Electronic Signature and Authentication Protocols

ICTU Student 155
Thai Nguyen University of Information and Communication Technology
Thai Nguyen University, Thai Nguyen, Vietnam
student155@ictu.edu.vn

***Abstract*—This thesis explores the concept of electronic commerce and the role of electronic signatures in ensuring the authenticity and integrity of transactions. It discusses the importance of electronic signatures in e-commerce and introduces the RSA and Elgamal signature schemes, detailing their cryptographic principles and practical applications. The author also presents a demonstration of an electronic signature program, highlighting its strengths and limitations. The study focuses on the theoretical aspects and practical implementation of these cryptographic protocols, aiming to enhance trust and security in online transactions.**

***Index Terms*—Electronic commerce, Electronic signature, RSA, Elgamal, Cryptographic protocol, Digital signature**

I. Introduction

The thesis introduces the concept of electronic commerce and the significance of electronic signatures in enhancing trust and security in online transactions. It provides an overview of the development of electronic commerce and its impact on various sectors, emphasizing the need for secure transaction methods. The study aims to explore the cryptographic principles and practical applications of electronic signatures, specifically focusing on the RSA and Elgamal schemes [1]. Related earlier ICTU undergraduate theses provide context for this English summary [9], [10], [11].

II. Methods

The author conducted a theoretical study and developed a demonstration program for an electronic signature using the RSA scheme. The program was tested for its ability to sign text files and verify signatures, identifying both its strengths and weaknesses. The Elgamal scheme was also briefly discussed, highlighting its cryptographic principles and potential applications. The implementation involved generating keys, signing text files, and verifying signatures, with the program tested on a variety of file sizes [1].

III. Results

The demonstration program successfully signed text files and verified signatures, demonstrating the accuracy of the RSA scheme. However, the program's random key generation process was found to be weak, and signing large files was time-consuming. The Elgamal scheme was shown to offer a different approach to digital signatures, with its security based on the difficulty of solving the discrete logarithm problem. The program's implementation faced challenges in key generation and performance with large files [1].

Supervisor: Lê Tuấn Anh, Thai Nguyen University of Information and Communication Technology (ltanh@ictu.edu.vn).

IV. Discussion

The implemented demonstration uses the RSA signature scheme to sign text files and verify signatures. The author's own assessment says that the generated random keys were too small to provide strong protection and that signing large files was slow. The text therefore supports a demonstration of the signing workflow, not a claim that the software was ready for secure transactions. Elgamal is discussed as another cryptographic scheme in the theoretical review. The proposed extensions include support for more file formats, a more usable interface, and a fuller signing and messaging application [1]. Earlier ICTU undergraduate work by Đinh Thị Thúy addressed encryption algorithms used in information authentication [8].

V. Conclusion

The author concludes that while the RSA scheme can effectively create and verify electronic signatures, the program's current implementation has limitations, such as weak key generation and slow performance with large files. Future work should focus on enhancing the program's capabilities and user experience. The Elgamal scheme offers an alternative approach, but its implementation also faces challenges in key generation and performance. The study highlights the need for continued research and development in cryptographic protocols for secure electronic transactions [1].

References

[1] ICTU Student 155, "Electronic Signature and Authentication Protocols," internal undergraduate thesis (original in Vietnamese), Thai Nguyen University of Information and Communication Technology, 2010.
[2] Andrew S.Tanenbaum, Computer Networks, Prentice Hall, New Jersey, Fourth Edition, 2003
[3] William Stallings, Network Sercurity Essentials, 2000
[4] Man Young Rhee, Wilay, Internet Sercurity – Cryptographic Principles, Algorithms and Protocol, 2003
[5] Hà Thị Thanh – Nguyễn Văn Tảo, Giáo trình an toàn và bảo mật thông tin, khoa công nghệ thông tin – Đại học Thái Nguyên
[6] TS Nguyễn Đại Thọ, An toàn mạng, Đại học Công Nghệ - ĐHQGHN
[7] Phạm Công Ngô, Lập trình C# từ cơ bản đến nâng cao, NXB Giáo Dục
[8] Đinh Thị Thúy, "Study of Cryptographic Algorithms," internal undergraduate thesis, Thai Nguyen University of Information and Communication Technology, 2008.
[9] ICTU Student 107, "RSA Algorithm and Electronic Signature Application," internal undergraduate thesis, Thai Nguyen University of Information and Communication Technology, 2009.
[10] 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.

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