CƠ SỞ TOÁN HỌC CHO CÁC BIẾN THỂ CỦA RSA

Trần Đình Long[1*], Võ Anh Duy[2]

[1] Khoa Toán, trường Đại học Khoa học, Đại học Huế

[2] Trường THCS Tôn Đức Thắng, thị xã Đông Hòa, tỉnh Phú Yên

* Email: tdlong@husc.edu.vn

Ngày nhận bài: 4/5/2021; ngày hoàn thành phản biện: 18/6/2021; ngày duyệt đăng: 02/11/2021

TÓM TẮT

Có rất nhiều biến thể của RSA từ khi hệ mã này dược công bố đầu tiên vào năm 1978. Các biến thể này của RSA được thiết lập trên các cấu trúc đại số khác nhau, vì vậy chúng được xây dựng về mặt toán học theo các cách khác nhau. Chúng tôi sẽ chỉ ra rằng, các biến thể này có thể được xây dựng trên cùng một nền tảng toán học sử dụng các công cụ trong lý thuyết nhóm.

Từ khóa: nhóm, RSA.

TOWARD A UNIFORM ESTABLISHING RSA CRYPTOSYSTEMS

Long T. D[1*], Duy V. A.[2]

[1] Faculty of Mathematics, University of Sciences, Hue University

[2] Ton Duc Thang Secondary School, Dong Hoa City, Phu Yen District

* Email: tdlong@husc.edu.vn

ABSTRACT

There have been many RSA cryptosystems which firstly came into existence since 1978. These RSA cryptosystems rely on different algebraic structures, therefore they were constructed in various ways. We show that, by group based tools, such cryptosystems can be established uniformly.

Keywords: group, homomorphism, RSA cryptosystem.

Trần Đình Long sinh ngày 18/01/1963 tại Thừa Thiên Huế. Năm 1984, ông tốt nghiệp cử nhân ngành Toán tại Trường Đại học Tổng hợp Huế. Năm 1997 tốt nghiệp thạc sỹ ngành Công nghệ thông tin tại trường QUT (Queensland University of Technology). Ông bào vệ tiến sĩ ngành Khoa học Máy tính năm 2015 tại trường Đại học Khoa học Tự nhiên thành phố Hồ Chí Minh.

Lĩnh vực nghiên cứu: Mã hóa thông tin, Đại số.

Võ Anh Duy sinh ngày 02/05/1990 tại Phú Yên. Năm 2012, ông tốt nghiệp ngành Sư phạm Tin học tại Trường Đại học Phú Yên. Năm 2016, ông tốt nghiệp Thạc sĩ ngành Khoa học máy tính tại trường Đại học Khoa học, ĐH Huế. Từ năm 2019, ông theo học lớp Cao học ngành Toán ứng dụng của trường Đại học Khoa học, ĐH Huế.

Lĩnh vực nghiên cứu: Toán ứng dụng.