RSA for key exchange and authentication purposes, ensuring secure and private communication over public networks.

- **Secure Email (e.g., PGP and S/MIME):**

  Encryption tools like PGP (Pretty Good Privacy) and S/MIME (Secure/Multipurpose Internet Mail Extensions) utilize RSA for encrypting email messages and attachments, ensuring only the intended recipient can decrypt and read them.

- **Digital Signatures in Documents and Software:**

RSA-based digital signatures provide a means to verify the authenticity and integrity of documents, software packages, and updates. This ensures that the content hasn't been tampered with and originates from a trusted source.

- **Payment Gateways and Digital Transactions:**

RSA encryption secures online financial transactions, ensuring that sensitive payment information, like credit card numbers, remains confidential during transmission.

- **IoT (Internet of Things) Security:**

As IoT devices proliferate, ensuring their communication remains secure is crucial. RSA encryption can be used in IoT ecosystems to establish secure channels between devices, gateways, and servers.

- **Database Security:**

Some database systems employ RSA encryption to protect sensitive data, ensuring that even if unauthorised individuals gain access to the database, the encrypted data remains unintelligible without the appropriate decryption key.

PROPOSED SYSTEMS

When envisioning new systems for secure communication using RSA encryption, it's essential to consider emerging challenges, technologies, and application domains. Here are some proposed systems that could benefit from RSA encryption:

- **Decentralised Communication Platforms:**

With the rise of decentralised technologies like blockchain, there's potential for creating decentralised communication platforms where users can securely exchange messages, voice calls, or even video calls. RSA encryption could be integrated to ensure end-to-end encryption and user authentication.

- **Healthcare Data Exchange Platforms:**

Given the sensitivity of healthcare data, there's a need for secure platforms that allow healthcare providers, laboratories, and patients to exchange medical records, test results, and other health-related information securely. RSA encryption can ensure the confidentiality and integrity of this data.

- **Secure Voting Systems:**

To address the challenges of electronic voting, a secure voting system could be designed using RSA encryption to ensure that votes remain confidential, tamper-proof, and verifiable.

- **Smart Grid Communication:**

In the realm of smart grids where devices communicate to manage and optimise energy consumption, RSA encryption can secure these communications, ensuring that commands, data, and control signals are not intercepted or manipulated.

- **Secure Messaging Apps for Enterprises:**

Tailored for businesses, these apps could offer functionalities like secure file sharing, collaboration tools, and communication channels—all encrypted using RSA, ensuring that sensitive corporate information remains confidential.

- **Supply Chain and Logistics Security:**

Given the complexities of global supply chains, a system that employs RSA encryption can secure communications between various stakeholders, ensuring that product details, shipment information, and other critical data remain confidential and unaltered.

- **Secure Remote Learning Platforms:**

As remote and online learning becomes more prevalent, a platform could be developed that allows educators and students to interact, share resources, and collaborate securely. RSA encryption would ensure that educational content and communication channels are protected.

