Judul Artikel: Adopsi Pembangkit Kunci Blum Blum Shub dan Bilangan Euler Pada Algoritma Extended Vigenere

1.Sitasi artikel:

Ardianto,E.,Handoko,W.T.,Lestariningsih,E.,& Sutanto,F.A. (2023*).Adopsi Pembangkit Kunci Blum-Blum Shub dan Bilangan Euler Pada Algoritma Extended Vigenere.Halaman 41-48.*

2.Latar Belakang & Tujuan:

Kebutuhan akan keamanan data dalam komunikasi digital terus meningkat, mendorong pengembangan metode kriptografi yang lebih kuat. Algoritma Vigenerik klasik meskipun lebih baik dari Caesar cipher masih rentan terhadap analisis frekuensi.Extended Vigenere Algoritma berupaya meningkatkan keamanan, namun kekuatan utamanya sangat bergantung pada kualitas kunci. Artikel ini menunjukkan untuk meningkatkan kekuatan Algoritma Extended Vigenere dengan mengintegrasikan pembangkit kunci Belum Belum Shub (BBS) untuk menghasilkan deret kunci yang acak dan aman, serta memanfaatkan bilangan Euler untuk memperkuat proses enkripsi atau manajemen kunci, dengan harapan dapat menciptakan sistem kriptografi yang lebih resisten terhadap serangan.

3.Metode:

Penelitian ini mengusulkan metode hibrida yang menggabungkan pembangkit kunci Belum Belum Shub (BBS) dan bilangan Euler ke dalam Algoritma Extended Vigenere. Proses dimulai dengan generasi kunci menggunakan BBS, sebuah generator bilangan pseudo-acak kriptografi yang dikenal karena keamanannya yang tinggi, tergantung pada properti bilangan prima besar.Bilangan Euler (fungsi totient Euler) Kemudian diintegrasikan, kemungkinan untuk memperluas ruang kunci, memodulasi proses enkripsi, atau bahkan dalam pemilihan parameter awal untuk BBS, sehingga menghasilkan kunci yang lebih kompleks dan sulit diprediksi. Kunci yang dihasilkan ini kemudian digunakan dalam proses enkripsi Extended Vigenere, yang mengaplikasikan operasi modular pada setiap karakter plaintext dengan karakter kunci yang sesuai, namun dengan rentang karakter yang

lebih luas (misalnya,256 karakter ASCII) dibandingkan vinere klasik. Implementasi melibatkan langkah-langkah seperti inisialisasi parameter BBS generasi deret bilangan acak penerapan fungsi Euler dan akhirnya proses substitusi polialfabetik menggunakan Extended Vigenere.

4.Hasil/Temuan Kunci:

Hasil penelitian ini diharapkan menunjukkan peningkatan signifikan dalam keamanan Algoritma Extended Vigenere. Integrasi BBS menghasilkan deret kunci yang memiliki sifat keanjakan yang sangat baik, sehingga mempersulit upaya kriptanalisis berbasis statistik. Pemanfaatan Bilangan Euler lebih lanjut memperumit hubungan antara plaintext,kunci, dan ciphertext, meningkatkan kompleksitas matematis algoritma. Uji coba performa dan keamanan seperti uji statistik ke ancakan (misalnya,NIST SP 800-22) dan analisis kompleksitas, kemungkinan menunjukkan bahwa sistem yang diusulkan lebih tahan terhadap serangan brute-force dan analisis frekuensi dibandingkan Extended Vigenere tanpa modifikasi. Meskipun demikian, mungkin terdapat kompromi dalam hal kecepatan komputasi karena kompleksitas tambahan dari generasi kunci BBS dan perhitungan Euler.

5.Kontribusi & Keterbatasan:

Kontribusi utama dari penelitian iIni membuka jalan bagi pengembangan sistem keamanan data yang lebih robust. Namun penelitian ini mungkin Memiliki keterbatasan, seperti kompleksitas implementasi yang lebih tinggi,kebutuhan akan komputasi yang lebih intensif untuk generasi kunci dan enkripsi/deskripsi, serta potensi kerentanan baru yang mungkin muncul dari interaksi antara ketiga komponen yang belum sepenuhnya dieksplorasi. Selain itu, skalabilitas untuk data yang sangat besar juga bisa menjadi tantangan.

6.Takeawai:

Artikel ini memberikan pelajaran berharga tentang bagaimana kombinasi cerdas dari berbagai konsep kriptografi dapat meningkatkan keamanan sistem yang sudah ada.Untuk praktik atau proyek, ini menunjukkan pentingnya memilih generator kunci yang kuat dan memahami dasar-dasar teori bilangan untuk merancang algoritma enkripsi yang lebih aman dan efisien.