# Implementasi Kriptografi Hibrida *Blum Blum Shub*-Vernam *Cipher* dan Merkle-Hellman *Knapsack* dalam Penyandian Pesan Teks disertai Pengujian *Avalanche Effect*

**SKRIPSI**

Diajukan untuk memenuhi sebagian syarat untuk memperoleh gelar

Sarjana Matematika


Oleh:

IRFAN MAULANA YUSUF SUTRISNO

2103203

**PROGRAM STUDI MATEMATIKA**

**FAKULTAS PENDIDIKAN MATEMATIKA DAN ILMU PENGETAHUAN ALAM**

**UNIVERSITAS PENDIDIKAN INDONESIA**


**2025**

# LEMBAR HAK CIPTA

## Implementasi Kriptografi Hibrida *Blum Blum Shub*-Vernam *Cipher* dan Merkle-Hellman *Knapsack* dalam Penyandian Pesan Teks disertai Pengujian *Avalanche Effect*

Oleh

Irfan Maulana Yusuf Sutrisno
NIM 2103203

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

**LEMBAR PENGESAHAN**

IRFAN MAULANA YUSUF SUTRISNO

IMPLEMENTASI KRIPTOGRAFI HIBRIDA *BLUM BLUM SHUB*-VERNAM *CIPHER* DAN MERKLE HELLMAN *KNAPSACK* DALAM PENYANDIAN PESAN TEKS DISERTAI PENGUJIAN *AVALANCHE EFFECT*

Disetujui dan disahkan,

Pembimbing I

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

Pembimbing II,

**Isnie Yusnitha, Ph.D.**
**NIP. 198506092012122002**

Mengetahui,

Ketua Program Studi Matematika

**Dr. Kartika Yulianti, M.SI.**
**NIP. 198207282005012001**

# ABSTRAK

Dalam era digital, pertukaran informasi rahasia melalui jaringan komputer menjadi kebutuhan yang tak terhindarkan. Untuk menjaga kerahasiaan dan integritas informasi tersebut, penelitian ini mengimplementasi kriptografi hibrida Vernam *Cipher* dengan Merkle-Hellman *Knapsack*. Vernam *Cipher* adalah kriptografi simetris yang dikenal aman, namun memiliki kelemahan yaitu panjang kunci yang digunakan harus sama dengan panjang pesan atau plainteks, sehingga digunakan pembangkit bilangan acak *Blum Blum Shub* untuk menghasilkan kunci Vernam. Sedangkan Merkle-Hellman *Knapsack* adalah kriptografi asimetris yang bergantung pada sulitnya memecahkan *Knapsack problem*. Merkle-Hellman *Knapsack* digunakan untuk mengenkripsi kunci Vernam. Sistem hibrida ini dirancang untuk mengamankan baik pesan maupun kunci yang digunakan. Kinerja keamanan dari setiap kriptografi diuji menggunakan pengujian *Avalanche Effect*. Pengujian *Avalanche Effect* memanfaatkan perubahan setiap bit yang terjadi pada cipherteks. Hasil pengujian menunjukkan bahwa kombinasi *Blum Blum Shub* dan Vernam *Cipher* memberikan perubahan yang signifikan pada cipherteks, sementara Merkle-Hellman *Knapsack* memberikan dasar matematis yang kuat untuk keamanan sistem. Program aplikasi dibuat dengan menggunakan *Graphical User Interface* (GUI) dalam bahasa pemograman *Python*.

**Kata Kunci**: *Avalanche Effect*, *Blum Blum Shub*, Kriptografi Hibrida, Merkle-Hellman *Knapsack*, *Python*, Vernam *Cipher*.

# *ABSTRACT*

*In the digital era, the exchange of confidential information through computer networks has become an inevitable need. To maintain the confidentiality and integrity of the information, this research implements a hybrid cryptography of Vernam Cipher with Merkle-Hellman Knapsack. Vernam Cipher is a symmetric cryptography that is known to be secure, but has the disadvantage that the key length used must be the same as the length of the message or plaintext, so the Blum Blum Shub random number generator is used to generate the Vernam key. Meanwhile, Merkle-Hellman Knapsack is an asymmetric cryptography that depends on the difficulty of breaking the Knapsack problem. Merkle-Hellman Knapsack is used to encrypt the Vernam key. This hybrid system is designed to secure both the message and the key used. The security performance of each cryptography is tested using Avalanche Effect testing. Avalanche Effect testing utilizes each bit change that occurs in the ciphertext. The results show that the combination of Blum Blum Shub and Vernam Cipher provides significant changes to the ciphertext, while Merkle-Hellman Knapsack provides a strong mathematical basis for system security. The application program was created using Graphical User Interface (GUI) in Python programming language.*