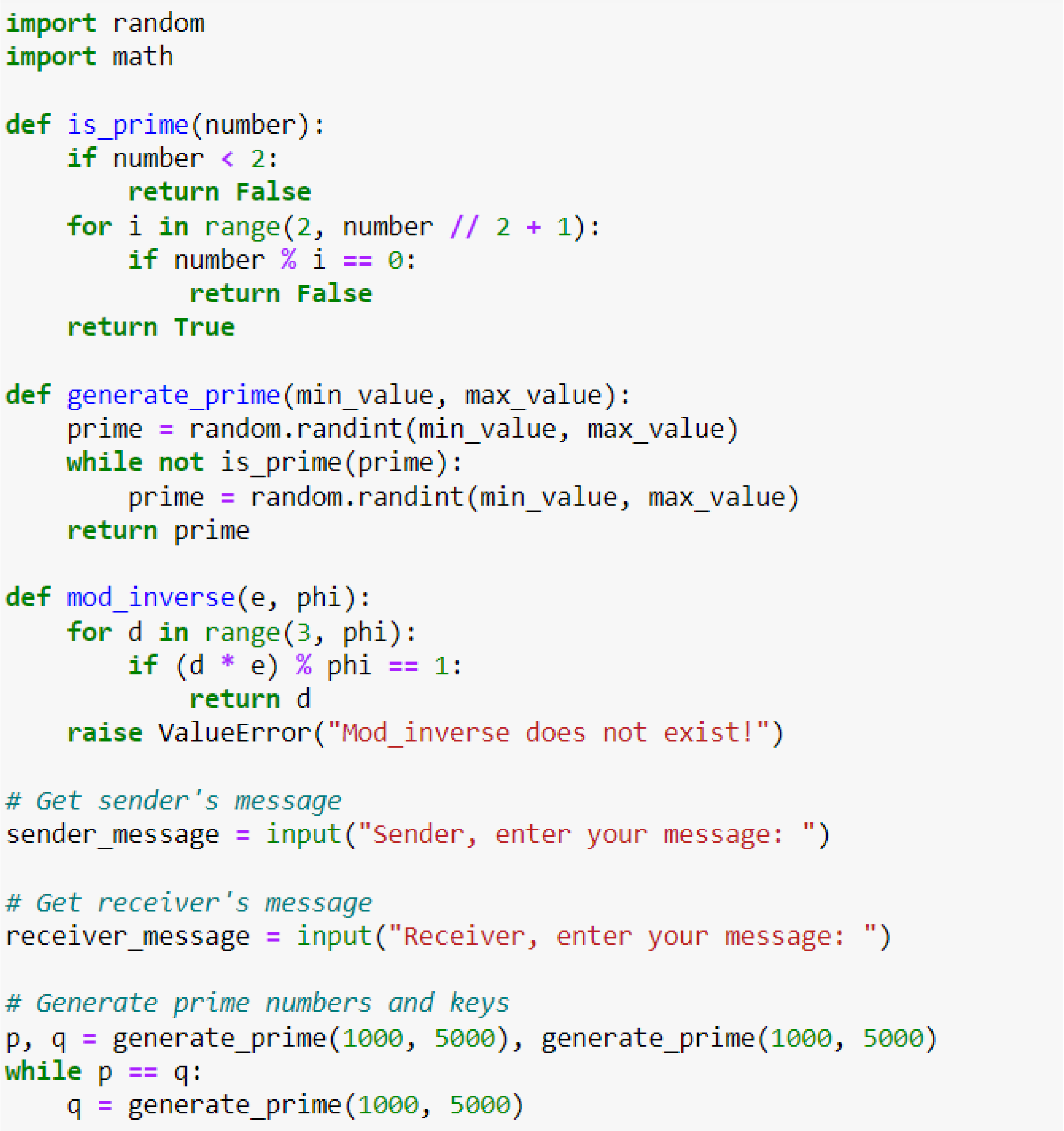
- **Secure Cloud Storage and Backup Solutions:**

With the increasing reliance on cloud storage, there's a need for solutions that offer secure storage and backup services. RSA encryption can be integrated into these solutions to ensure that data stored in the cloud remains encrypted and secure from unauthorised access.

