# Identifikasi Nilai Keacakan berdasarkan Reposisi Fungsi XOR pada Blok Pertama LFSR A5/1

Artikel Ilmiah

**Diajukan kepada**
**Fakultas Teknologi Informasi**
**untuk memperoleh gelar Sarjana Komputer**

Peneliti:
Ayub Susilo Wibowo (672019150)
Alz Danny Wowor, S.Si., M.Cs.

**Program Studi Teknik Informatika**
**Fakultas Teknologi Informasi**
**Universitas Kristen Satya Wacana**
**Salatiga**
**2022**

# Surat Pernyataan

Artikel Ilmiah berikut ini :

| | | |
|---|---|---|
| Judul | : | Identifikasi Nilai Keacakan berdasarkan Reposisi Fungsi XOR pada Blok Pertama LFSR A5/1 |
| Pembimbing | : | Alz Danny Wowor, S.Si., M.Cs |

adalah benar hasil karya saya :

| | | |
|---|---|---|
| Nama | : | Ayub Susilo Wibowo |
| NIM | : | 672019150 |

Di dalam tugas akhir ini tidak terdapat keseluruhan atau sebagian tulisan atau gagasan orang lain yang saya ambil dengan cara menyalin atau meniru dalam bentuk rangkaian kalimat atau gambar serta simbol yang saya aku seolah-olah sebagai karya saya tanpa memberikan pengakuan pada penulis atau sumber aslinya.
Pernyataan ini dibuat dengan sebenar-benarnya sesuai dengan ketentuan yang berlaku dalam penulisan karya ilmiah.

Salatiga, 27 November 2023

Ayub Susilo Wibowo

# Identifikasi Nilai Keacakan berdasarkan Reposisi Fungsi XOR pada Blok Pertama LFSR A5/1

Ayub Susilo Wibowo [1], Alz Danny Wowor[2]

Program Studi Teknik Informatika, Fakultas Teknologi Informasi,
Universitas Kristen Satya Wacana,
Jl. Dr. O. Notohamidjojo No 1-10, Salatiga 50714, Jawa Tengah

email: [1]672019150@student.uksw.edu, [2]alzdanny.wowor@uksw.edu



**Abstrak**

Penelitian ini merancang proses pembangkitan bilangan acak, menggunakan pendekatan LFSR dengan skema A5/1 pada tiga fungsi umpan balik. XOR digunakan sebagai operasi dalam menentukan nilai keluaran bit baru terhadap iterasi berikutanya pada fungsi umpan balik. *Runs Test*, *Mono Bit*, dan *Block bit*, digunakan bahan uji dalam menghasilkan keluaran acakan terhadap suatu inputan. Penggunaan tiga fungsi umpan balik di gunakan dalam pengujian, perbanding terhadap penelitian terdahulu yang menghasilkan bilangan acak. Pada uji enkripsi plainteks serta cipherteks menunjukan tingkat korelasi ”Sangat Kecil” dan ”Kecil” dengan nilai rata-rata yang mendekati 0. Penggunaan LFSR skema A5/1 dengan tiga fungsi XOR, menghasilkan keluaran yang acak serta dapat digunakan terhadap *Stream Chiper*

**Kata Kunci:** *Skema A5/1, Stream Cipher, Linear Feedback Shift Register.*

**Abstract**

*The study designed the process of generating random numbers, using the LFSR approach with the A5/1 scheme on three feedback functions. XOR is used as an operation in determining the value of the new bit output against the following iteration on the feedback function. Test runs, Mono Bit, and Block Bi, use test materials in producing random outputs against an input. The use of three feedback functions was used in testing, compared to previous research that produced random numbers. In the encryption test, plaintext and ciphertext show correlation levels of ”very small” and ”small” with an approximate average value of 0. Using the A5/1 scheme LFSR with three XOR functions, results in random outputs and can be used against Stream Chiper*.

**Keywords:** *Skema A5/1, Stream Cipher, Linear Feedback Shift Register.*

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

[2]Pengajar Fakultas Teknologi Informasi, Universitas Kristen Satya Wacana, Salatiga