# RSA Algorithm - *Team DekhaJak*

Afzal Hossain Alif [1] Abdur Rouf [2] Mst. Aysa Siddika Meem[3] Md Sadaf Shahriar [4] Md Arman Munshi [5] Najmul Ahsan Shuvo[6]

Department of Computer Science and Engineering
Independent University, Bangladesh
Dhaka, Bangladesh.
{[1]2131050,[2]2231499,[3]2220281,[4]2130276,[5]2230029,[6]1730863}@iub.edu.bd

## Abstract

In this project, we explore the RSA algorithm and its application in ensuring data security. We discuss the challenges we faced, including handling large ASCII encrypted integers generated by RSA, and our solution of using custom charset encode-decode functions to reduce cipher size. RSA was chosen due to its complexity and high computational requirements for decryption, ensuring strong security for sensitive data. We also explore substitute uses of RSA and discuss its potential alternative solution.

## Introduction

In the digital age, data security is paramount. The RSA algorithm is a key player in safeguarding information, addressing the challenge of secure data transmission in an insecure environment. RSA ensures secure communication by encrypting data in a way that only authorized parties with the decryption key can decipher it. This solves the real-world issue of protecting sensitive data, like personal information and financial transactions, in insecure digital channels.

Operating on the principles of public-key cryptography, RSA uses unique mathematical properties of prime numbers. Its security relies on the difficulty of factoring large semiprime numbers, making it a robust solution for secure online transactions, digital signatures, and confidential communication.

In a nutshell, RSA's asymmetric encryption and reliance on mathematical complexity make it a vital tool for secure data transmission.

## Substitute Use of the Algorithm

The RSA algorithm's significance goes beyond encryption and decryption. Its versatility finds applications in vital cybersecurity areas.

RSA is pivotal in Virtual Private Networks (VPNs) by securing key exchange for encrypted connections over untrusted networks. In Secure Sockets Layer (SSL) certificates, RSA's digital signatures ensure website authenticity and data privacy, crucial for secure online interactions.

RSA's digital signatures validate documents, emails, and software. It guarantees the sender's identity, ensuring secure code distribution, tamper-proof emails, and authenticated documents.

The RSA algorithm is a cornerstone of cybersecurity. Its multifaceted roles encompass VPNs, SSL certificates, secure email, code signing, and beyond. Its contributions fortify online privacy, data integrity, and trust in digital transactions.

