Meningkatkan Keamanan Data Menggunakan Super Enkripsi Kombinasi *Rail Fence* dan *Vigenere Autokey*

Nabil Syahfiar dan Eka Ardhianto

Program Studi Teknik Informatika, Fakultas Teknologi Informasi dan Industri,
Universitas Stikubank Semarang,
Jl. Tri Lomba Juang No.1, Semarang
Email :nabilsyahfiar@mhs.unisbank.ac.id, ekaardhianto@edu.unisbank.ac.id

Abstrak

Pentingnya data di era digital ini membuat banyaknya ancaman dan resiko dari pembobolan data. Oleh karenanya, dibutuhkan suatu protokol keamanan untuk menjaga data tersebut. Penggunaan kriptografi merupakan salah satu solusi dari permasalahan tersebut. Rail Fence Cipher adalah salah satu algoritma kriptografi yang dapat digunakan untuk mengenkripsi suatu data untuk menjaga keamanan data tersebut. Namun penggunaan algoritma Rail Fence Cipher mulai ditinggalkan karena kekuatan keamanannya yang sudah mulai berkurang. Dengan melakukan konsep super enkripsi, algoritma Rail Fence Cipher yang dikombinasikan dengan algoritma Vigenere Autokey dapat menambah kekuatan keamanan dengan sangat signifikan. Hal tersebut dibuktikan dengan peningkatan nilai entropi dari rata-rata 4,9722 menjadi 7,1418 dimana peningkatan tersebut mencapai 43,84%. Selain menggunakan entropi, pengujian menggunakan avalanche effect juga menunjukkan peningkatan yang sangat signifikan. Nilai avalanche effect menggunakan algoritma tunggal Rail Fence hanya memperoleh rata-rata 36,03% dibandingkan penggunaan konsep super enkripsi yang mencapai 56,41%. Dengan peningkatan nilai entropi dan avalanche effect yang sangat signifikan tersebut, maka kekuatan keamanan dari konsep super enkripsi dipastikan meningkat jauh jika dibandingkan dengan penggunaan algoritma kriptografi tunggal.

Kata kunci :Rail Fence, Autokey, Super Enkripsi, Entropi, *Avalanche Effect*

Pendahuluan

Data merupakan elemen penting di era digital ini. Menjaga data adalah salah satu tantangan yang berat karena banyaknya ancaman dan resiko. Berbagai kasus pencurian dan pembobolan data terjadi akibat kurangnya protokol keamanan data yang dimiliki [1]. Karena itu, dibutuhkan suatu protokol keamanan untuk melindungi data agar tidak disalah gunakan oleh pihak yang tidak berwenang. Kriptografi adalah salah satu teknik pengamanan data yang banyak digunakan saat ini [2]. Kriptografi merupakan cabang ilmu yang bertujuan untuk mengamankan sebuah informasi dengan mengacak informasi tersebut sehingga tidak dapat dipahami oleh pihak yang tidak berwenang. Dalam kriptografi ada dua jenis teknik yang populer digunakan, yaitu algoritma kriptografi dengan teknik subtitusi dan algoritma kriptografi dengan teknik transposisi [3].

Rail Fence Cipher merupakan salah satu algoritma kriptografi yang menggunakan teknik transposisi. Rail Fence Cipher menggunakan teknik transposisi berbasis level atau baris dan nilai baris dari algoritma ini disebut kunci yang digunakan untuk proses enkripsi dan dekripsi. Algoritma ini bekerja dengan cara mengacak urutan huruf-huruf pesan dengan mengubah posisi karakter dalam plaintext. Proses enkripsi melibatkan penulisan plaintext secara vertikal ke bawah sepanjang n baris, dimulai dari baris atas dan kemudian turun ke baris berikutnya. Ketika mencapai akhir baris, lanjutkan ke baris berikutnya dan seterusnya. Ciphertext dihasilkan dengan membaca karakter secara horizontal dari baris pertama hingga baris terakhir [4].

Vigenere Cipher adalah algoritma kriptografi dengan teknik subtitusi yang menggunakan substitusi cipher monoalphabetic untuk membuat struktur plaintext asli tampak agak kabur dalam ciphertext [5]. Vigenere Autokey adalah salah satu pengembangan dari Vigenere yang karakter plaintextnya digeser ke kanan sesuai dengan kunci yang ditambahkan, berbeda dengan Vigenere yang menambahkan kunci langsung ke pesan yang ingin dienkripsi [6]. Algoritma Vigenere Autokey beroperasi dengan menggunakan sebuah kunci yang sama panjanganya dengan pesan plaintext yang

DOI : http://dx.doi.org/10.32409/jikstik.23.3.3612

dienkripsi. Setiap karakter dari plaintext digabungkan dengan karakter yang sesuai dari kunci untuk menghasilkan ciphertext. Kunci dapat berupa karakter apa saja, namun harus dirahasiakan untuk menjaga keamanan dari ciphertext [7].

