MỘT BIẾN THỂ CỦA HỆ MÃ RSA TRÊN CẤU TRÚC DỰA VÀO VÀNH BERGMAN

Trần Đình Long[1], Lê Thị Kim Nga[2]
[1]Khoa Toán,
Trường Đại học Khoa học, Đại học Huế
[2]Khoa Công Nghệ Thông Tin
Trường Đai học Sư Phạm TP Hồ Chí Minh
trandinhlong1963@yahoo.com.vn, kimnga412@gmail.com

Tóm tắt

Dựa trên các kết quả về các phép tính trên vành $End(\mathbb{Z}_p \times \mathbb{Z}_{p^k})$, bài báo xây dựng một hệ mã trong đó mã hóa và giải mã được thực hiện theo kiểu lũy thừa, với mỗi văn bản là một 2×2 ma trận. Mặc dù cần đến nhiều phép tính hơn trong các quá trình mã hóa và giải mã, hệ mã có nhiều ưu điểm so với hệ mã RSA gốc trong việc tấn công bằng dàn 2 chiều hoặc tấn công bằng cách chọn văn bản gốc.

Từ khóa: hệ mã RSA, đồng cấu vành, tấn công dàn.

A RSA VARIANT ON BERGMAN RING BASED PLATFORM

***Tran Dinh Long*[1], *Le Thi Kim Nga*[2]**
[1]Faculty of Mathematics, School of Science, Hue University
[2]Faculty of Information Technology, Ho Chi Minh City University of Education
trandinhlong1963@yahoo.com.vn, kimnga412@gmail.com

Abstract

Based on the arithmetic of the ring $End(\mathbb{Z}_p \times \mathbb{Z}_{p^k})$, the paper constructs an exponent type encryption and decryption cryptosystem, where each plaintext is a 2×2 matrix. Althought involving more operations in encryption and decryption phases than that in original RSA one, the cryptosystem has some advantages in avoiding lattice and chosen plaintext attacks compared to original RSA cryptosystem.

Key words: RSA cryptosystem, ring endomorphism, lattice attack.