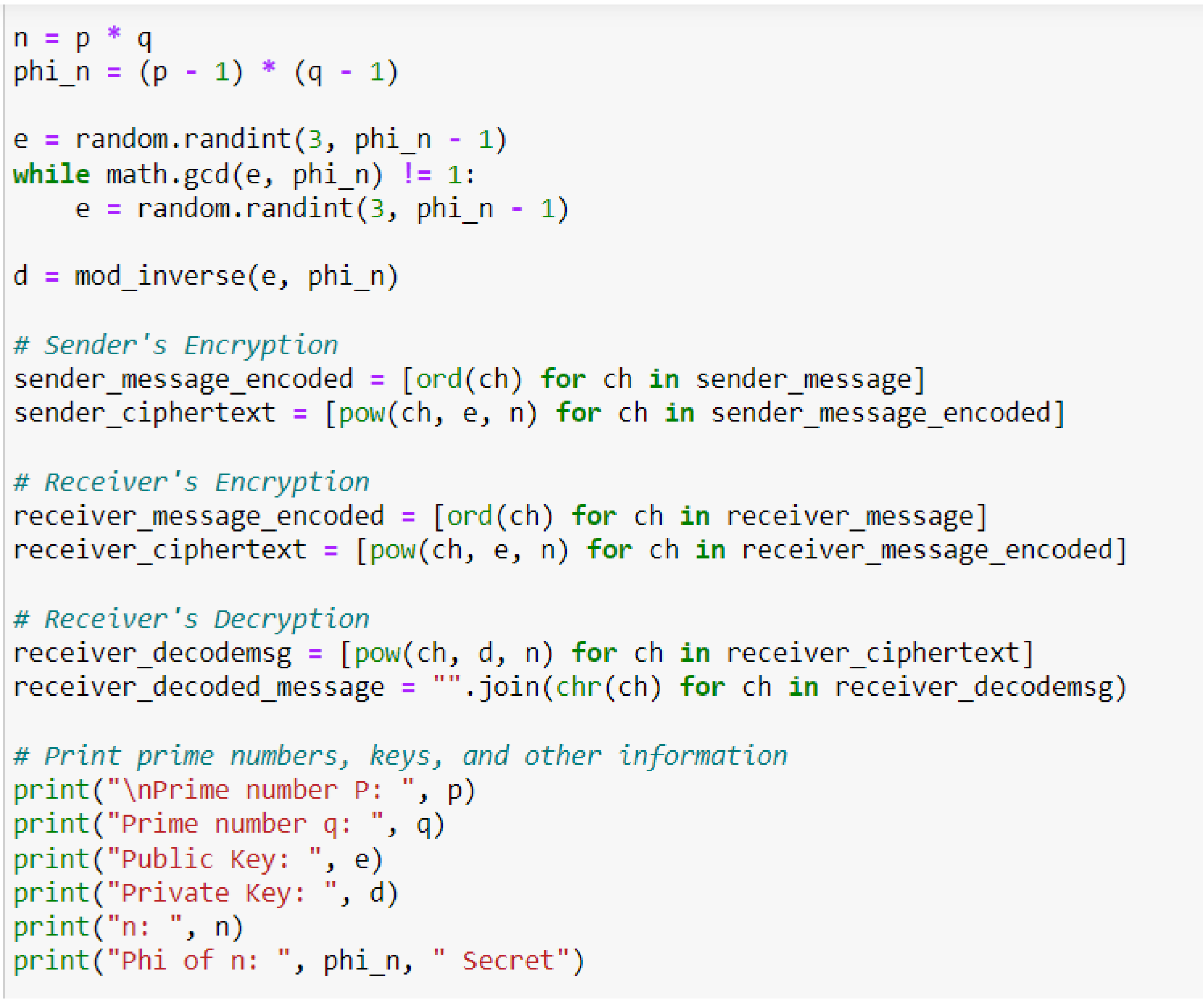
- **Personal Data Vaults:**

Given growing concerns about personal data privacy, a personal data vault system could be developed where individuals store and manage their sensitive personal information. RSA encryption would be pivotal in ensuring the security and confidentiality of this data.

