ABSTRAK

Marselinus Junardi Rebu. 2015. *Kriptografi Klasik*. Makalah. Program Studi Matematika, Jurusan Matematika, Fakultas Sains dan Teknologi, Universitas Sanata Dharma, Yogyakarta.

Makalah ini membahas beberapa sandi *symetris-key* untuk mengenkripsi maupun mendekripsi pesan. Setiap perhitungan pada fungsi enkripsi dan fungsi dekripsi dilakukan menggunakan aritmetika modulo, khususnya modulo 26. Kriptanalisis, yaitu metode untuk memecahkan sandi, juga dipaparkan dalam tugas akhir ini untuk beberapa sandi.

Dalam tugas akhir ini, kunci yang digunakan untuk masing-masing sandi bervariasi, dapat berupa bilangan, pasangan terurut, dan matriks. Kunci-kunci ini harus mempunyai invers agar proses dekripsi dapat dilakukan. Oleh karena itu, kunci yang sulit ditebak akan menghasilkan teks-sandi yang sulit dipecahkan oleh kriptanalis.

ABSTRACT

Marselinus Junardi Rebu. 2015. *Classical Cryptography*. Paper. Mathematics Study Program, Department of Mathematics, Faculty of Science and Technology, Sanata Dharma Unyversity, Yogyakarta.

This paper discusses some cipher of *symetris-key* to encrypt and decrypt messages. Every calculation on encryption function and decryption function is performed using modular arithmetic, especially modulo 26. Cryptanalysis, the method to break the cipher, is also presented in this paper for some cipher.

In this paper, the key used for each cipher varies, it can be a number, ordered pairs, or a matrix. These keys must have an inverse in order that decryption process can be performed. Therefore, the key which is difficult to guess will generate ciphertext that is difficult to break by the cryptanalyst.