**Kata Kunci**: *Avalanche Effect, Blum Blum Shub, Hybrid Cryptography, Merkle-Hellman Knapsack, Python, Vernam Cipher*.

# DAFTAR ISI

# DAFTAR GAMBAR

# DAFTAR TABEL

# DAFTAR PUSTAKA


Aghniya, R. D. R., dkk (2019). Kriptografi dengan Mengkomposisikan Vigenere *Cipher* dan Algoritma *Knapsack* Merkle-Hellman. Jurnal EurekaMatika, 7(2), 52-62.

Akmal, D. A., Dhani, D. M., & Syahila, F. (2024). Kombinasi Kriptografi Modern Dalam Keamanan Pesan Teks. Saturnus : Jurnal Teknologi Dan Sistem Informasi, *2*(3), 119–128. https://doi.org/10.61132/saturnus.v2i3.204.

Amalya, N., dkk. (2023). Kriptografi dan Penerapannya Dalam Sistem Keamanan Data. Jurnal Media Informatika, 4(2), 90-93.

Ariyus, D. (2008). Pengantar Ilmu Kriptografi Teori Analisis dan Implementasi. Andi: Yogyakarta.

Burton, D. (2011). Elementary Number Theory. McGraw Hill.

Camreon, P. J. (2003). *Notes on Crypthography*. London: Queen Mary, University of london

Feistel, H. (1973). Cryptography and computer privacy. Scientific american, 228(5), 15-23.

Menezes, A. J., Oorschot, P. C., & Vanstone, S. A. (1996). *Handbook of Applied Cryptography*. CRC Press.

Munir, R. (2019). Kriptografi Edisi Kedua. Bandung: Informatika Bandung.

Muslih & Handoko, L. B (2022). Pengujian Avalanche Effect pada Kriptografi Teks Menggunakan Autokey Cipher. STEKOM, 2(1)

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.

Pratiwi, R., dkk(2022). Bulletin of Information Technology (BIT) Perancangan Keamanan Data Pesan Dengan Menggunakan Metode Kriptografi Caesar Cipher. Jurnal BIT, *3*(4), 367–373. https://doi.org/10.47065/bit.v3i1

Rosen, K. H. (1984). *Elementary number theory and its applications*. Addison Wesley Pub. Co.

Saputra, M. W., Sapitri, A., & Putri, M. A. (2023). Penerapan Kriptosistem Hibrida Untuk Mengenkripsi Pesan Menggunakan Algoritma RSA *Cipher*. *Journal science Informatica and Robotics*, 1(1), 10-21

Sari, D. R., & Pawelloi, A. I. (2022). Penerapan Kriptografi Pada File Teks dengan Menggunakan Merkle-Hellman Knapsack Berbasis Android. Jurnal Sintaks Logika, 2(3), 1-10.

Sianturi, C. F. (2020). Modifikasi Pembangkit Kunci Algoritma RSA Dengan Menerapkan Algoritma Blum Blum Shub (BBS). *Technology and Science BITS*, *2*(1), 39–43.

Silitonga, P. D. P., & Pakpahan, S. (2021). *Application of Integers in Vernam Cipher Cryptography* (*One Time Pad*). JURNAL INFOKUM, 9(2), 350-353. http://infor.seaninstitute.org/index.php/infokum/index

Stallings, W. (2005). *Cryptography and Network Security Principles and Practices (4 ed.).Prentice Hall.*

Stinson, D. R. & Rosen, K.H. (Penyunting). (2006). *Criptography: Theory and Practice*. 3rd Ed. Chapman & Hall/CRC: Ontario

Suhardi. (2016). Algoritma Kriptografi Data Sederhana dengan Metode *Exclusive OR* (XOR). Jurnal Teknovasi, 03(2), 23-31.

Tornea, O., Dkk. (2011). DNA Vernam Cipher. Proc. 3rd Int.Conf. E-Health Bioeng.

Wardini, K. (2024). Kriptografi Hibrida *Atbash, Autokey Cipher*, dan Algoritma El Gamal dalam Pengamanan Pesan Teks dan Pengujian *Avalanche Effect*.

Wantah, M. F. A., dkk (2023). Analisis Penggunaan Bahasa Pemrograman *Python* Untuk Materi Kalkulus Limit. Jurnal Matematika, Fisika, Algoritma dan Sains, 1(1), 100-105.