JURNAL MULTI MEDIA DAN IT
VOL.08 NO.02 (2024), PP. 130-137
P-ISSN : 2548-9534 | E-ISSN : 2548-9550

Perbandingan *Cryptography* Klasik *Vigenere Cipher* Dengan *Cryptography* Modern *RC4* Dalam Tingkat Keamanan Jaringan Komputer

Suryani Kurnia Dewi

Pendidikan Informatika, Universitas Trunojoyo Madura

INFORMASI ARTIKEL

Sejarah Artikel:
Diterima Redaksi: 03 September 2024
Revisi Akhir: 31 Desember 2024
Diterbitkan *Online*: 31 Desember 2024

KATA KUNCI

Kriptografi, RC4, Vigenere Cipher

KORESPONDENSI

Suryani Kurnia Dewi
Pendidikan Informatika, Universitas Trunojoyo Madura
suryanikdf6@gmail.com

ABSTRACT

Kriptografi merupakan aspek penting dalam era digital untuk menjaga keamanan informasi dalam jaringan komputer. Penelitian ini bertujuan untuk membandingkan dua jenis kriptografi, yaitu kriptografi klasik (Vigenere Cipher) dan kriptografi modern (RC4), dalam keamanan jaringan komputer. Metode penelitian yang digunakan adalah Systematic Literature Review, yang melibatkan pengumpulan, evaluasi, dan literatur terkait. Hasilnya menunjukkan bahwa Vigenere Cipher memiliki kelebihan dalam implementasi yang mudah dan kemampuan mengatasi analisis frekuensi, tetapi rentan terhadap serangan brute-force jika panjang kunci tidak cukup panjang. Sementara itu, RC4, meskipun cepat dan fleksibel, memiliki kelemahan keamanan signifikan seperti kerentanan terhadap serangan terhadap kunci terkait. Dalam kesimpulannya, kriptografi modern seperti RC4 memiliki masalah keamanan yang signifikan meskipun kompleksitasnya lebih tinggi daripada Vigenere Cipher. Oleh karena itu, dalam penggunaan di jaringan komputer, disarankan untuk memilih algoritma kriptografi yang memenuhi standar keamanan terkini.

DOI: https://doi.org/10.46961/jommit.v8i2

1. PENDAHULUAN

Dalam era digital saat ini, perlindungan informasi menjadi semakin krusial, terutama dalam jaringan komputer. Kemajuan teknologi telah memfasilitasi pertukaran data yang cepat dan efisien, namun seiringan dengan itu juga meningkatkan potensi risiko terhadap kebocoran informasi dan serangan siber. Teknik seperti steganografi dan kriptografi dikembangkan untuk menjamin kerahasiaan informasi. Metode-metode ini tidak terbatas pada satu teknik perlindungan data saja, namun juga dapat digabungkan atau dimodifikasi melalui penggunaan algoritma yang berbeda. (Utami Rukmaliani, Rosnita, 2020). Oleh karena itu, penerapan teknik kriptografi sebagai langkah yang sangat penting dalam menjaga keamanan data semakin menjadi fokus utama.

Kriptografi adalah suatu seni dan ilmu yang digunakan untuk melindungi data atau informasi yang dikirimkan dengan cara mengubahnya menjadi kode-kode tertentu. Data tersebut hanya dikirmkan kepada seseorang yang memiliki kuncinya, yang digunakan untuk mengubah kode-kode tersebut kembali menjadi data atau informasi asli yang dikirmkan. (Azura et al., 2023). Kriptografi dapat mencegah akses yang tidak berwenang mengenai informasi sensitif ketika disimpan. ia menggunakan enkripsi untuk melindungi transfer data melalui jaringan.

Ada dua jenis kriptografi: kriptografi klasik dan kriptografi modern. Kriptografi klasik digunakan sebelum era komputer dan biasanya menggunakan teknik kunci simetris. Metode penyembunyian pesan dalam kriptografi klasik adalah melalui substitusi atau transposisi, atau kombinasi keduanya. Di sisi laon, algoritma kriptografi modern mengggunakan pemrosesan biner dan manipulasi simbol berdasaekan kode ASCII (American Standard Code for Information Interchange) karena beroperasi di lingkungan komputer digital, sehingga memrlukan pemahaman dasar matematika untuk menguasainya. (Dimas Mayoni Aji Sasono et al., 2023).

