Perancangan Kriptografi *Block Cipher* Berbasis Pola Lapangan Balap Sepeda *(Velodrome)*

Reza Galih Kurniawan[1], **Magdalena A. Ineke Pakereng**[2]
Fakultas Teknologi Informasi
Universitas Kristen Satya Wacana
Jl. Diponegoro 52-60, Salatiga 50711, Indonesia
E-mail: 672013005@student.uksw.edu[1], ineke.pakereng@staff.uksw.edu[2]

Abstract

In this study, A new Velodrome base Block Cipher Cryptography was designed. This cryptography intended with 64-bit size block, using 4 process and 20 circle, where 2nd and 3rd process transmitted using S-box table to develop more randomized Ciphertext. In a Velodrome base Block Cipher Cryptography conduct a test using Avalanche Effect and Correlation value, where the character changing up to 49,921875%. So, this can be an alternative for data security.

Keywords : *Block Cipher, Cryptography, Velodrome base, S-BOX, Avanlache Effect.*

Abstrak

Dalam penelitian ini, dirancang Kriptografi *Block Cipher* Berbasis Pola Lapangan Balap Sepeda *(Velodrome)* untuk membuat kriptografi baru, kriptografi ini dirancang dengan ukuran blok 64 bit, dengan menggunakan 4 proses dan 20 putaran, dimana proses ke-2 dan ke-3 ditransformasikan menggunakan tabel *S-Box* untuk mendapatkan *Ciphertext* yang lebih acak. Pada Kriptografi *Block Cipher* Berbasis Pola Lapangan Balap Sepeda *(Velodrome)* dilakukan pengujian dengan menggunakan *Avalanche Effect* dan nilai Korelasi, dimana terjadi perubahan karakter mencapai 49,921875%. sehingga dapat digunakan sebagai alternatif dalam mengamankan data.

Kata Kunci : *Block Cipher*, Kriptografi, Pola Lapangan Balap Sepeda *(Velodrome)*, *S-BOX*, *Avalanche Effect*.

[1)] Mahasiswa Program Studi Teknik Informatika, Fakultas Teknologi Informasi, Universitas Kristen Satya Wacana
[2)] Staff Pengajar Fakultas Teknologi Informasi, Universitas Kristen Satya Wacana Salatiga