Salah satu cara untuk meningkatkan keamanan dari suatu algoritma kriptografi yaitu dengan mengombinasikan dua algoritma. Super enkripsi adalah suatu konsep yang mengombinasikan dua atau lebih algoritma kriptografi untuk meningkatkan keamanan dari algoritma kriptografi yang sudah ada [8], [9]. Pada penelitian sebelumnya disebutkan bahwa algoritma Rail Fence Cipher rentan terhadap serangan brute force karena algoritma Rail Fence Cipher tidak mengubah setiap karakternya, sehingga pola frekuensi karakter plaintext tetap terlihat pada ciphertext [10]. Pada penelitian [11], dijelaskan bahwa penggunaan konsep super enkripsi dapat meningkatkan keamanan hingga 20% daripada menggunakan satu algoritma kriptografi. Selain itu, konsep super enkripsi juga efektif diterapkan pada citra, hasil yang diperoleh dari penggunaan super enkripsi pada citra yaitu citra yang dienkripsi terkesan rusak dan tidak dapat dilihat oleh aplikasi penampil citra [12]. Oleh karena itu, diusulkan konsep super enkripsi yang mengombinasikan algoritma Rail Fence Cipher yang merupakan algoritma dengan teknik transposisi dengan algoritma Vigenere Autokey yang merupakan algoritma dengan teknik subtitusi.

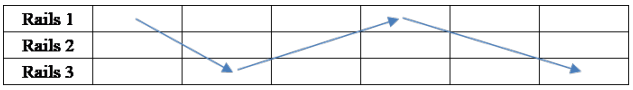
Pada penelitian Implementasi Skema QR-Code dan Digital Signature menggunakan Kombinasi Algoritma RSA dan AES untuk Pengamanan Data Sertifikat Elektronik, penggunaan super enkripsi yang mengombinasikan algoritma kriptografi RSA dan AES serta penggunaan SHA-3 menunjukkan peningkatan yang cukup signifikan. Waktu yang dibutuhkan untuk pemrosesan pada konsep super enkripsi masih relatif sama dibandingkan waktu pemrosesan menggunakan satu algoritma kriptografi saja. Nilai entropi yang dihasilkan dari proses enkripsi terbilang cukup bagus di angka 4,96 yang mana hampir mendekati 8, juga nilai avalanche effect yang mencapai 40,61% yang membuktikan bahwa perubahan karakter pada chipertext sudah lumayan acak [9].

Penelitian Pengamanan Data melalui Model Super Enkripsi Autokey Cipher dan Transposisi Kolom menggunakan kombinasi algoritma kriptografi autokey cipher dan transposisi kolom. Hasil dari kombinasi kedua algoritma kriptografi tersebut dapat memberikan tingkat keamanan yang lebih baik dengan rata-rata nilai avalanche effect mencapai 30,76%. Nilai tersebut meningkat cukup signifikan dibandingkan algoritma kriptografi autokey cipher tunggal yang nilai avalanche effect nya hanya 1,66% dan transposisi kolom yang nilainya sebesar 18,03%. Tingkat akurasi dari proses enkripsi juga terhitung sangat baik mencapai 100%, artinya plaintext awal dengan plaintext hasil dekripsi memiliki bentuk yang sama [1].

Metode Penelitian

Kriptografi merupakan kata yang berasal dari bahasa Yunani “cryptos” yang artinya rahasia, dan “graphien” yang artinya tulisan, jadi kriptografi bisa disebut “tulisan rahasia” [13]. Pada perkembangannya, kriptografi dapat diartikan sebagai cara untuk mengamankan suatu informasi dengan cara menyusun acak informasi tersebut hingga tidak dapat dikenali oleh orang yang tidak berwenang [14]. Tujuan dari kriptografi sendiri adalah memastikan bahwa informasi yang ingin disampaikan hanya dapat diakses oleh orang yang sah atau orang yang mempunyai kewenangan atas informasi tersebut [15].

Rail Fence Cipher merupakan algoritma kriptografi yang menggunakan teknik subtitusi. Proses enkripsi pada Rail Fence Cipher cukup mudah, plaintext disusun kebawah secara diagonal sampai bawah sesuai dengan rails yang telah ditentukan dan kemudian disusun keatas dengan pola yang sama sampai ke rails paling atas. Pola tersebut diulang sampai semua karakter pada plaintext masuk ke dalam rails. Setelah menerapkan pola tersebut, ciphertext dihasilkan dengan cara membaca karakter dari kiri ke kanan dari setiap baris rails dimulai dari rails paling atas [16]. Pola Rail Fence dengan kunci 3 rails, plaintext harus disusun sampai habis membentuk pola diagonal dari kebawah sampai keatas hingga membentuk seperti pola yang dapat dilihat pada Gambar 1.



Gambar 1: Pola rail fence cipher 3 rails

Untuk menerapkan algoritma Rail Fence pada sebuah pesan, sebagai contoh disini menggunakan kata “SEMARANG” dengan 3 rails. Tiga karakter pertama yaitu “SEM” diletakkan secara diagonal kebawah sebanyak 3 baris. Selanjutnya, karena baris ketiga sudah terisi, dilanjutkan dua karakter “AR” diletakkan secara diagonal keatas dari rails 2 hingga rails paling atas, yaitu rails 1. Kemudian dilanjutkan dengan rails 2 dan 3 yang diisi oleh karakter “A” dan “N”. Terakhir, karakter “G” diletakkan pada rails 2 karena rails 3 telah diisi dan dilanjutkan pola diagonal keatas. Karena karakter dalam kata “SEMARANG” habis pada huruf “G”, maka proses enkripsi telah selesai dan membentuk pola seperti pada Gambar 2.

