Perancangan Kriptografi Block Cipher Berbasis Pada Teknik Formasi Permainan Bola

[1]Fredly Dick Paliama, [2]Alz Danny Wowor
Fakultas Teknologi Informasi
Universitas Kristen Satya Wacana
Jl. Diponegoro 52-60, Salatiga 50711, Indonesia
Email: [1)]fredlydickpaliama@yahoo.com, [2)], alzdanny.wowor@staff.uksw.edu

Abstract

Cryptography plays an important role in the security of the data or information. On the other hand, many cryptographic been solved by cryptanalyst, so that vital information may become unsafe. Creating a block cipher algorithm is to replace the old algorithm also to improve messaging security. In this research, to design a cryptographic cipher block using the technique of football games as pattern formation randomization in plaintext. in the encryption and decryption process is designed twelve rounds to get the ciphertext and plaintext after XOR-ed with a key that has been regenerated. the avalanche effect refers to a desirable property of cryptographic algorithms, typically block ciphers and cryptographic hash functions. When an input is changed slightly, the output changes significantly. In the case of high-quality block ciphers, such a small change in either the key or the plaintext should cause a drastic change in the ciphertext.
Keywords: *block cipher, cryptography, symmetric key, groove formation technique of football games, ASCII*

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. Membuat algoritma cipher blok adalah untuk menggantikan algoritma yang lama juga untuk memperbaiki kemanan pesan. Dari penelitain ini, untuk merancang sebuah kriptografi block cipher menggunakan teknik formasi permainan bola sebagai pola pengacakan pada plainteks. proses enkripsi dan dekripsi dirancang sebanyak dua belas putaran untuk mendapatkan cipherteks dan plainteks setelah di-XOR dengan kunci yang sudah diregenerasi. Avalanche efek mengacu pada properti yang diinginkan dari algoritma kriptografi, biasanya blok cipher dan fungsi hash kriptografi. ketika sebuah input berubah sedikit, perubahan output yang signifikan. Dalam kasus cipher blok berkualitas tinggi, seperti perubahan kecil di kunci atau plaintext harus menyebabkan perubahan drastis dalam ciphertext.
Kata Kunci : *block cipher, kriptografi, kunci simetris, alur teknik formasi permainan bola,* ASCII

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