Salah satu contoh kriptografi klasik adalah vingenere chiper. Vigenere cipher merupakan salah satu algoritma yang menggunakan kunci simetris dan dapat digunakan untuk mengkodekan pesan(Gusti et al., 2020). Algoritma vigenere cipher merupakan salah satu teknik kriptografi klasik yang di kembangkan dari Caesar Cipher dimana cara enkripsinya menggunakan alfabet yang disusun secara diagonal dalam suatu tabel.(Aisyiah et al., 2023)

https://doi.org/10.46961/jommit.v8i2

. Di sisi lain, kriptografi modern, seperti algoritma RC4, menawarkan tingkat keamanan yang lebih tinggi dengan mengadopsi pendekatan matematis yang lebih kompleks. Algoritma ini beroperasi dengan menggunakan kunci enkripsi yang dihasilkan dari array state *256-bit* yang diinisialisasi dengan sebuah kunci yang memiliki panjang *1-256 bit*. setelah inisialisasi, *array stat*e ini diacak kembali dan diproses untuk menghasilkan sebuah kunci enkripsi yang kemudian digunakan untuk meng-XOR dengan *plaintext* atau *ciphertext*, sehingga menghasilkan *output* dari proses enkripsi atau deskripsi.

Banyaknya jenis kriptografi baik yang klasik maupun modern, penelitian ini mencoba untuk melakukan analisis perbandingan antara kriptografi klasik (*Vigenere Cihper*) dengan kriptografi modern (*RC4*). Oleh karena itu, penelitian ini bertujuan untuk mengungkap fakta-fakta dan informasi yang ditemukan melalui penelitian sebelumnya.

2. TINJAUAN PUSTAKA

2.1. Keamanan Jaringan

Keamanan jaringan komputer adalah proses yang dirancang untuk mencegah dan mendeteksi akses tidak sah ke jaringan komputer. Tujuan utama keamanan jaringan komputer adalah untuk memitigasi risiko ancaman fisik dan logis, baik langsung maupun tidak langsung, yang dapat mengganggu aktivitas yang sedang berlangsung dalam jaringan. Selain itu, hal ini bertujuan untuk melindungi data dalam sistem komputer dari berbagai ancaman, memastikan integritas dan keamanannya.

2.1.1. Criptography

Cryptography adalah ilmu tentang teknik enkripsi yang mengubah pesan asli (plaintest) menjadi pesan acak yang tidak dapat dibaca (ciphertext) dengan menggunakan kunci enkripsi. Deskripdi menggunakan kunci deskripsi dapat mengambil data asli. Kemungkinan seseorang tanpa kunci deskripsi mendapatkan pesan asli dalam jangka waktu yang wajar sangatlah rendah. (Alfan et al., 2021)

2.1.2. Cryptography Classic

Kriptografi dibagi menjadi dua jenis yaitu kriptografi klasik dan kriptografi modern, kriptografi klasik digunakan sebelum era kompuer dan sebagian besar menggunakan teknik kunci simetris. Metode untuk menyembunyikan pesan melibatkan substitusi atau transposisi, atau bahkan kombinasi keduanya. Substitusi merupakan proses penggantian karakter pada plaintext dengan karakter yang berbeda untuk menghasilkan ciphertext. Di sisi lain, transposisi melibatkan penataan ulang karakter dalam teks biasa untuk membuat teks tersandi. Kombinasi kompleks dari kedua teknik ini menjadi dasar berbagai algoritma kriptografi modern. Contoh algoritma kriptografin klasik antara lain: *Caesar Cipher*, *Vigenere Cipher*, dan *Hill Cipher*.(Dimas Mayoni Aji Sasono et al., 2023)

2.1.3. Vigenere Chiper

Vigenere cipher adalah sandi substitusi polialfabetik yang dilakukan dengan menambahkan indeks setiap karakter teks biasa ke indeks karakter kunci berdasarkan Vignere Square atau tabel Vignere. (Susila Bahri, 2023)

