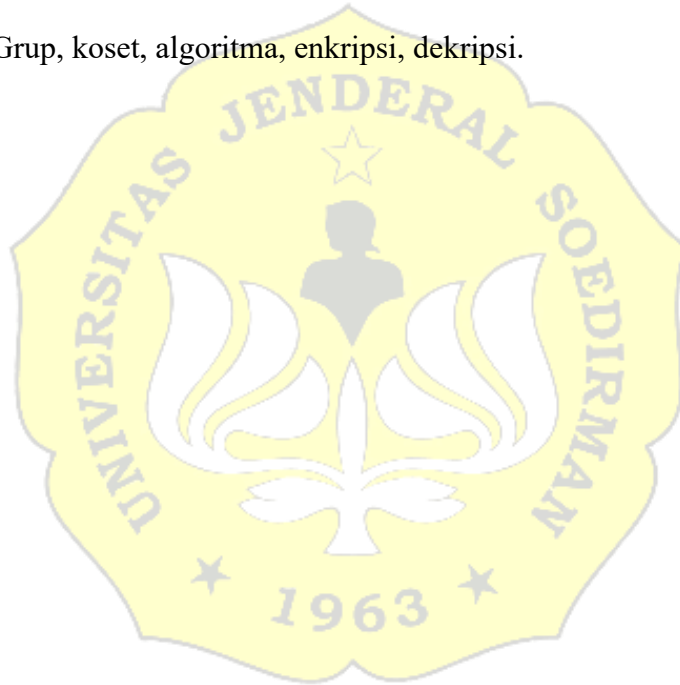


ABSTRAK

Penelitian ini membahas tentang penerapan koset grup aditif himpunan bilangan bulat $\mathbb{Z}$ dalam perancangan algoritma kriptografi. Pembahasan diawali dengan tinjauan teori grup, subgrup dan koset sebagai dasar matematis pengembangan sistem kriptografi. Penelitian menggunakan subgrup $60\mathbb{Z}$ untuk membentuk koset yang dimanfaatkan dalam proses enkripsi dan dekripsi. Selanjutnya, rancangan algoritma kriptografi tersebut diimplementasikan dalam bentuk program enkripsi-dekripsi dengan pendekatan koset grup menggunakan bahasa pemrograman C++. Hasil penelitian yang diperoleh berupa rancangan algoritma kriptografi dengan menggunakan himpunan koset $\mathbb{Z}/60\mathbb{Z}$ dan diimplementasikan dalam bahasa C++. Pemanfaatan koset pada $\mathbb{Z}/60\mathbb{Z}$ memperkuat keamanan algoritma kriptografi dengan membagi pesan dalam kelas-kelas ekuivalensi yang membuat proses pemulihan pesan tanpa kunci yang tepat menjadi lebih sulit.

Kata kunci: Grup, koset, algoritma, enkripsi, dekripsi.



ABSTRACT

This research discusses the application of the additive coset groups of integer set $\mathbb{Z}$ in the design of cryptographic algorithms. The discussion begins with a review of group theory, subgroups, and cosets as the mathematical foundation for developing cryptographic systems. This study uses the subgroup $60\mathbb{Z}$ to form cosets utilized in the encryption and decryption processes. Furthermore, the design of cryptographic algorithm is implemented as an encryption-decryption program using the coset group approach with the C++ programming language. The results of the study consist of the design of a cryptographic algorithm using the coset set $\mathbb{Z}/60\mathbb{Z}$, implemented in C++. The use of cosets in $\mathbb{Z}/60\mathbb{Z}$ strengthens the security of the cryptographic algorithm by dividing messages into equivalence classes, making the message recovery without the correct key more difficult.

Keywords: Group, coset, algorithm, encryption, decryption.

