KRIPTOGRAFI GAMBAR MENGGUNAKAN ALGORITMA *AFFINE CIPHER* DAN *CRYPTOGRAPHICALLY SECURE PSEUDORANDOM NUMBER GENERATOR* BERBASIS *CHAOS*

SKRIPSI

Diajukan untuk memenuhi sebagian syarat memperoleh gelar Sarjana Matematika

Oleh:

Rajestika Faldela Ramanov

NIM 2004800

PROGRAM STUDI MATEMATIKA

FAKULTAS PENDIDIKAN MATEMATIKA DAN ILMU PENGETAHUAN ALAM

UNIVERSITAS PENDIDIKAN INDONESIA

2024

LEMBAR HAK CIPTA

KRIPTOGRAFI GAMBAR MENGGUNAKAN ALGORITMA *AFFINE CIPHER* DAN *CRYPTOGRAPHICALLY SECURE PSEUDORANDOM NUMBER GENERATOR* BERBASIS *CHAOS*

Oleh:
Rajestika Faldela Ramanov
2004800

Diajukan untuk memenuhi sebagian syarat memperoleh gelar Sarjana Matematika pada Program Studi Matematika Fakultas Pendidikan Matematika dan Ilmu Pengetahuan Alam

LEMBAR PENGESAHAN

RAJESTIKA FALDELA RAMANOV

KRIPTOGRAFI GAMBAR MENGGUNAKAN ALGORITMA *AFFINE CIPHER* DAN *CRYPTOGRAPHICALLY SECURE PSEUDORANDOM NUMBER GENERATOR* BERBASIS *CHAOS*

Disetujui dan disahkan,

Pembimbing I

Dra. Hj. Rini Marwati, M.S.
NIP. 196606251990012001

Pembimbing II

Ririn Sispiyati, M.Si.
NIP. 198106282005012001

Mengetahui,

Ketua Program Studi Matematika

Dr. Kartika Yulianti, M.Si.
NIP. 198207282005012001

ABSTRAK

Kriptografi dapat mengamankan informasi dengan menyandikan (enkripsi) sehingga informasi menjadi tidak terbaca. Pada penelitian ini, kriptografi diterapkan pada gambar menggunakan algoritma *Affine Cipher* dengan memanfaatkan pembangkit bilangan acak *CSPRNG* berbasis *Chaos* sebagai kunci-kunci yang digunakan *Affine Cipher*. Pemanfaatan pembangkit bilangan acak diharapkan memberikan peningkatan keamanan dalam hal kualitas enkripsi. Implementasi ini dilakukan menggunakan program aplikasi yang juga digunakan untuk validasi bahwa gambar yang telah dienkripsi dapat dikembalikan seperti semula (dekripsi). Selain itu, analisis kualitas penyandian dilakukan untuk mengetahui peningkatan kualitas enkripsi *Affine Cipher* dengan dan tanpa memanfaatkan *CSPRNG* berbasis *Chaos*. Hasil dari penelitian ini menunjukkan bahwa algoritma kriptografi dapat diterapkan pada gambar, validasi berhasil dilakukan, dan pemanfaatan *CSPRNG* berbasis *Chaos* pada *Affine Cipher* secara signifikan meningkatkan kualitas enkripsi gambar.

Kata Kunci: Kriptografi, Kriptografi Gambar, *Affine Cipher*, *CSPRNG* berbasis *Chaos*

ABSTRACT

Cryptography can secure information by encrypting it so that it becomes unreadable.. In this research, cryptography is applied to images using Affine Cipher algorithm by utilizing Chaos-based CSPRNG random number generator as the keys used by Affine Cipher. The utilization of random number generator is expected to provide increased security in terms of encryption quality. This implementation is done using an application program that is also used for validation that the encrypted image can be restored to its original state (decryption). In addition, encryption quality analysis was conducted to determine the improvement of Affine Cipher encryption quality with and without utilizing Chaos-based CSPRNG. The results of this research show that the cryptographic algorithm can be applied to images, validation is successfully performed, and the utilization of Chaos-based CSPRNG on Affine Cipher significantly improves the image encryption quality.

Keywords: *Cryptography, Image Cryptography, Affine Cipher, Chaos-based CSPRNG*

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

DAFTAR LAMPIRAN

DAFTAR PUSTAKA

Burton, D. M (2010). *Elementary Number Theory.* New York: McGraw-Hill.

Dhruv, A. J., Patel, R., & Doshi, N. (2021). Python: The Most Advanced Programming Language for Computer Science Applications. *Science and Technology Publications, Lda*, 292-299. doi: 10.5220/0010307900003051

Irwansyah, E. & Moniaga, J. V. (2014). *Pengantar Teknologi Informasi*. Yogyakarta: Deepublish.

Menezes, A. J., van Oorschot, P. C., & Vanstone, S. A. (2001). *Handbook of Applied Cryptography.* Amerika Serikat: CRC Press.

Munir, R. (2019). *Kriptografi Edisi Kedua*. Bandung: Penerbit INFORMATIKA.

Naufal, M. F., Marwati, R., & Sispiyati, R. (2021). Kriptografi Audio Menggunakan Transposisi dan Affine Cipher yang Dikembangkan dengan Algoritma Blum Blum Shub. *Jurnal EurekaMatika*, 9(1), 1-14.

Nurul, S., Anggrainy, S., & Aprelyani, S. (2022). Faktor-Faktor Yang Mempengaruhi Keamanan Sistem Informasi: Keamanan Informasi, Teknologi Informasi Dan Network (Literature Review SIM). *Jurnal Ekonomi Manajemen Sistem Informasi*, *3*(5), 564—573. doi: https://doi.org/10.31933/jemsi.v3i5

Stinson, D. R. (2006). *Cryptography Theory and Practice Third Edition*. Boca Raton: Chapman & Hall/CRC.

Sulistiyanti, S. R., Setyawan FX. A., & Komarudin, M. (2016). *Pengolahan Citra Dasar dan Contoh Penerapannya.* Yogyakarta: Teknosain.

Wu, Y., Yang, G., Jin, H., & Noonan, J. P. (2012). Image Encryption using the Two-dimensional Logistic Chaos Map. *Journal of Electronic Imaging. 21*(1). 1—29 doi: 10.1117/1.JEI.21.1.013014

Zelvian, M. R. (2023). *Kriptografi Gambar dengan Menggunakan Algoritma Blowfish*. Universitas Pendidikan Indonesia, Bandung