2.1.4. Criptography Modern

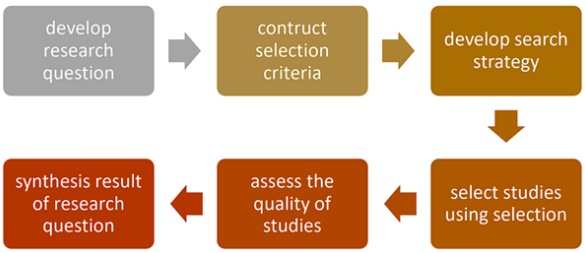
Cryptography Modern merupakan penyempurnaan dari teknik yang digunakan dalam kriptografi klasik. Algoritme dalam kriptografi modern menggunakan pemrosesan biner dan manipulasi simbol berdasarkan kode ASCII (American Standard Code for Information Interchange) karena beroperasi di lingkungan komputer digital, sehingga memerlukan pemahaman dasar matematika untuk menguasainya. Algoritme ini juga lebih kompleks, membuat kriptanalisi sulit memecahkan ciphertext tanpa mengetahui kuncintya.. ada tiga jenis kunci dalam kriptografi modern: simetris, asimetris dan hybrid. (Susila Bahri, 2023)

2.1.5. RC4

RC4 merupakan jenis aliran kode yang berarti operasi enkripsinya dilakukan per karakter 1 byte untuk sekali operasi. RC4 adalah tipe stream cipher. Ini memproses unit atau memasukkan data pada satu waktu. Satuan atau data adalah byte atau bahkan terkadang bit Algoritma kriptografi Rivest Code 4 (RC4) merupakan salah satu algoritma kunci simetris dibuat oleh RSA Data Security Inc (RSA ASI) yang berbentuk stream cipher. Algoritma ini ditemukan pada tahun 1987 oleh Ronald Rivest dan menjadi simbol keamanan RSA (merupakan singkatan dari tiga nama penemu yaitu Rivest, Shamir, and Adleman). (Alfan et al., 2021)

3. KONSEP PERANCANGAN

Pada penelitian ini menggunakan metode *Systematic Literature Review* untuk mengetahui perbandingan antara kriptografi klasik dan modern dalam segi keamanan. Metode ini merupakan prosedur sistematis dalam mengumpulkan, mengevaluasi, dan mengintegrasikan literatur yang relevan dengan topik penelitian. Menurut (Zawacki-Richter et al., 2019). rancangan prosedur penelitian *Systematic Literature Review* sebagai berikut:



Gambar 1. Prosedur Penelitian Systematic Literature Review

Mengenai prosedur yang dipaparkan pada Gambar 1 berikut adalah uraian rinci tentang prosedur yang diterapkan:

a. *Develop Research Questions*
   Pada tahapan penelitian ini, Perbandingan Cryptography Klasik Vigenere Cipher Dengan Cryptography Modern RC4 Dalam Tingkat Keamanan Jaringan Komputer terdiri dari empat pertanyaan sebagai berikut:
   1. Apa prinsip dasar dari kriptografi klasik Vigenere Cipher dan kriptografi modern RC4?
   2. Bagaimana kekuatan dan kelemahan dari masing-masing metode kriptografi tersebut dalam keamanan jaringan komputer?

3. Dalam perbandingan tingkat keamanan, apa yang menjadi perbedaan antara kriptografi klasik Vigenere Cipher dan kriptografi modern RC4 dalam penggunaan pada jaringan komputer?

b. *Selection Criteria*
Tahapan ini peneliti melakukan pemilihan artikel ilmiah sebagai dasar kajian literatur review. Adapun kriteria pemilihan artikel ilmiah ditunjukan pada Tabel 1.

