

**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

©Irfan Maulana Yusuf Sutrisno

Universitas Pendidikan Indonesia

Juli 2025

Hak Cipta dilindungi Undang-Undang

Skripsi ini tidak boleh diperbanyak seluruhnya atau sebagian dengan dicetak
ulang, difotocopi, atau cara lainnya tanpa izin penulis

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,



Isniet 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 pemrograman *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

LEMBAR HAK CIPTA.....	i
LEMBAR PENGESAHAN	ii
LEMBAR PERNYATAAN	ii
KATA PENGANTAR.....	iv
UCAPAN TERIMA KASIH	v
ABSTRAK	vi
<i>ABSTRACT</i>	vii
DAFTAR ISI.....	viii
DAFTAR GAMBAR.....	x
DAFTAR TABEL	xi
BAB 1 PENDAHULUAN	1
1.1 Latar Belakang.....	1
1.2 Rumusan Masalah	4
1.3 Tujuan Penelitian	4
1.4 Manfaat Penelitian.....	4
BAB II KAJIAN PUSTAKA	5
2.1 Teori Dasar Matematika	5
2.2 Kriptografi	6
2.2.1 Istilah dalam Kriptografi	6
2.2.2 Kriptosistem	7
2.2.3 Teori <i>Coding</i>	8
2.3 Vernam <i>Cipher</i>	9
2.4 <i>Pseudo Random Number Generator</i>	10
2.5 <i>Blum-Blum Shub</i>	11
2.6 Algoritma Merkle-Hellman <i>Knapsack</i>	12
2.6.1 <i>Knapsack Problem</i>	12
2.6.2 <i>Superincreasing Knapsack</i>	12
2.7 Pengujian Avalanche Effect	14
2.8 <i>Python</i>	15
BAB III METODOLOGI PENELITIAN	16
3.1 Identifikasi Masalah	16
3.2 Model Dasar	16
3.3 Pengembangan Model Dasar	18

3.4	Konstruksi Program.....	19
3.4.1	Input dan Output	20
3.4.2	Algoritma Deskriptif	20
3.4.3	Rancangan Tampilan Program	22
3.4.4	<i>Library Python</i>	25
3.5	Proses Validasi.....	26
3.6	Penarikan Kesimpulan.....	26
BAB IV	HASIL DAN PEMBAHASAN.....	27
4.1	Skema Kriptografi Hibrida <i>Blum Blum Shub-Vernam Cipher</i> dan Merkle Hellman <i>Knapsack</i> dan Pengujian <i>Avalanche Effect</i>	27
4.2	Pseudocode Program	29
4.2.1	Pseudocode Pembangkitan Kunci	30
4.2.2	Pseudocode Enkripsi	30
4.2.3	Pseudocode Dekripsi	34
4.2.4	Pseudocode Pengujian <i>Avalanche Effect</i>	36
4.3	Tampilan Program	39
4.3.1	<i>Menu</i> 'Pembangkitan Kunci'	40
4.3.2	<i>Menu</i> 'Enkripsi'	41
4.3.3	<i>Menu</i> 'Dekripsi'	42
4.3.4	<i>Menu</i> 'Uji AE'	42
4.4	Validasi Program	44
4.4.1	Validasi Pembangkitan Kunci pada Program	44
4.4.2	Validasi Enkripsi pada Program	45
4.4.3	Validasi Dekripsi pada Program.....	47
4.4.4	Validasi Uji <i>Avalanche Effect</i> pada Program.....	48
4.4.5	Perbandingan Nilai Uji <i>Avalanche Effect</i>	49
BAB V	KESIMPULAN DAN SARAN	51
5.1	Kesimpulan.....	51
5.2	Saran.....	52
DAFTAR PUSTAKA		53
LAMPIRAN		55

DAFTAR GAMBAR

Gambar 2.1: Skema Kriptografi Sederhana	8
Gambar 3.1: Skema Algoritma Vernam <i>Cipher</i>	17
Gambar 3.2: Skema Merkle-Hellman <i>Knapsack</i>	18
Gambar 3.3: Skema Model Penggabungan	19
Gambar 3.4: Rancangan Tampilan Utama.....	22
Gambar 3.5: Rancangan Tampilan Pembangkitan Kunci.....	22
Gambar 3.6: Rancangan Tampilan Enkripsi.....	23
Gambar 3.7: Rancangan Tampilan Dekripsi	23
Gambar 3.8: Rancangan Tampilan Pengujian Vernam Cipher	24
Gambar 3.9: Rancangan Tampilan Pengujian Vernam Cipher dan BBS.....	24
Gambar 3.10: Rancangan Tampilan Pengujian Merkle-Hellman Knapsack	25
Gambar 4.1: Skema Kriptografi Hibrida <i>Blum Blum Shub</i> -Vernam <i>Cipher</i> dan Merkle Hellman <i>Knapsack</i>	27
Gambar 4.2: Skema Pengujian <i>Avalanche Effect</i> pada Kriptografi Vernam <i>Cipher</i>	28
Gambar 4.3: Skema Pengujian <i>Avalanche Effect</i> pada Kriptografi <i>Blum Blum Shub</i> Vernam <i>Cipher</i>	28
Gambar 4.4: Skema Pengujian <i>Avalanche Effect</i> pada Kriptografi Merkle-Hellman <i>Knapsack</i>	28
Gambar 4.5: Menu Utama	39
Gambar 4.6: Menu Panduan	40
Gambar 4.7: Menu Pembangkitan Kunci	40
Gambar 4.8: Menu Enkripsi.....	41
Gambar 4.9: Menu Dekripsi	42
Gambar 4.10: Menu Vernam <i>Cipher</i>	43
Gambar 4.11: Menu Vernam <i>Cipher</i> + BBS.....	43
Gambar 4.12: Menu Merkle-Hellman.....	44

DAFTAR TABEL

Tabel 2.1: Tabel ASCII.....	9
Tabel 2.2: Contoh Solusi <i>Superincreasing Knapsack</i>	13
Tabel 3.1: Tabel Input dan Output	20
Tabel 4.1: Tabel Enkripsi Vernam <i>Cipher</i>	46
Tabel 4.2: Tabel Enkripsi Merkle-Hellman <i>Knapsack</i>	46
Tabel 4.3: Tabel Dekripsi Merkle-Hellman <i>Knapsack</i>	48
Tabel 4.4: Tabel Dekripsi Vernam <i>Cipher</i>	48
Tabel 4.5: Tabel Pengujian <i>Avalanche Effect</i>	49
Tabel 4.6: Tabel Perbandingan Nilai <i>Avalanche Effect</i>	50

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 Cryptography*. 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.