Rails 1	S				R			
Rails 2		E		A		A		G
Rails 3			M				N	

Gambar 2: Contoh pola rail fence cipher

Setelah menerapkan pola diatas, maka ciphertext dapat dibaca dari kiri pada setiap baris rails,

pada baris pertama adalah "SR", kemudian pada baris kedua adalah "EAAG" dan baris ketiga adalah "MN" seperti pada Gambar 3.

Gambar 3: Pola membaca ciphertext

Hasil akhir dari enkripsi Rail Fence dengan 3 rails menggabungkan karakter dari ketiga baris rails yang menghasilkan ciphertext "SREAAGMN".

Vigenere Autokey adalah pengembangan dari Vigenere yang karakter plaintextnya digeser ke kanan sesuai dengan kunci yang ditambahkan, berbeda dengan Vigenere yang menambahkan kunci langsung ke pesan yang ingin dienkripsi [3]. Vigenere Autokey Cipher ditemukan pada tahun 1586 oleh Blaise de Vigenere [6]. Penggunaan Vigenere Autokey Cipher dapat dilihat pada rumus 1 dan rumus 2.

$$Enkripsi = Plaintext + Kunci \quad (1)$$

$$Dekripsi = Ciphertext – Kunci\ \% \quad (2)$$

Karakter dari plaintext dan kunci diubah terlebih dahulu kedalam bentuk kode sesuai dengan standar ASCII 256. Setelah itu dapat dilakukan perhitungan rumus 1 dan rumus 2 diatas. Perbedaan utama Vigenere Autokey dengan Vigenere biasa adalah pada penggunaan kunci ditambahkan pada plaintext. Untuk mengenkripsi pesan "JAKARTA" dengan kunci otomatis "JAWA" maka kunci baru harus dibuat dengan cara meletakkan kunci di depan plaintext lalu menggeser plaintext ke kanan namun tetap mempertahankan panjang dari plaintext. Dari plaintext "JAKARTA" dengan kunci otomatis "JAWA" maka kunci yang digunakan untuk proses enkripsi adalah "JAWAJAK". Kode ASCII dari karakter "J" pada plaintext dan kunci adalah 74. Kemudian dari plaintext "JAKARTA" dienkripsi menggunakan algoritma Autokey Vigenere menghasilkan ciphertext "", ¢, œ • Œ".

Super enkripsi merupakan konsep pengkombinasian dua algoritma kriptografi yang tujuannya untuk memperkuat keamanan dibandingkan menggunakan satu algoritma kriptografi saja [17], [18]. Proses enkripsi pada konsep super enkripsi diawali dengan enkripsi menggunakan algoritma pertama, hasil ciphertext dari algoritma pertama dienkripsi menggunakan algoritma kedua sehingga menghasilkan ciphertext dari konsep super enkripsi. Proses dekripsi dilakukan dari urutan terakhir proses enkripsi.

Avalanche effect merupakan metode yang digunakan untuk mencari perubahan suatu pesan atau teks saat dilakukan proses enkripsi dengan menghitung rasio antara jumlah bit dari cipherteks yang berubah dan jumlah bit dari plainteks sebelum diubah dalam proses enkripsi. Pengujian menggunakan metode avalanche effect dianggap baik apabila rasio perubahan jumlah bit berada diatas 45% yang mana 50% adalah hasil yang dianggap baik sehingga cukup sulit diserang oleh pihak yang tidak berwenang [6], [19]. Rumus dari Avalanche Effect dapat dilihat pada rumus 3.

$$AE = \frac{jumlahbityangberubah}{totaljumlahbit} X\ 100 \quad (3)$$

Entropi merupakan salah satu parameter yang digunakan untuk mengukur keacakan dari sebuah informasi, jika nilai entropi semakin mendekati 8 maka informasinya akan semakin acak [9], [20]. Dengan itu, semakin tinggi nilai entropi dari hasil enkripsi, maka semakin aman algoritma enkripsi tersebut [21]. Entropi dapat dihitung menggunakan rumus pada rumus 4.

$$H_m = \sum_{ii=1}^{n} P(m_i)\ log_2 \frac{1}{P(m_i)} \quad (4)$$

Dimana $\sum_{i=1}^{n}$adalah operator penjumlahan untuk probabilitas dari i ke n. Sedangkan $P(m_i)$ merupakan probabilitas dari satu kejadian.

