

# **Optimasi Pembangkit Bilangan Acak Dengan Fungsi Polinomial Dan Kombinasi Metode Iterasi**

**JURNAL**

**Diajukan Kepada Program Studi S1 Teknik Informatika**

**Fakultas Teknologi Informasi**

**Guna Memperoleh Gelar Sarjana Komputer**

Repositori Institusi | Universitas Kristen Satya Wacana  
repository.uksw.edu



**Oleh:**

**Siska Angelina  
672020123**

**PROGRAM STUDI S1 TEKNIK INFORMATIKA  
FAKULTAS TEKNOLOGI INFORMASI  
UNIVERSITAS KRISTEN SATYA WACANA  
SALATIGA  
2024**

## Lembar Pengesahan

Judul Artikel : Optimasi Pembangkit Bilangan Acak Dengan Fungsi  
Polinomial Dan Kombinasi Metode Iterasi  
Nama Mahasiswa : Siska Angelina  
NIM : 672020123  
Program Studi : Teknik Informatika  
Fakultas : Teknologi Informasi

Menyetujui,



Alz Danny Wowor, S.Si., M.Cs.  
Pembimbing



Prof. Ir. Daniel H. F. Manongga, M.Sc., Ph.D.  
Dekan



Budhi Kristianto, S.Kom., M.Sc., Ph.D.  
Ketua Program Studi

Dinyatakan Lulus Proses Review Tanggal : (tanggal review)

Reviewer :

- Magdalena A. Ineke Pakereng, M.Kom.



# Pernyataan

Yang bertandatangan di bawah ini,

Nama : Siska Angelina

NIM : 672020123

Program Studi : S1 Teknik Informatika

Fakultas : Fakultas Teknologi Informasi, Universitas Kristen Satya Wacana

menyatakan dengan sesungguhnya bahwa tugas akhir dengan judul:

**Optimasi Pembangkit Bilangan Acak Dengan Fungsi Polinomial Dan Kombinasi**

**Metode Iterasi**

yang dibimbing oleh:

1. Alz Danny Wowor, S.Si., M.Cs.

adalah benar hasil karya saya.

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 akui seolah-olah sebagai karya saya tanpa memberikan pengakuan pada penulis atau sumber aslinya.

Jakarta, 16 Mei 2024



Siska Angelina

# Optimasi Pembangkit Bilangan Acak Dengan Fungsi Polinomial Dan Kombinasi Metode Iterasi

Siska Angelina <sup>1</sup>, Alz Danny Wowor<sup>2</sup>

Program Studi Teknik Informatika, Fakultas Teknologi Informasi,  
Universitas Kristen Satya Wacana,  
Jl. Dr. O. Notohamidjojo No 1-10, Salatiga 50714, Jawa Tengah  
email: <sup>1</sup>672020123@student.uksw.edu, <sup>2</sup>alzdanny.wowor@uksw.edu

## Abstrak

Penelitian ini menggunakan fungsi polinomial dan memadukan metode iterasi untuk menghasilkan bilangan acak. Simulasi dengan nilai awal  $x_0 = -1.4$  yang memiliki nilai optimal dan menghasilkan empat nilai yang dapat dijadikan kunci. Hasil visual merepresentasikan bahwa setiap kumpulan data menghasilkan bentuk grafik yang *chaotic* dan diasumsikan acak berdasarkan uji statistik yaitu *run test*, *mono bit* dan *block bit*. Setiap nomor acak yang dihasilkan melewati uji kriptografi dan dapat menghasilkan plainteks dan cipherteks yang independen secara statistik. Fungsi polinomial terpilih adalah  $(x - (x^2 - 4))/2x$  yang telah terbukti sebagai pembangkit bilangan acak yang efektif dan bisa digunakan untuk memperoleh bilangan acak bersifat CSPRNG berbasis *chaos*

**Kata Kunci:** Fungsi polinomial; Newton Raphson; *Fixed Point Iteration*; CSPRNG Chaos

## Abstract

*This research uses a polynomial function and combines the iteration method to generate random numbers. Simulation with an initial value of  $x_0 = -1.4$  which has an optimal value and produces four values that can be used as keys. The visual results represent that each data set produces a graphical shape that is chaotic and is assumed to be random based on statistical tests namely run test, mono bit and block bit. Each random number generated passes the cryptographic test and can produce statistically independent plaintext and ciphertext. Selected polynomial function is  $(x - (x^2 - 4))/2x$  has been proven to be an effective random number generator and can be used to generate chaos-based CSPRNG random numbers..*

**Keywords:** *Polynomial Function; Newton Raphson; Fixed Point Iteration; CSPRNG Chaos*

---

<sup>1</sup>Mahasiswa Program Studi Teknik Informatika, Fakultas Teknologi Informasi, Universitas Kristen Satya Wacana, Salatiga

<sup>2</sup>Pengajar Fakultas Teknologi Informasi, Universitas Kristen Satya Wacana, Salatiga