VII-O-11

MỘT MÔ HÌNH TỔNG QUÁT CHO HỆ MÃ HÓA RSA

Trần Đình Long[1], Trần Đan Thư[2], Nguyễn Đình Thúc[2]
[1]Trường ĐH Huế
[2]Khoa Công nghệ Thông tin, Trường ĐH Khoa học Tự nhiên - ĐHQG Tp.HCM

Tóm tắt

Từ khi được công bố lần đầu tiên vào 1976, hệ mã hóa RSA đã được sử dụng rộng rãi trong nhiều lĩnh vực áp dụng. Đó là lý do tại sao các hệ mã hóa RSA mở rộng lại được nghiên cứu và công bố. Mặc dù được trình bày dưới nhiều quan điểm khác nhau, một số hệ mã RSA mở rộng lại có cùng một mô hình toán học. Bài báo này đề nghị một mô hình tổng quát cho hệ mã RSA trên vành thương của vành Euclid, một số hệ mã RSA mở rộng đã biết cũng thuộc vào mô hình này.

Từ khoá: hệ mã hóa RSA, hàm Euler, vành Euclid.

A GENERAL MODEL FOR RSA CRYPTOSYSTEM

Tran Đinh Long[1], Tran Đan Thu[2], Nguyen Đinh Thuc[2]
[1]Hue University
[2]Faculty of Information Technology, University of Science - VNU HCMC

Abstract

Since RSA was first introduced in 1976, it then has been widely used in various applications. That is the reason why many RSA variants have been considered. However, although being presented under many points of view, some of them have the same mathematical model. In this article, we propose a framework for RSA on quotient ring of an Euclidean ring which covers some modified RSA.

Key words: RSA cryptosystem, Euler function, Euclidean ring.