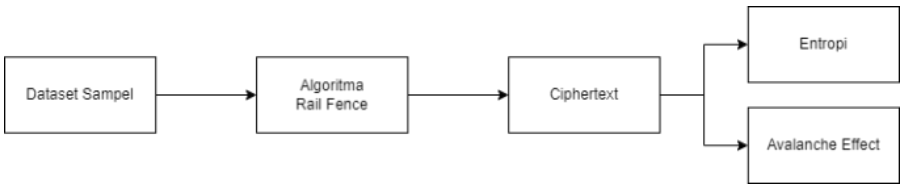
Kerangka Penelitian

Penelitian yang dijalankan dibagi menjadi tiga tahap. Tahap pertama dilakukan adalah tahap eksperimen awal. Tahap eksperimen awal dilakukan untuk menguji tingkat keamanan dari algoritma Rail Fence Cipher. Tahap kedua adalah tahap desain konsep super enkripsi, konsep yang diajukan dalam penelitian untuk menembah kekuatan keamanan dari tahap eksperimen awal. Selanjutnya adalah tahap yang terakhir yaitu tahap evaluasi. Kerangka penelitian dapat dilihat pada Gambar 4.

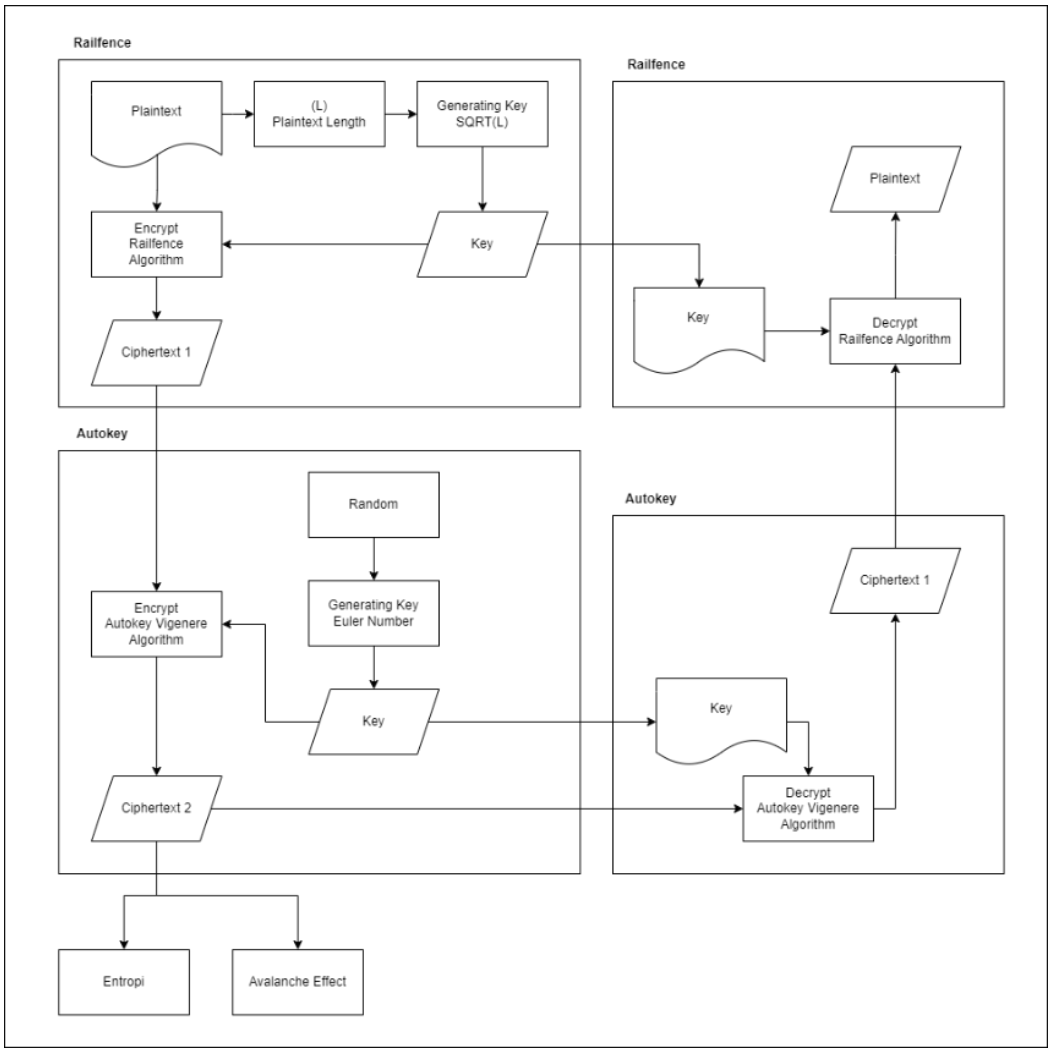
Gambar 4: Kerangka penelitian

Eksperimen Awal

Eksperimen awal adalah tahap pengujian dari algoritma Rail Fence. Algoritma Rail Fence Cipher diujikan pada data Astronomer's Telegram Dataset yang isinya berupa laporan singkat laporan astronomi melalui telegram. Pengujian digunakan empat ukuran sampel yaitu 1 kb, 2 kb, 3 kb, dan 4 kb yang setiap ukuran sampelnya memuat empat sampel data. Hasil dari eksperimen awal akan diuji menggunakan entropi dan avalanche effect. Alur pengujian dari eksperimen awal dapat dilihat pada Gambar 5. Hasil dari ekseperimen awal ini akan menjadi pembanding apakah konsep super enkripsi yang diajukan efektif untuk menambah keamanan dari algoritma Rail Fence Cipher.



