APLIKASI ALJABAR PADA KRIPTOGRAFI DAN KEAMANAN INFORMASI

Muhamad Zaki Riyanto
Program Studi Pendidikan Matematika FKIP UAD
Jl. Prof. Dr. Soepomo, SH. Janturan Yogyakarta
E-mail: zaki@mail.ugm.ac.id

ABSTRAK

Informasi rahasia yang dikirimkan melalui jalur komunikasi yang tidak aman seperti internet, mempunyai resiko yang besar untuk disadap oleh pihak-pihak yang tidak berhak mengetahui informasi rahasia tersebut. Salah satu hal yang dapat dilakukan adalah dengan menyandikan informasi tersebut menjadi kode-kode yang tidak dapat dimengerti. Seni dan ilmu untuk menjaga kerahasiaan informasi disebut dengan kriptografi.

Dalam sejarahnya, kriptografi telah digunakan sejak zaman Romawi kuno, perang dunia, hingga era digital dan teknologi informasi seperti saat ini. Dari awal perkembangannya, metode yang digunakan untuk proses penyandian menggunakan perhitungan-perhitungan yang sederhana. Seiring dengan perkembangan teknologi, metode yang digunakan juga terus berkembang, seperti penggunaan komputer dengan perhitungan-perhitungan matematika yang rumit.

Salah satu bidang Matematika yang sangat berperan dalam kriptografi adalah aljabar. Banyak dari metode yang digunakan pada kriptografi menggunakan operasi-operasi aljabar yang didefinisikan atas suatu struktur aljabar, seperti pada grup, ring dan lapangan. Dalam makalah ini dibahas mengenai beberapa aplikasi aljabar yang digunakan dalam kriptografi, khususnya mengenai struktur aljabar (aljabar abstrak) dan aljabar linear. Metode kriptografi yang diberikan adalah Caesar cipher, shift cipher, cipher permutasi, Hill cipher, ElGamal dan RSA.

Kata Kunci : aljabar, enkripsi, dekripsi, kriptografi

ABSTRACT

The confidential information that sent via an insecure communication channels like the internet, have a greater risk to be tapped by the parties are not entitled to know the confidential information. One of the things that can be done is to encrypt information into code that can not be understood. Art and science to keep the confidentiality of information is called cryptography.

Historically, cryptography has been used since ancient Roman times, world war, until the digital age and information technology as it is today. From the beginning of its development, the method used for the encoding process using simple calculations. Along with the development of technology, the methods used are also growing, such as the use of computers with mathematical calculations are complicated.

One area of Mathematics that has a very important role in cryptography is algebra. Many of the methods used in cryptography using algebraic operations are defined over an algebraic structure, as in the group, ring and field. In this paper, its discussed about several applications of algebra that used in cryptography, especially on the structure of algebra (abstract algebra) and linear algebra. Given cryptographic method is Caesar cipher, shift cipher, permutation cipher, Hill cipher, ElGamal and RSA.

Keywords: algebra, cryptography, decryption, encryption