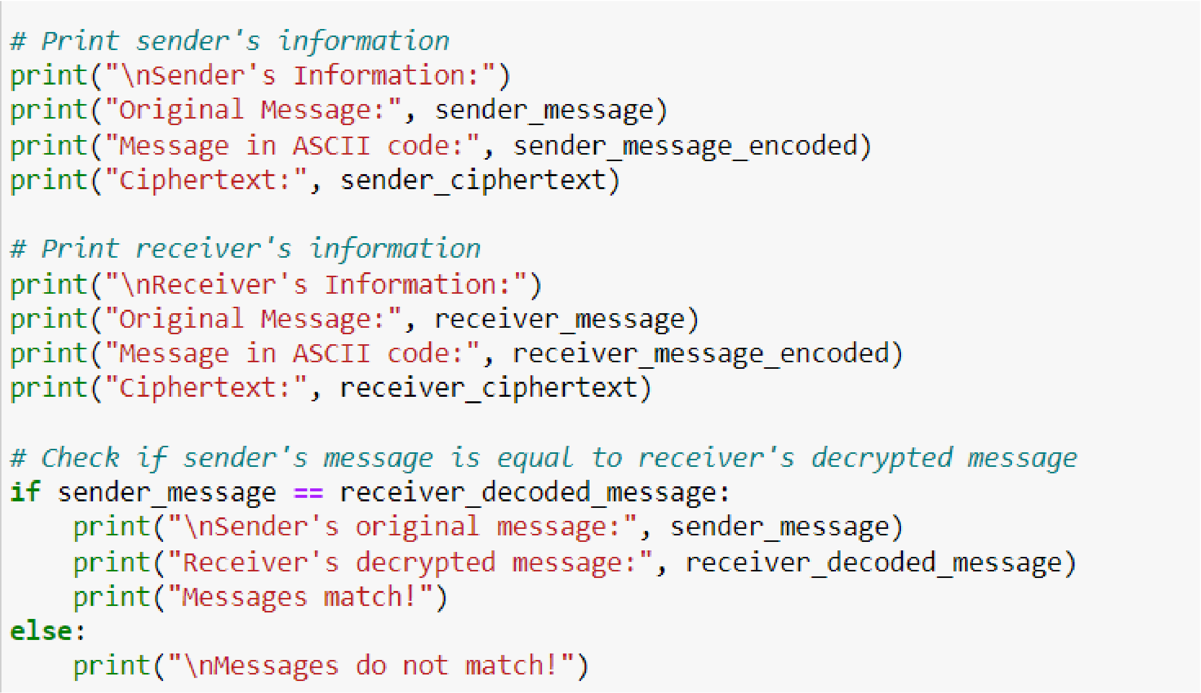
IMPLEMENTATION



```python
import random
import math

def is_prime(number):
    if number < 2:
        return False
    for i in range(2, number // 2 + 1):
        if number % i == 0:
            return False
    return True

def generate_prime(min_value, max_value):
    prime = random.randint(min_value, max_value)
    while not is_prime(prime):
        prime = random.randint(min_value, max_value)
    return prime

def mod_inverse(e, phi):
    for d in range(3, phi):
        if (d * e) % phi == 1:
            return d
    raise ValueError("Mod_inverse does not exist!")

# Get sender's message
sender_message = input("Sender, enter your message: ")

# Get receiver's message
receiver_message = input("Receiver, enter your message: ")

# Generate prime numbers and keys
p, q = generate_prime(1000, 5000), generate_prime(1000, 5000)
while p == q:
    q = generate_prime(1000, 5000)
```