Gambar 5: Alur pengujian eksperimen awal



Gambar 6: Usulan desain konsep super enkripsi

Usulan Desain Konsep Super Enkripsi

Konsep super enkripsi yang diusulkan adalah penggabungan algoritma Rail Fence Cipher dan Vigenere Autokey Cipher yang bertujuan untuk menambah tingkat keamanan data yang dapat dilihat pada Gambar 6. Data yang diperlukan adalah plaintext dan kunci untuk setiap algoritma. Plaintext yang digunakan pada penelitian ini sama dengan yang digunakan pada eksperimen awal, yaitu Astronomer's Telegram Dataset.

Sama dengan tahap eksperimen awal, pengujian digunakan empat ukuran sampel yaitu 1 kb sampai 4 kb yang setiap ukuran sampelnya memuat empat sampel data. Percobaan menggunakan masing masing satu kunci untuk algoritma Rail Fence Cipher dan Vigenere Autokey Cipher. Kunci yang dipakai pada algoritma Rail Fence Cipher adalah hasil perhitungan square root dari panjang plaintext, dan kunci yang dipakai pada algoritma Vigenere Autokey Cipher adalah kunci random 16 bytes yang dibangkitkan dengan menggunakan euler number.

Proses enkripsi diawali dengan menggunakan algoritma Rail Fence Cipher. Setelah diperoleh ciphertext dari proses enkripsi menggunakan algoritma Rail Fence Cipher, kemudian ciphertext tersebut dilakukan enkripsi menggunakan algoritma Vigenere Autokey Cipher sehingga diperoleh ciphertext yang kedua. Kemudian, dilakukan evaluasi menggunakan Entropi dan Avalanche Effect, yang nilainya dibandingkan dengan data eksperi-

men awal.

Tahap terakhir dari penelitian ini adalah tahap evaluasi. Pada tahap ini, hasil dari eksperimen awal yang menggunakan algoritma Rail Fence Cipher akan dibandingkan dengan hasil konsep super enkripsi kombinasi dari algoritma Rail Fence Cipher dan Vigenere Autokey Cipher. Nilai entropi dan avalanche effect dari masing-masing tahap akan dibandingkan untuk melihat apakah konsep super enkripsi yang diajukan dapat menambah tingkat keamanan dari algoritma Rail Fence.

Hasil dan Pembahasan

Langkah pertama pengujian adalah eksperimen awal. Eksperimen awal dilakukan untuk menguji tingkat keamanan dari algoritma Rail Fence Cipher. Hasil yang di dapatkan akan digunakan sebagai pembanding dengan hasil dari konsep super enkripsi yang diajukan. Algoritma Rail Fence Cipher diujikan menggunakan 16 sampel data dengan menggunakan kunci hasil dari square root panjang sampel yang digunakan. Hasil pengujian dari algoritma Rail Fence Cipher mendapatkan nilai entropi tertingga mencapai 5,1374 sedangkan nilai terendahnya adalah 4,7593 dan untuk hasil rata-rata nilai entropinya mencapai angka 4,9722. Sedangkan untuk pengujian menggunakan avalanche effect, nilai avalanche effect tertinggi yang bisa didapatkan adalah 39,66% dan untuk nilai terendahnya adalah 34,17% lalu untuk rata-rata nilai avalanche effect nya sebesar 36,03%. Data dari hasil pengujian algoritma Rail Fence Cipher dapat dilihat pada Tabel 1.

.

Tabel 1: Hasil Eksperimen Awal

Ukuran Sampel	Nama Sampel	Entropi	Avalanche Effect (%)
4 kb	ATEL #11975	4,8565	35,34
	ATEL #11646	4,9844	35,94
	ATEL #11559	4,9957	35,79
	ATEL #11946	4,9574	35,48
3 kb	ATEL #11458	4,9786	35,66
	ATEL #11611	4,9431	35,62
	ATEL #12252	5,0711	36,50
	ATEL #11789	4,7359	34,17
2 kb	ATEL #12136	4,9456	35,36
	ATEL #11326	4,9300	36,05
	ATEL #12139	4,7909	35,15
	ATEL #12035	5,1374	37,09
1 kb	ATEL #11772	4,9817	37,08
	ATEL #11883	4,7593	34,75
	ATEL #11692	5,4069	39,66
	ATEL #11182	5,0814	36,84

Hasil eksperimen awal sudah di dapatkan, selanjutnya akan dilakukan pengujian untuk konsep super enkripsi menggunakan algoritma Rail Fence Cipher dikombinasikan dengan Vigenere Autokey Cipher. Menggunakan sampel yang sama dengan sampel eksperimen awal, nilai entropi tertinggi yang bisa didapatkan mencapai 7,2086 sedangkan nilai terendahnya adalah 7,0393, dapat dilihat bahwa peningkatannya cukup signifikan dari hasil pengujian eksperimen awal. Pengujian menggunakan avalanche effect mendapatkan nilai tertinggi mencapai 57,33% dan nilai terendahnya 55,79%. Dalam pengujian avalanche effect pun terlihat penggunaan konsep super enkripsi dengan kombinasi Rail Fence Cipher dan Vigenere Autokey Cipher dapat meningkatkan nilai avalanche effect dengan cukup signifikan dibandingkan dengan pengujian algoritma tunggal pada eksperimen awal. Sedangkan untuk rata-rata nilai entropi dari pengujian konsep super enkripsi dapat mencapai 7,1418 dan rata-rata nilai avalanche effect nya adalah sebesar 56,41%. Hasil lengkap dari pengujian konsep super enkripsi dengan mengombinasikan Rail Fence Cipher dengan Vigenere Autokey Cipher dapat dilihat pada Tabel 2.