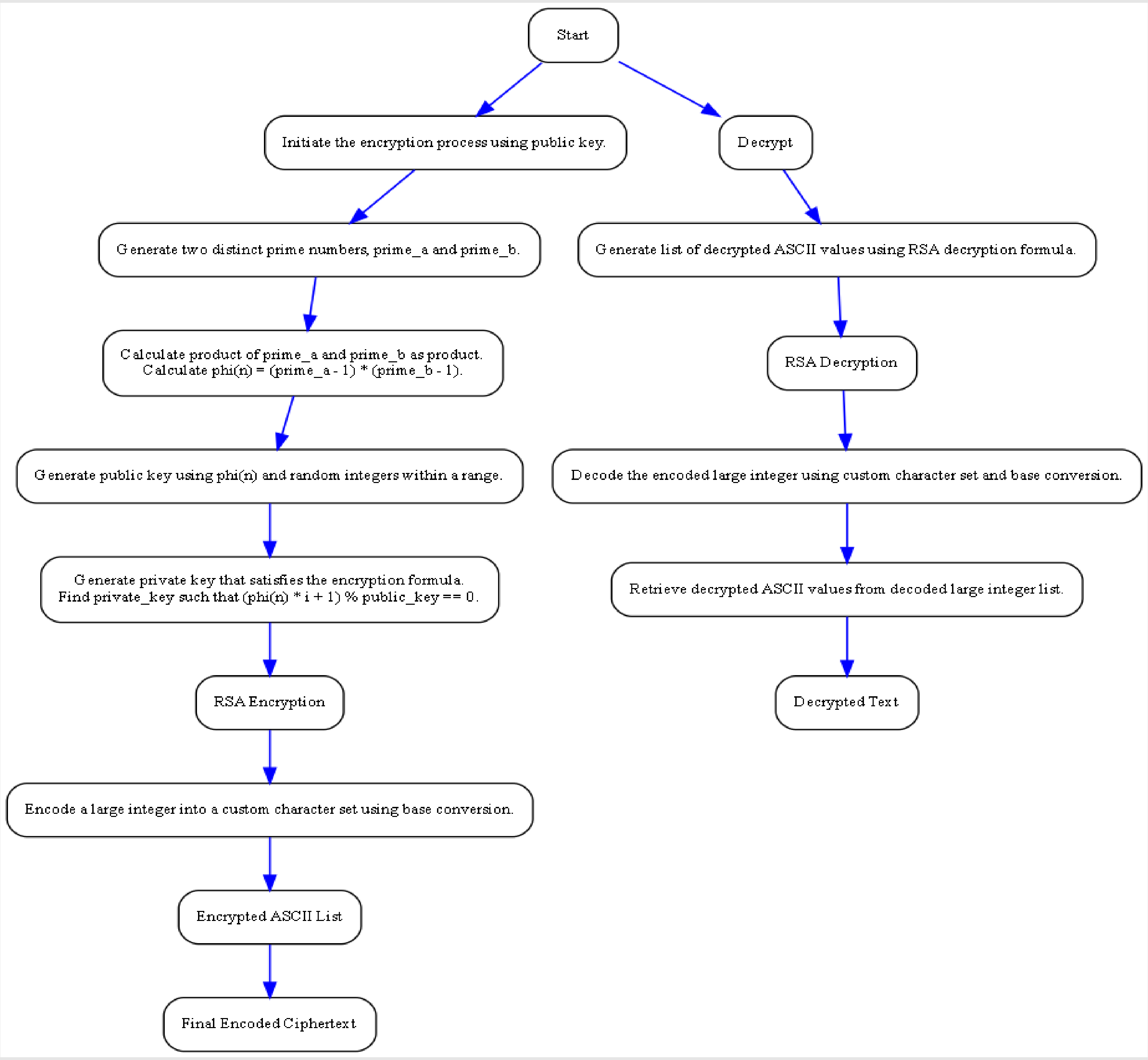
## Methodology

### Encryption Path ("En"):

- The algorithm generates two random prime numbers within a specified range: primeA and primeB.
- The product of these prime numbers product and the Euler's totient function phiN are calculated.
- The public key publicKey is determined by selecting a suitable integer between a range that is coprime with phiN.
- The private key privateKey is calculated based on the multiplicative inverse of the public key modulo phiN.
- The plaintext is converted to ASCII values and then encrypted using the public key and product. The encrypted ASCII values are stored in encryptedStrList.
- The encrypted ASCII values are concatenated to form a large integer bigInt.
- The large integer is encoded using a custom character set and the encodeLargeInteger function to generate the final ciphertext.

### Decryption Path ("De"):

- The ciphertext is decoded using the custom character set and the decodeLargeInteger function, retrieving the encrypted ASCII values as a list.
- The private key and product are used to decrypt each encrypted ASCII value back to the original ASCII values.
- The original ASCII values are converted back to characters, forming the decrypted plaintext.
- The decrypted plaintext is returned as the output.



Start

Initiate the encryption process using public key.

Generate two distinct prime numbers, prime_a and prime_b.

Calculate product of prime_a and prime_b as product.
Calculate phi(n) = (prime_a - 1) * (prime_b - 1).

Generate public key using phi(n) and random integers within a range.

Generate private key that satisfies the encryption formula.
Find private_key such that (phi(n) * i + 1) % public_key == 0.

RSA Encryption

Encode a large integer into a custom character set using base conversion.

Encrypted ASCII List

Final Encoded Ciphertext

Decrypt

Generate list of decrypted ASCII values using RSA decryption formula.

RSA Decryption

Decode the encoded large integer using custom character set and base conversion.

Retrieve decrypted ASCII values from decoded large integer list.

Decrypted Text

The encryption and decryption processes are represented as separate paths to emphasize their distinct operations.