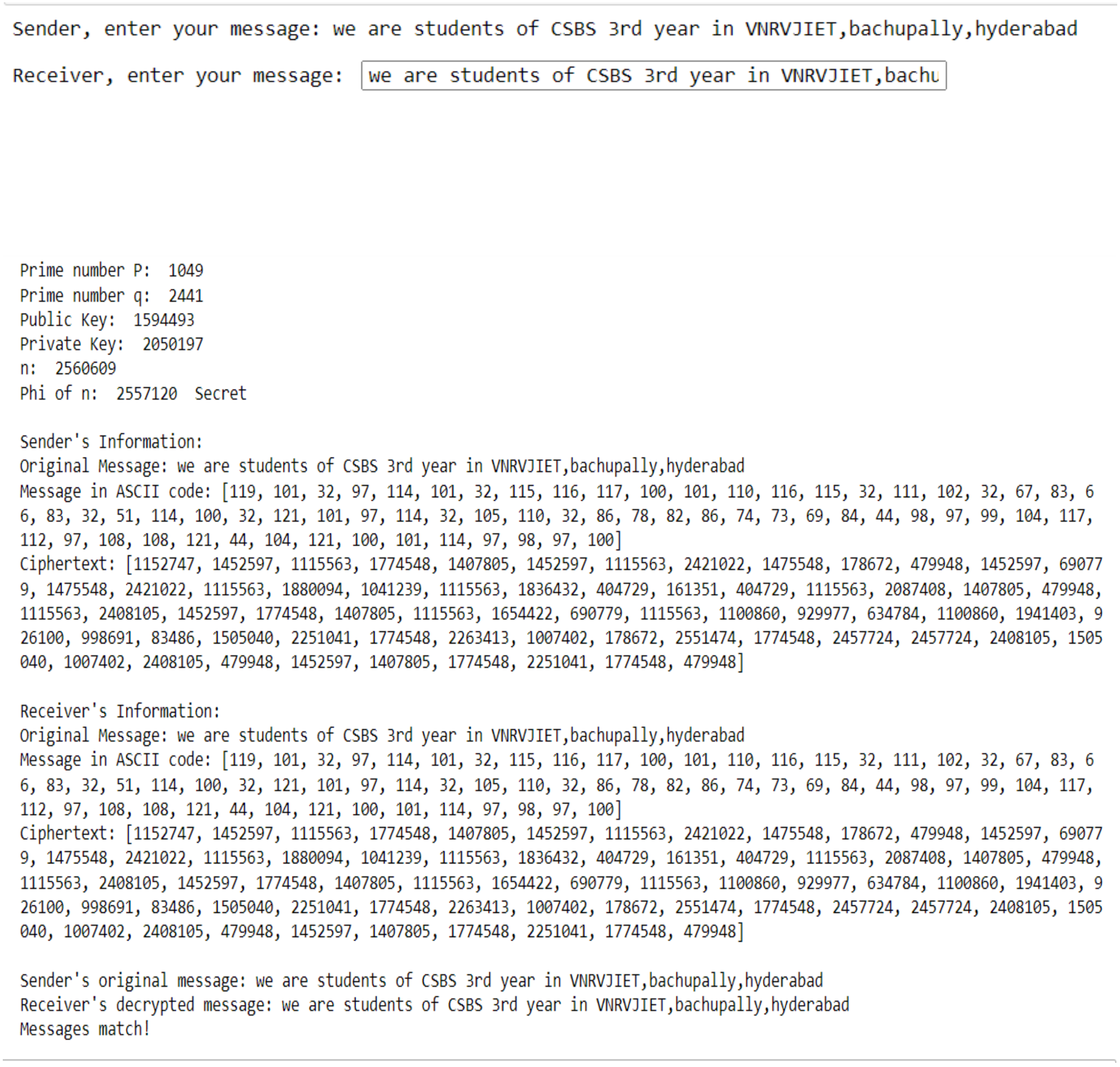


```
n = p * q
phi_n = (p - 1) * (q - 1)

e = random.randint(3, phi_n - 1)
while math.gcd(e, phi_n) != 1:
    e = random.randint(3, phi_n - 1)

d = mod_inverse(e, phi_n)

# Sender's Encryption
sender_message_encoded = [ord(ch) for ch in sender_message]
sender_ciphertext = [pow(ch, e, n) for ch in sender_message_encoded]

# Receiver's Encryption
receiver_message_encoded = [ord(ch) for ch in receiver_message]
receiver_ciphertext = [pow(ch, e, n) for ch in receiver_message_encoded]

# Receiver's Decryption
receiver_decodemsg = [pow(ch, d, n) for ch in receiver_ciphertext]
receiver_decoded_message = "".join(chr(ch) for ch in receiver_decodemsg)

# Print prime numbers, keys, and other information
print("\nPrime number P: ", p)
print("Prime number q: ", q)
print("Public Key: ", e)
print("Private Key: ", d)
print("n: ", n)
print("Phi of n: ", phi_n, " Secret")
```