.

Tabel 2: Hasil Konsep Super Enkripsi

Ukuran Sampel	Nama Sampel	Entropi	Avalanche Effect (%)
4 kb	ATEL #11975	7,1357	57,33
	ATEL #11646	7,1821	56,68
	ATEL #11559	7,2086	55,79
	ATEL #11946	7,1730	56,16
3 kb	ATEL #11458	7,1667	56,09
	ATEL #11611	7,1561	56,71
	ATEL #12252	7,1796	56,07
	ATEL #11789	7,0939	56,98
2 kb	ATEL #12136	7,1687	56,73
	ATEL #11326	7,1689	56,57
	ATEL #12139	7,1003	56,49
	ATEL #12035	7,1802	56,09
1 kb	ATEL #11772	7,0957	56,25
	ATEL #11883	7,0393	56,75
	ATEL #11692	7,1161	55,79
	ATEL #11182	7,1034	56,07

Hasil yang sangat baik ditunjukkan dari pengujian konsep super enkripsi dengan mengombinasikan Rail Fence Cipher dengan Vigenere Autokey Cipher yang hasilnya menunjukkan peningkatan yang sangat signifikan pada pengujian menggunakan entropi maupun avalanche effect. Berdasarkan hasil pengujian, dari keempat sampel yang digunakan peningkatan nilai entropi dari eksperimen awal yang menggunakan algoritma tunggal Rail Fence Cipher ke konsep super enkripsi yang mana mengombinasikan algoritma Rail Fence Cipher dengan algoritma Vigenere Autokey dapat mencapai 43,84%. Dengan peningkatan sangat signifikan tersebut menunjukkan bahwa tingkat keacakan sampel yang diujikan meningkat hampir mencapai nilai 8 sehingga keamanan dari algoritma super enkripsi menggunakan Rail Fence Cipher dan Vigenere Autokey Cipher meningkat. Selain dalam pengujian entropi, dalam pengujian avalanche effect juga mengalami peningkatan yang signifikan. Dengan nilai avalanche effect pada tiap sampel yang mencapai 50%, dapat dipastikan bahwa sam-

pel tersebut mengalami perubahan jumlah bit yang tinggi. Perubahan bit tersebut membuat data menjadi tersamarkan sehingga pihak yang tidak berwenang tidak dapat mengetahui isi data tersebut. Pada Tabel 3 diperlihatkan detail perbandingan dari hasil pengujian entropi dari eksperimen awal dengan hasil pengujian entropi dari konsep super enkripsi dengan mengombinasikan Rail Fence Cipher dan Vigenere Autokey Cipher.

Tabel 3: Perbandingan Entropi Hasil Pengujian

Ukuran Sampel	Nama Sampel	Eksperimen Awal	Konsep Super Enkripsi
4 kb	ATEL #11975	4,8565	7,1357
	ATEL #11646	4,9844	7,1821
	ATEL #11559	4,9957	7,2086
	ATEL #11946	4,9574	7,1730
3 kb	ATEL #11458	4,9786	7,1667
	ATEL #11611	4,9431	7,1561
	ATEL #12252	5,0711	7,1796
	ATEL #11789	4,7359	7,0939
2 kb	ATEL #12136	4,9456	7,1687
	ATEL #11326	4,9300	7,1689
	ATEL #12139	4,7909	7,1003
	ATEL #12035	5,1374	7,1802
1 kb	ATEL #11772	4,9817	7,0957
	ATEL #11883	4,7593	7,0393
	ATEL #11692	5,4069	7,1161
	ATEL #11182	5,0814	7,1034

Perbandingan avalanche effect dari kedua pengujian juga dapat dilihat pada Tabel 4.

Tabel 4: Perbandingan Avalanche Effect Hasil Pengujian

Ukuran Sampel	Nama Sampel	Eksperimen Awal (%)	Konsep Super Enkripsi (%)
4 kb	ATEL #11975	35,34	57,33
	ATEL #11646	35,94	56,68
	ATEL #11559	35,79	55,79
	ATEL #11946	35,48	56,16
3 kb	ATEL #11458	35,66	56,09
	ATEL #11611	35,62	56,71
	ATEL #12252	36,50	56,07
	ATEL #11789	34,17	56,98
2 kb	ATEL #12136	35,36	56,73
	ATEL #11326	36,05	56,57
	ATEL #12139	35,15	56,49
	ATEL #12035	37,09	56,09
1 kb	ATEL #11772	37,08	56,25
	ATEL #11883	34,75	56,75
	ATEL #11692	39,66	55,79
	ATEL #11182	36,84	56,07

Hasil dari pengujian menggunakan entropi dan avalanche effect yang sudah dilakukan menunjukkan bahwa mengombinasikan dua algoritma kriptografi dapat meningkatkan keamanan data dengan cukup baik sehingga kemungkinan akses oleh pihak yang tidak berwenang dapat diatasi. Dengan meningkatnya keacakan informasi data dan perubahan jumlah bit dalam data membuat ciphertext yang dihasilkan dari proses enkripsi menjadi sangat berbeda dengan plaintext sehingga akan semakin sulit untuk pihak yang tidak berwenang mengetahui informasi dalam data tersebut.