Jenis Kriteria	**Keterangan**
Kriteria *inclusion* (penerimaan)	a. Artikel ilmiah sesuai dengan topik penelitian yaitu kriptografi klasik Vigenere Cipher dan kriptografi modern RC4. b. Publikasi 2019-2024. c. Teks lengkap.
Kriteria *exclusion* (penolakan)	a. Artikel ilmiah penelitian di luar topik penelitian. b. Publikasi tahun sebelum 2019. c. Teks tidak lengkap.

c. *Developing the Search Strategy*
Pada tahap ini peneliti melakukan proses pencarian artikel ilmiah menggunakan google schoolar, dan semantic scholar.

d. *The Study Selection Process*
Tahap berikutnya yaitu proses pemilihan studi, dimana setiap artikel yang ditemukan harus diperiksa judul dan abstrak untuk mengetahui relevansi artikel dengan tema penelitian yang sedang dilakukan.

e. *Appraising the Quality of Studies*
Dalam penelitian ini data yang ditemukan akan dievaluasi berdasarkan kriteria penilaian kualitas. Adapun kriteria yang digunakan untuk menilai artikel ilmiah yaitu kesesuaian antara tujuan dengan metode penelitian, kesesuaian tujuan penelitian dengan instrumen yang digunakan, dan relevansi penggunaan daftar pustaka.

f. *Synthesis Result of Research Question*
Pada tahap ini semua artikel ilmiah yang sudah dipilih akan dikaji berdasarkan tiga pertanyaan yang sudah ditetapkan sebelumnya. Selanjutnya dibuatkan kesimpulan berdasarkan informasi yang dipaparkan, dan melakukan pembahasan yang diuraikan secara rinci.

4. HASIL DAN PEMBAHASAN

Sebanyak 15 artikel ilmiah dipilih untuk dianalisis secara sistematis setelah melalui proses pemilihan berdasarkan persyaratan kelayakan. Persyaratan kelayakan tersebut meliputi artikel ilmiah yang relevan dengan topik penelitian tentang kriptografi klasik (Vigenere Cipher) dan kriptografi modern (RC4), rentang publikasi dari tahun 2019-2024, serta memiliki teks yang lengkap. Berikut adalah hasil rangkuman studi literatur terkait analisis perbandingan kriptografi klasik (Vigenere Cipher) dan kriptografi modern (RC4).

Tabel 1. Ringkasan Studi Literatur

No	Penulis	RQ (1,2, dan 3)
1	(Ngemba et al., 2024)	RC4 adalah algoritma kriptografi stream yang cepat dan mudah diimplementasikan, menggunakan kunci variabel untuk enkripsi data secara berurutan. Keunggulannya terletak pada kecepatan dan efisiensi, namun memiliki kelemahan dalam keamanan karena rentan terhadap serangan statistik dan kerentanan terhadap serangan WEP, membuat tingkat keamanannya relatif rendah dibandingkan dengan algoritma kriptografi modern.
2	(Alfan et al., 2021)	Prinsip dasar dari algoritma RC4 adalah melakukan enkripsi secara stream dengan menghasilkan byte stream pseudorandom berdasarkan kunci yang disediakan. Ini dilakukan melalui dua algoritma utama, yaitu Key Scheduling Algorithm (KSA) untuk menginisialisasi permutasi dalam array dan Pseudo-Random Generation Algorithm (PRGA) untuk menghasilkan stream pseudorandom dari byte. RC4 memiliki kekuatan dalam kecepatan dan efisiensi karena proses enkripsinya per karakter 1 byte, namun juga memiliki kelemahan dalam keamanan karena rentan terhadap serangan statistik dan serangan WEP, serta terdapat kerentanan terhadap serangan yang dapat memperoleh kunci enkripsi yang digunakan. Oleh karena itu, tingkat keamanan RC4 relatif rendah dibandingkan dengan algoritma kriptografi modern yang lebih canggih.
3	(Dimas Mayoni Aji Sasono et al., 2023)	RC4 adalah stream cipher yang dirancang oleh Ron Rivest, menggunakan dua algoritma utama: Key Scheduling Algorithm (KSA) untuk menginisialisasi state array dan Pseudo-Random Generation Algorithm (PRGA) untuk menghasilkan keystream yang di-XOR dengan plaintext. Keunggulan RC4 terletak pada kecepatannya dan kesederhanaannya, namun kelemahannya mencakup bias dalam keystream, kerentanan terhadap serangan kriptografi, dan risiko jika menggunakan kunci yang sama berulang kali. Meskipun pernah