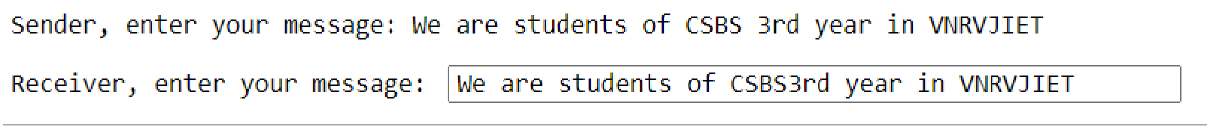
```
# Print sender's information
print("\nSender's Information:")
print("Original Message:", sender_message)
print("Message in ASCII code:", sender_message_encoded)
print("Ciphertext:", sender_ciphertext)

# Print receiver's information
print("\nReceiver's Information:")
print("Original Message:", receiver_message)
print("Message in ASCII code:", receiver_message_encoded)
print("Ciphertext:", receiver_ciphertext)

# Check if sender's message is equal to receiver's decrypted message
if sender_message == receiver_decoded_message:
    print("\nSender's original message:", sender_message)
    print("Receiver's decrypted message:", receiver_decoded_message)
    print("Messages match!")
else:
    print("\nMessages do not match!")
```

OUTPUT

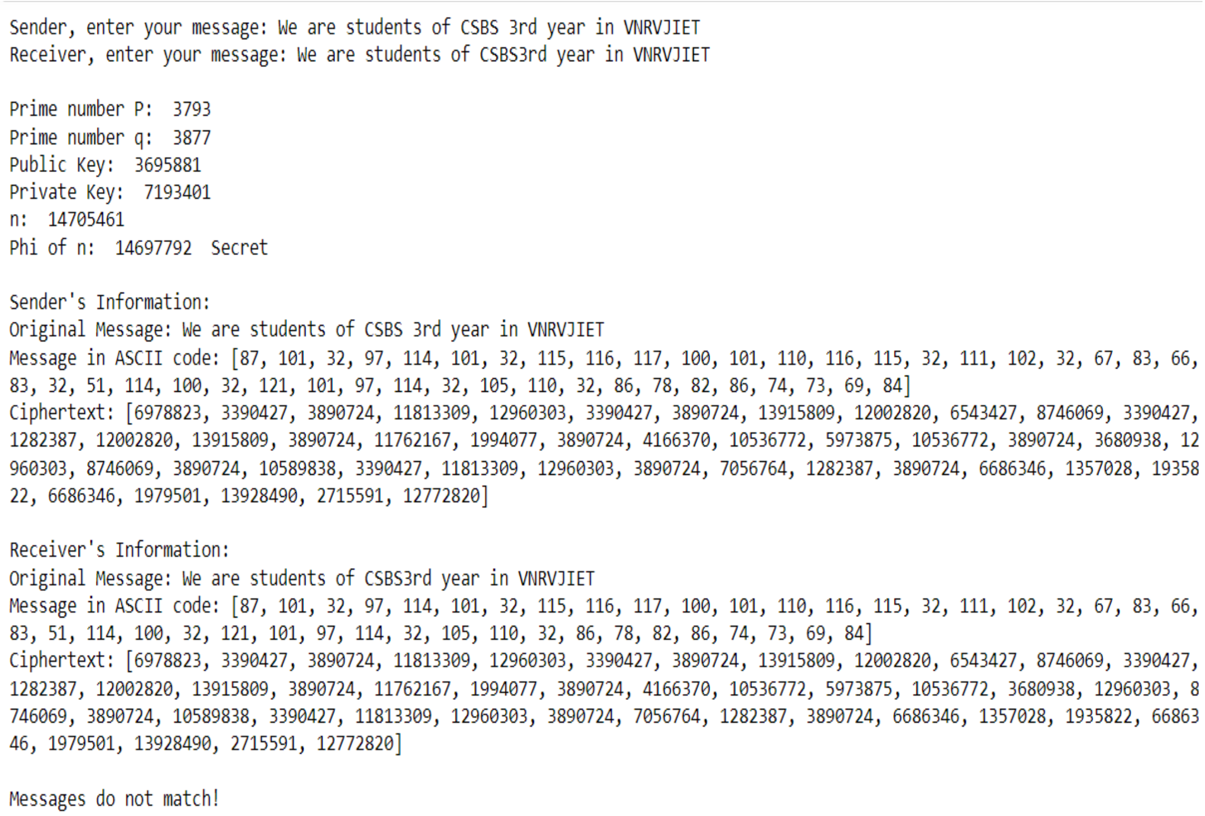


```
Sender, enter your message: we are students of CSBS 3rd year in VNRVJIET,bachupally,hyderabad

Receiver, enter your message: we are students of CSBS 3rd year in VNRVJIET,bachu
```

```
Prime number P:  1049
Prime number q:  2441
Public Key:  1594493
Private Key:  2050197
n:  2560609
Phi of n:  2557120  Secret

Sender's Information:
Original Message: we are students of CSBS 3rd year in VNRVJIET,bachupally,hyderabad
Message in ASCII code: [119, 101, 32, 97, 114, 101, 32, 115, 116, 117, 100, 101, 110, 116, 115, 32, 111, 102, 32, 67, 83, 6
6, 83, 32, 51, 114, 100, 32, 121, 101, 97, 114, 32, 105, 110, 32, 86, 78, 82, 86, 74, 73, 69, 84, 44, 98, 97, 99, 104, 117,
112, 97, 108, 108, 121, 44, 104, 121, 100, 101, 114, 97, 98, 97, 100]
Ciphertext: [1152747, 1452597, 1115563, 1774548, 1407805, 1452597, 1115563, 2421022, 1475548, 178672, 479948, 1452597, 69077
9, 1475548, 2421022, 1115563, 1880094, 1041239, 1115563, 1836432, 404729, 161351, 404729, 1115563, 2087408, 1407805, 479948,
1115563, 2408105, 1452597, 1774548, 1407805, 1115563, 1654422, 690779, 1115563, 1100860, 929977, 634784, 1100860, 1941403, 9
26100, 998691, 83486, 1505040, 2251041, 1774548, 2263413, 1007402, 178672, 2551474, 1774548, 2457724, 2457724, 2408105, 1505