Penutup

Berdasarkan hasil eksperimen yang telah dilakukan sebelumnya, dapat disimpulkan bahwa penggunaan konsep super enkripsi dapat meningkatkan tingkat keamanan dari algoritma Rail Fence Cipher secara signifikan. Hal ini dibuktikan dengan peningkatan nilai entropi ketika menggunakan algoritma Rail Fence Cipher dibandingkan dengan konsep super enkripsi yang menggabungkan algoritma Rail Fence Cipher dengan algoritma Vigenere Autokey Cipher. Nilai entropi rata-rata mencapai 7,1418, mendekati nilai maksimum 8, yang menunjukkan bahwa informasi dari sampel yang diuji menjadi sangat acak.

Selain itu, pengujian menggunakan avalanche effect juga mengalami peningkatan yang signifikan dengan rata-rata mencapai 56,41%. Ini menunjukkan bahwa perubahan kecil pada input menghasilkan perubahan besar pada output enkripsi, membuat hasil enkripsinya sulit dikenali atau ditebak.

Untuk pengembangan selanjutnya, disarankan untuk menguji kombinasi algoritma kriptografi yang berbeda. Hal ini bertujuan untuk memperkuat tingkat keamanan dari algoritma yang mungkin sudah mulai ditinggalkan atau dianggap kurang aman. Dengan mencoba berbagai kombinasi algoritma, diharapkan dapat ditemukan metode yang lebih kuat dan aman untuk melindungi informasi. Selain kombinasi algoritma lain, pengembangan lebih lanjut dapat dilakukan dengan aspek lain seperti:

1. Analisis kinerja, selain keamanan mengukur kinerja dari kombinasi algoritma ini sangat penting untuk melihat seberapa efisien algoritma super enkripsi ini dengan melihat waktu enkripsi dan dekripsi, penggunaan sumber daya, dan skalabilitas.

2. Uji coba menggunakan data lain, seperti gambar dan video untuk memastikan bahwa kombinasi algoritma super enkripsi ini tetap efektif di berbagai jenis data.

3. Melakukan pengujian terhadapat serangan kriptografi, tujuannya untuk untuk memastikan bahwa kombinasi algoritma super enkripsi dapat menahan serangan tersebut.

Dengan melakukan pengembangan dan pengujian lebih lanjut ini, diharapkan dapat ditemukan solusi kriptografi yang lebih kuat, efisien, dan dapat diandalkan untuk melindungi informasi penting di era digital saat ini.

Daftar Pustaka

[1] Muhammad Fadlan, Haryansyah, dan Rosmini, "Pengamanan Data melalui Model Super Enkripsi Autokey Cipher dan Transposisi Kolom", Jurnal RESTI (Rekayasa Sistem dan Teknologi Informasi), vol. 5, no. 6, hlm. 1113–1119, doi: 10.29207/resti.v5i6.3566, Des 2021.

[2] Megawati, Muhammad Fitra Hamidy, Sasqia Ismi Aulia, Yuhendri Putra, dan Mhd Arief Hasan, "Enkripsi dan Deskripsi File Menggunakan Kombinasi Vigenere dan Shift Cipher di Python", SATIN - Sains dan Teknologi Informasi, vol. 7, no. 1, hlm. 102–111, doi: 10.33372/stn.v7i1.686, Jun 2021.

[3] M. Fadlan, R. Rosmini, dan H. Haryansyah, "Perpaduan Algoritma Kriptografi Atbash dan Autokey Cipher dalam Mengamankan Data", Jurnal Media Informatika BUDIDARMA, vol. 5, no. 3, hlm. 806, doi: 10.30865/mib.v5i3.3019, Jul 2021.

[4] R. Diky Zailani, Khairil, dan A. Al Akbar, "Android-Based Cryptography Applications Using The Rail Fence Cipher Algorithm", Jurnal Media Computer Science, vol. 2, no. 2, hlm. 303–318, 2023.

[5] R. Oktafiani, E. I. H. Ujianto, dan R. Rianto, "Kombinasi Algoritma Kriptografi Vigenere Cipher dan SHA256 untuk Keamanan Basis Data", Jurnal Sistem Komputer dan Informatika (JSON), vol. 4, no. 3, hlm. 433, doi: 10.30865/json.v4i3.5583, Mar 2023.

[6] L. Budi Handoko, "Pengujian Avalanche Effect Pada Kriptografi Teks Menggunakan Autokey Cipher", 2st Proceeding STEKOM, vol. 2, no. 1, hlm. 127–134, 2022.

