RSA Information Encryption

ICTU Student 164
Thai Nguyen University of Information and Communication Technology
Thai Nguyen University, Thai Nguyen, Vietnam
student164@ictu.edu.vn

***Abstract*—This thesis explores classical encryption methods and focuses on the RSA encryption algorithm. It covers the RSA algorithm, its key generation, encryption and decryption processes, and the security of the RSA system. The author also discusses various number-theoretic algorithms used in RSA, such as the square and multiply algorithm, the extended Euclidean algorithm, and primality testing algorithms. The thesis concludes with a demonstration of an RSA encryption program developed using Visual Basic 6.0, highlighting its limitations and suggesting future improvements. The study provides a comprehensive overview of classical encryption methods, emphasizing the importance of data security in the digital age. It also highlights the limitations of the implemented program, such as its limited file type support and the need for further research to optimize the algorithm for larger data sets.**

***Index Terms*—RSA, encryption, Visual Basic 6.0, public key cryptography, data security**

I. Introduction

The thesis introduces the importance of data security in the digital age, emphasizing the need for secure data transmission. It discusses the limitations of classical encryption methods and the introduction of public key cryptography, particularly the RSA algorithm, which is widely used for secure data transmission. The author explores various classical encryption methods, including shift cipher, affine cipher, and Vigenère cipher, to provide a foundation for understanding the RSA algorithm. The introduction also discusses the significance of the RSA algorithm in modern cryptography and its role in ensuring secure data transmission [1]. Published books on the methods and subject of this project provide context for this English summary [6]. Related earlier ICTU undergraduate theses provide context for this English summary [7], [8], [9]. Published articles on the methods and subject of this project provide context for this English summary [10].

II. Methods

The author implemented the RSA algorithm using Visual Basic 6.0 to create a demonstration program for encrypting and decrypting data files. The program was developed to provide a basic understanding of the RSA algorithm, but it has limitations in terms of file type support and network application. The implementation involved generating keys, performing encryption and decryption operations, and using number-theoretic algorithms such as the square and multiply algorithm, the extended Euclidean algorithm, and primality testing algorithms. The program was tested with simple text files, but it could not handle complex file formats such as images or audio files [1].

Supervisor: Ngô Thị Lan Phương, Thai Nguyen University of Information and Communication Technology (ntlphuong@ictu.edu.vn).

III. Results

The developed program successfully demonstrated the RSA encryption and decryption processes. However, it was noted that the program was limited to simple file types and could not be applied to complex file formats such as images or audio files. The program was tested with text files, and the encryption and decryption processes worked as expected. The author also implemented the square and multiply algorithm, the extended Euclidean algorithm, and primality testing algorithms, which were used in the encryption and decryption processes. However, the program did not provide a comprehensive evaluation of the security of the RSA system [1].

IV. Discussion

The author discusses the limitations of the implemented program, including its limited file type support and the need for further research to optimize the algorithm for larger data sets. The thesis suggests potential improvements such as expanding file type support and optimizing the algorithm for better performance. The author also highlights the importance of further research in the field of cryptography, particularly in the area of public key cryptography. The limitations of the implemented program are discussed, and the author suggests that future work should focus on enhancing the program's functionality and performance [1].

V. Conclusion

The thesis concludes that while the RSA algorithm is a robust method for data encryption, the implementation in Visual Basic 6.0 is limited in its practical application. The author suggests future work to enhance the program's functionality and performance. The study provides a comprehensive overview of classical encryption methods and the RSA algorithm, emphasizing the importance of data security in the digital age. The author acknowledges the limitations of the implemented program and suggests that future research should focus on expanding file type support and optimizing the algorithm for larger data sets [1].

References

[1] ICTU Student 164, ”RSA Information Encryption,” internal undergraduate thesis (original in Vietnamese), Thai Nguyen University of Information and Communication Technology, 2010.

[2] Phạm Huy Điển - Hà Huy Khoái, Mã hóa thông tin - Cơ sở toán học và ứng dụng, Viện Toán học, năm 2004

[3] Nguyễn Thị Kiều Duyên, Lập trình Virual Basic 6.0, NXB Trẻ

[4] Hà Thị Thanh, Nguyễn Văn Tảo, Nguyễn Lan Oanh, Bài giảng An toàn và bảo mật thông tin, Khoa CNTT – ĐH Thái nguyên

[5] Đinh Xuân Lâm, Sách Visual Basic cho sinh viên và kỹ thuật viên Khoa Công nghệ thông tin, NXB Thống kê

[6] Arto Salomaa, ”Public-Key Cryptography,” Springer Berlin Heidelberg, 1990. ISBN 9783662026298. DOI: 10.1007/978-3-662-02627-4.

[7] ICTU Student 42, ”RSA Public Key Cryptography: Encryption, Decryption, and Digital Signature,” internal undergraduate thesis, Thai Nguyen University of Information and Communication Technology, 2008.

[8] ICTU Student 94, ”Research on Public Key Cryptographic System and Implementation of RSA Algorithm for Electronic Signature,” internal undergraduate thesis, Thai Nguyen University of Information and Communication Technology, 2009.

[9] Đỗ Thị Phương Lan, ”Some Attacks on the RSA Public Key Cryptosystem,” internal undergraduate thesis, Thai Nguyen University of Information and Communication Technology, 2008.

[10] G. R. Blakley, ”Two Issues in Public Key Cryptography: RSA Bit Security and a New Knapsack Type System (Ben-Zion Chor),” SIAM Review, vol. 30, no. 4, pp. 664-665, 1988. DOI: 10.1137/1030155.