040, 1007402, 2408105, 479948, 1452597, 1407805, 1774548, 2251041, 1774548, 479948]

Receiver's Information:
Original Message: we are students of CSBS 3rd year in VNRVJIET,bachupally,hyderabad
Message in ASCII code: [119, 101, 32, 97, 114, 101, 32, 115, 116, 117, 100, 101, 110, 116, 115, 32, 111, 102, 32, 67, 83, 6
6, 83, 32, 51, 114, 100, 32, 121, 101, 97, 114, 32, 105, 110, 32, 86, 78, 82, 86, 74, 73, 69, 84, 44, 98, 97, 99, 104, 117,
112, 97, 108, 108, 121, 44, 104, 121, 100, 101, 114, 97, 98, 97, 100]
Ciphertext: [1152747, 1452597, 1115563, 1774548, 1407805, 1452597, 1115563, 2421022, 1475548, 178672, 479948, 1452597, 69077
9, 1475548, 2421022, 1115563, 1880094, 1041239, 1115563, 1836432, 404729, 161351, 404729, 1115563, 2087408, 1407805, 479948,
1115563, 2408105, 1452597, 1774548, 1407805, 1115563, 1654422, 690779, 1115563, 1100860, 929977, 634784, 1100860, 1941403, 9
26100, 998691, 83486, 1505040, 2251041, 1774548, 2263413, 1007402, 178672, 2551474, 1774548, 2457724, 2457724, 2408105, 1505
040, 1007402, 2408105, 479948, 1452597, 1407805, 1774548, 2251041, 1774548, 479948]

Sender's original message: we are students of CSBS 3rd year in VNRVJIET,bachupally,hyderabad
Receiver's decrypted message: we are students of CSBS 3rd year in VNRVJIET,bachupally,hyderabad
Messages match!
```



```
Sender, enter your message: We are students of CSBS 3rd year in VNRVJIET
Receiver, enter your message: We are students of CSBS3rd year in VNRVJIET
```



```
Sender, enter your message: We are students of CSBS 3rd year in VNRVJIET
Receiver, enter your message: We are students of CSBS3rd year in VNRVJIET

Prime number P:  3793
Prime number q:  3877
Public Key:  3695881
Private Key:  7193401
n:  14705461
Phi of n:  14697792  Secret

Sender's Information:
Original Message: We are students of CSBS 3rd year in VNRVJIET
Message in ASCII code: [87, 101, 32, 97, 114, 101, 32, 115, 116, 117, 100, 101, 110, 116, 115, 32, 111, 102, 32, 67, 83, 66,
83, 32, 51, 114, 100, 32, 121, 101, 97, 114, 32, 105, 110, 32, 86, 78, 82, 86, 74, 73, 69, 84]
Ciphertext: [6978823, 3390427, 3890724, 11813309, 12960303, 3390427, 3890724, 13915809, 12002820, 6543427, 8746069, 3390427,