## Rationale for the Algorithm's Selection

The selection of the RSA algorithm for this project was underpinned by its well-established reputation for robust and dependable security features within the realm of modern cryptography. The algorithm's selection is rooted in its distinctive reliance on the formidable computational challenge of factoring large prime numbers, a task recognized as exceptionally arduous within the realm of number theory. This unique characteristic engenders a highly asymmetrical encryption scheme wherein encryption is straightforward, yet decryption without access to the corresponding private key becomes an intractable problem.

Central to RSA's appeal is its inherent complexity, which renders it resilient against a range of cryptographic attacks, including brute-force and deterministic methods. This complexity is harnessed from the inherently intricate nature of prime factorization, a mathematical problem that has long stymied attempts to create computationally efficient algorithms capable of undermining the RSA paradigm. This factor lends the algorithm a steadfastness that is particularly well-suited for applications necessitating robust data protection and privacy.

Furthermore, the mathematical foundation upon which RSA is predicated has been rigorously examined and tested by cryptographic experts over decades, solidifying its trustworthiness within both theoretical and practical contexts. The algorithm's proven track record in various applications, ranging from secure communication channels to digital signatures, underscores its versatile utility in safeguarding sensitive information across diverse domains. Prominent industry leaders such as Amazon, Microsoft, and IBM have incorporated RSA into their products, attesting to its significance in modern cybersecurity frameworks.

## Alternative Solution

While the RSA algorithm offers robust security, exploring alternatives like Advanced Encryption Standard (AES) unveils certain advantages. AES, a symmetric-key algorithm, offers faster encryption and decryption, making it ideal for resource-intensive applications. However, implementing AES from scratch presents considerable challenges due to its complexity.

### AES vs. RSA Performance:

AES outperforms RSA in terms of speed, especially for large datasets. RSA's complexity arises from its reliance on large prime numbers and intricate mathematical operations, which affect its computational efficiency.

### Enhancing Current System:

In our existing system, we can optimize the big integer encoder and decoder, potentially utilizing more efficient algorithms to reduce encoding size. Additionally, replacing the current two-prime key generation method with a more sophisticated approach involving multiple inputs could bolster security and key diversity.

### Trade-offs and Considerations:

While AES holds performance advantages, RSA's asymmetric nature contributes to its unique security features. AES requires secure key exchange mechanisms, while RSA's public-private key pair offers a seamless way to distribute keys. Implementing AES might necessitate existing infrastructure changes to accommodate symmetric encryption's characteristics.

While AES offers enticing performance gains, the complexity of implementation and the nuanced trade-offs between AES and RSA underscore the importance of careful algorithm selection aligned with specific security and performance needs.

## Conclusion

In conclusion, the RSA algorithm stands as a testament to the enduring significance of cryptography in ensuring secure communications within the digital landscape. This project delved into the intricate workings of the RSA algorithm, elucidating its foundational principles and real-world applications. By meticulously investigating the algorithm's encryption and decryption processes, we unearthed its ability to safeguard sensitive information through the generation and manipulation of prime numbers, thereby facilitating robust data protection.

The algorithm's inherent security is underpinned by its reliance on the arduous task of prime factorization, rendering it impervious to brute-force attacks. Consequently, the RSA algorithm is not only a manifestation of theoretical complexity but also embodies practical resilience against adversarial efforts. As a result, it finds extensive employment in scenarios requiring secure data transmission, digital signatures, and authentication protocols.

Moreover, while the RSA algorithm serves as a cornerstone of contemporary cryptography, it is essential to acknowledge that the constant evolution of computing power necessitates continuous reassessment and refinement of cryptographic techniques. The algorithm's intricate nature, as witnessed in the intricate flowchart delineated above, not only underscores its significance but also prompts the exploration of potential enhancements.

To conclude, the RSA algorithm stands as an enduring exemplar of cryptography's potency in upholding data integrity, privacy, and security. This exploration offered valuable insights into its underlying mechanics and applicability, cementing its position as a pivotal tool in safeguarding the digital realm against ever-evolving threats. As the digital landscape evolves, the RSA algorithm's foundational principles remain as a steadfast safeguard, paving the way for a secure and interconnected future.