Pemenuhan Prinsip *Shannon* (*Confussoin* dan *Diffusion*) pada *Block Cipher* dengan Pola Anyaman Rambut Papua (ARAP) menggunakan *Constanta* Bilangan Prima

[1)]Fhilep Rogel Jober, [2)] Alz Danny Wowor
Fakultas Teknologi Informasi
Universitas Kristen Satya Wacana
Jl. Diponegoro 52-60, Salatiga 50771, Indonesia
Email: [1)] 672010157@student.uksw.edu,
[2)]alzdanny.wowor@staff.uksw.edu.

Abstract

Cryptography plays an important role in the security of the data or information. On the other hand, cryptographic many have been solved by cryptanalyst, so that vital information to become unsafe. By modifying the Block Cipher with the principle Shannon (Confussion and Diffusion) using Prime Numbers Constanta. ARAP so Modifications can also fulfill the principle of diffusion-shannon confusion with the increase in the value of Avalance effect and also the principle of iterated cipher based on the increased value of the avalanche effect.

Keywords : Principle Shannon(Confussion and Diffusion), constanta primes, Avalanche effect, Papuaan Hair Wover

Abstrak

Kriptografi sangat berperan dalam keamanan suatu data atau informasi. Di sisi lain, kriptografi banyak yang telah dipecahkan oleh kriptanalis, sehingga informasi penting tersebut menjadi tidak aman. Dengan memodifikasi Block Cipher dengan prinsip *Shannon* (*Confussion* dan *Diffusion*) menggunakan *Constanta* Bilangan Prima. Sehingga Modifikasi ARAP juga dapat memenuhi prinsip *shannon* difusi-konfusi dengan peningkatan nilai *avalance effect* dan juga prinsip *iterated cipher* berdasarkan peningkatan nilai *avalanche effect*.

Kata Kunci : Prinsip Shannon(Konfusi dan Difusi), Konstanta Bilangan Prima, Avelance effect, Anyaman Rambut Papua

---

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