1282387, 12002820, 13915809, 3890724, 11762167, 1994077, 3890724, 4166370, 10536772, 5973875, 10536772, 3890724, 3680938, 12
960303, 8746069, 3890724, 10589838, 3390427, 11813309, 12960303, 3890724, 7056764, 1282387, 3890724, 6686346, 1357028, 19358
22, 6686346, 1979501, 13928490, 2715591, 12772820]

Receiver's Information:
Original Message: We are students of CSBS3rd year in VNRVJIET
Message in ASCII code: [87, 101, 32, 97, 114, 101, 32, 115, 116, 117, 100, 101, 110, 116, 115, 32, 111, 102, 32, 67, 83, 66,
83, 51, 114, 100, 32, 121, 101, 97, 114, 32, 105, 110, 32, 86, 78, 82, 86, 74, 73, 69, 84]
Ciphertext: [6978823, 3390427, 3890724, 11813309, 12960303, 3390427, 3890724, 13915809, 12002820, 6543427, 8746069, 3390427,
1282387, 12002820, 13915809, 3890724, 11762167, 1994077, 3890724, 4166370, 10536772, 5973875, 10536772, 3680938, 12960303, 8
746069, 3890724, 10589838, 3390427, 11813309, 12960303, 3890724, 7056764, 1282387, 3890724, 6686346, 1357028, 1935822, 66863
46, 1979501, 13928490, 2715591, 12772820]

Messages do not match!
```

CONCLUSION

The realm of secure communication stands at the forefront of digital advancement, addressing the critical need for confidentiality, authenticity, and integrity in our interconnected world. RSA encryption, with its robust mathematical foundation and widespread acceptance, emerges as a linchpin in this landscape.

Moreover, as data continues to be the lifeblood of modern enterprises and personal interactions, the importance of RSA encryption in safeguarding this data cannot be overstated. Its adaptability across sectors, from the intricacies of healthcare data to the vastness of supply chains, underscores its universal relevance.

In conclusion, as we navigate the complexities of the digital age, the role of RSA encryption in fortifying our communication channels against adversaries remains pivotal. Its legacy as a cornerstone of cryptographic security is not just a testament to its past achievements but also a beacon guiding future innovations in the quest for digital trust and security.