Some Information Encryption Methods and Their Application in Information Verification

ICTU Student 165
Thai Nguyen University of Information and Communication Technology
Thai Nguyen University, Thai Nguyen, Vietnam
student165@ictu.edu.vn

***Abstract*—This thesis explores various encryption methods and their application in information verification. It covers classical encryption systems such as Vigenere, Hill, and affine ciphers, as well as modern public key algorithms like RSA and ElGamal. The author also discusses the Java programming language and its security APIs, developing a program that can generate keys, sign, and verify documents. The work aims to enhance understanding of encryption techniques and their practical implementation in Java. The author successfully developed a program that can generate keys, sign, and verify documents. The program is user-friendly and meets the basic requirements of the thesis. The author also gained a deeper understanding of Java programming and its security APIs. Future work should focus on further research into encryption architectures and improving the program to better meet real-world requirements.**

***Index Terms*—encryption, information verification, Java programming, public key algorithms, ciphers, security APIs**

I. Introduction

The thesis aims to understand encryption methods and their application in information verification. It covers classical encryption systems like Vigenere, Hill, and affine ciphers, as well as modern public key algorithms such as RSA and ElGamal. The author also delves into the Java programming language and its security APIs, developing a program that can generate keys, sign, and verify documents. The work is based on a comprehensive review of existing literature, including textbooks and research papers on cryptography and Java security. The author acknowledges the limitations of the study, such as the limited time and practical experience, which may have affected the depth of the research [1].

II. Methods

The thesis discusses various encryption methods, including classical ciphers and modern public key algorithms. It also covers the Java programming language and its security APIs, using these to develop a program that can generate keys, sign, and verify documents. The author implemented the Vigenere, Hill, and affine ciphers, as well as the RSA and ElGamal public key algorithms. The program was developed using the Java programming language and the Java Cryptography Architecture (JCA) and Java Secure Socket Extension (JSSE) APIs. The author tested the program by generating keys, signing, and verifying documents, and found that the program met the basic requirements of the thesis [1].

Supervisor: ICTU Teacher 106, Thai Nguyen University of Information and Communication Technology.

III. Results

The author successfully developed a program that can generate keys, sign, and verify documents. The program is user-friendly and meets the basic requirements of the thesis. The author also gained a deeper understanding of Java programming and its security APIs. The program implemented the Vigenere, Hill, and affine ciphers, as well as the RSA and ElGamal public key algorithms. The author tested the program by generating keys, signing, and verifying documents, and found that the program performed as expected. However, the author noted that the program could be improved to better meet real-world requirements, such as increased security and efficiency [1].

IV. Discussion

The thesis discusses the importance of encryption methods in information verification and the practical implementation of these methods in Java. The author highlights the need for further research into encryption architectures and the support provided by Java security APIs. The author also notes that the program developed in the thesis could be improved to better meet real-world requirements, such as increased security and efficiency. The author suggests that future work should focus on further research into encryption architectures and improving the program to better meet real-world requirements [1]. Earlier ICTU undergraduate work by Đinh Thị Thúy addressed encryption methods for information verification [8].

V. Conclusion

The author successfully developed a program that can generate keys, sign, and verify documents. The program is user-friendly and meets the basic requirements of the thesis. The author also gained a deeper understanding of Java programming and its security APIs. Future work should focus on further research into encryption architectures and improving the program to better meet real-world requirements. The author acknowledges the limitations of the study, such as the limited time and practical experience, which may have affected the depth of the research [1].

References

[1] ICTU Student 165, "Some Information Encryption Methods and Their Application in Information Verification," internal undergraduate thesis (original in Vietnamese), Thai Nguyen University of Information and Communication Technology, 2010.

[2] Bùi Doãn Khanh – Nguyễn Đình Thúc – Hoàng Đức Hải, Giáo Trình Mã Hóa Thông Tin - Lý Thuyết Và Ứng Dụng, NXB Lao động – Xã hội, 12/2004
[3] Nguyễn Xuân Dũng, Bảo mật thông tin mô hình và ứng dụng, NXB Thống kê,2007
[4] Phạm Thế Bảo – Hoàng Đức Hải – Phương Lan, Bảo mật lập trình mạng trong java 2, Nhà xuất bản thống kê, 2005
[5] Phương lan – Hoàng Đức Hải, Lập trình java tập 1, NXB thống kê, 2003
[6] Nguyễn Đình Thúc – Bùi Doãn Khanh, Mã hóa thông tin với java, Nhà xuất bản lao động xã hội, 2006
[7] Rich Helton – Johenie Helton, Java Security Solutions, Wiley Publishing, Inc., Indianapolis, Indiana, 2002
[8] Đinh Thị Thúy, ”Study of Cryptographic Algorithms,” internal undergraduate thesis, Thai Nguyen University of Information and Communication Technology, 2008.