[7] R. I. Lazuardi dan N. Anwar, "Hybird Autokey Cipher Algorithm Implementation Reverse Key and Standard Data Encryption for App-Based Text Messages", Mobile and Forensics, vol. 5, no. 2, hlm. 42–48, doi: 10.12928/mf.v5i2.8451, Sep 2023.

[8] L. Agustina, I. Sujarwo, dan M. Khudzaifah, "Membangun Super Enkripsi untuk Mengamankan Pesan", Jurnal Riset Mahasiswa Matematika, vol. 2, no. 3, hlm. 84–89, doi: 10.18860/jrmm.v2i3.16335, Mar 2023.

[9] F. Nuraeni dkk., "Implementasi Skema QR-Code dan Digital Signature menggunakan Kombinasi Algoritma RSA dan AES untuk Pengamanan Data Sertifikat Elektronik", Seminar Nasional Teknologi Informasi Komunikasi dan Industri, vol. 12, no. 6, hlm. 43–52, 2020.

[10] Irwansyah, A. Fauzi, dan S. Syahputra, "A Combination Of A Rail Fence Cipher And Merkle Hellman Algorithm For Digital Image Security", Journal of Artificial Intelligence and Engineering Applications, vol. 2, no. 3, hlm. 133–143, 2023.

[11] C. Irawan, E. H. Rachmawanto, C. A. Sari, dan C. A. Sugianto, "Super Enkripsi File Dokumen Menggunakan Beaufort Cipher Dan Transposisi Kolom", Prosiding Seminar Nasional LPPM UMP, vol. 2, hlm. 556–563, 2020.

[12] D. Sinaga, C. Umam, D. Rosal, I. M. Setiadi, dan H. Rachmawanto, "Teknik Super Enkripsi Menggunakan Transposisi Kolom Berbasis Vigenere Cipher Pada Citra Digital (Super Encryption Technique Using Transposition Column Based On Vigenere Cipher On Digital Image)", Dinamika Rekayasa, vol. 14, no. 1, hlm. 57–64, 2018.

[13] D. Ratna, "Implementasi Algoritma Rail Fence Chiper Dalam Keamanan Data Gambar 2 Dimensi", Jurnal Pelita Informatika, vol. 7, no. 1, 2018.

[14] E. Ardhianto, R. S. Redjeki, E. Supriyanto, H. Murti, dan E. N. Wahyudi, "Adopsi Generator Kunci Euler Number dan Pembangkit Kunci Blum Blum Shub untuk Meningkatkan Confidentiality Level pada Extended Vigenere", Jurnal Informatika dan Teknologi, vol. 7, no. 1, hlm. 1, doi: 10.29408/jit.v7i1.21512, 2024.

[15] N. R. H. Dwi, Nilma, dan N. Pravitasari, "Penerapan Kriptografi AES untuk Keamanan Data Aplikasi Pemesanan Bibit Ternak pada BPSI UAT", Remik: Riset dan E-Jurnal Manajemen Informatika Komputer, vol. 8, no. 1, doi: 10.33395/remik.v8i1.13157, 2024.

[16] S. Godara, S. Kundu, dan R. Kaler, "An Improved Algorithmic Implementation of Rail Fence Cipher", International Journal of Future Generation Communication and Networking, vol. 11, no. 2, hlm. 23–32, doi: 10.14257/ijfgcn.2018.11.2.03, Mar 2018.

[17] Moch. H. Purwidiantoro dan D. F. K. Saputro Wibowo, "Super Encryption Concepts using Vigenere Cipher Modification to Produce Color Imaginary as Ciphertext", dalam Proceedings ofthe 1st International Conference on Recent Innovations, Scitepress, doi: 10.5220/0009946230293035, hlm. 3029–3035, Agu 2020.

[18] L. Valdho Falensky dan M. A. Ineke Pakereng, "Pengamanan Data Pasien Di UPT. Puskesmas Pujon Kalimantan Tengah Menggunakan Kriptografi Super Enkripsi", Jurnal Sains Komputer & Informatika (J-SAKTI), vol. 6, no. 2, hlm. 711–725, 2022.

[19] M. Fajar, A. Billy Kambodji, dan I. Alwiah Musdar, "Implementasi Algoritma Advanced Encryption Standard untuk Pengamanan Data Pengguna Aplikasi Media Sosial VirCle", Jurnal Algoritma, vol. 20, no. 2, hlm. 398–409, 2023.

[20] H. Murti, E. Lestariningsih, E. Supriyanto, dan E. Ardhianto, "Modifikasi Model Enkripsi Encryption With Covertext and Reordering menggunakan Fungsi Random dan Tabel Permutasi", Jurnal Informatika UPGRIS, vol. 8, no. 1, hlm. 65–68, 2022.

[21] F. Nuraeni, Y. H. Agustin, dan A. E. Purnama, "Implementasi Caesar Cipher And Advanced Encryption Standard (AES) Pada Pengamanan Data Pajak Bumi Bangunan", Jurnal Ilmiah MATRIK, vol. 22, no. 2, 2020.