		digunakan luas dalam protokol seperti WEP dan SSL/TLS, kelemahan signifikan telah membuat RC4 tidak lagi disarankan untuk aplikasi keamanan modern, digantikan oleh algoritma yang lebih aman seperti AES.
4	(Yanuba et al., 2023)	RC4 adalah algoritma kriptografi kunci simetris yang menggunakan stream cipher untuk enkripsi data, di mana S-Box diinisialisasi dan diacak dengan kunci untuk menghasilkan keystream yang digunakan dalam operasi XOR dengan plaintext atau ciphertext. Kelebihannya terletak pada kesederhanaan dan kecepatan, serta fleksibilitas panjang kunci. Namun, kelemahannya termasuk bias awal pada keystream, keberadaan "weak keys," dan kerentanannya yang terbukti dalam protokol WEP dan WPA. Meskipun RC4 dapat memberikan keamanan yang memadai dengan penggunaan hati-hati, kelemahan-kelemahan ini telah mendorong komunitas keamanan untuk beralih ke algoritma yang lebih modern seperti AES.
5	(Nurmadjid, 2023)	RC4 adalah algoritma stream cipher yang mengenkripsi data byte demi byte menggunakan kunci simetris, melalui proses Key Scheduling Algorithm (KSA) dan Pseudo-Random Generation Algorithm (PRGA). Kelebihannya termasuk implementasi yang mudah, operasi cepat, dan ketahanan terhadap kerusakan pada satu bit data tanpa mempengaruhi keseluruhan pesan. Namun, kelemahan RC4 mencakup kerentanannya terhadap analisis statistik dan serangan kunci terkait. Tingkat keamanan RC4 dalam penelitian yang diterapkan pada PT Fajar Mitra Krida Abadi menunjukkan bahwa modifikasi KSA dengan menambah iterasi 10 kali meningkatkan variabilitas ciphertext dan mempercepat proses dekripsi dibandingkan enkripsi. Penelitian ini juga menggarisbawahi pentingnya perlindungan data untuk mencegah kerusakan reputasi perusahaan akibat kebocoran data, dengan hasil pengujian menunjukkan bahwa semakin besar ukuran file, semakin lama waktu enkripsi dan dekripsinya, meskipun dekripsi tetap lebih cepat.
6	(Belakang, 2023)	RC4 adalah algoritma kriptografi jenis stream cipher yang cepat dan efisien, terdiri dari dua tahap utama: key setup dan stream generation, yang menghasilkan nilai pseudorandom
		untuk enkripsi melalui operasi XOR. Kekuatan RC4 terletak pada kecepatan dan fleksibilitas panjang kunci, namun kelemahannya mencakup kerentanan terhadap serangan analisis statistik dan inisialisasi yang lemah, membuatnya tidak lagi aman untuk aplikasi modern. Tingkat keamanannya dianggap rendah, sehingga banyak standar keamanan kini menggantinya dengan algoritma yang lebih kuat seperti AES.
7	(Busran & Jeri Widodo Putra, 2021)	RC4 adalah algoritma stream cipher yang menggunakan kunci untuk menghasilkan keystream untuk enkripsi data, dengan kecepatan sebagai keunggulan utamanya. Namun, kelemahan terkait dengan panjang kunci dan serangan statistik telah membuat keamanan RC4 dipertanyakan. Meskipun masih digunakan dalam beberapa aplikasi, penggunaan RC4 tidak direkomendasikan karena rentan terhadap serangan yang semakin canggih, dan algoritma enkripsi yang lebih kuat seperti AES lebih disarankan untuk mengamankan data.
8	(Noviyanti. P & Mira, 2022)	Vigenere Cipher adalah algoritma kriptografi klasik yang menggunakan tabel 26x26 dari alfabet A hingga Z dan sebuah kata kunci untuk mengenkripsi pesan. Setiap huruf dalam teks asli dienkripsi dengan menambahkan nilai posisi huruf pada teks dengan nilai posisi huruf pada kata kunci secara berulang, menciptakan penggeseran variabel. Kekuatan utama algoritma ini adalah kompleksitas polanya yang mengurangi risiko serangan frekuensi sederhana, namun kelemahannya terletak pada kerentanannya terhadap analisis frekuensi berulang dan metode Kasiski jika kata kunci diketahui atau terlalu pendek. Tingkat keamanannya cukup baik untuk serangan sederhana, tetapi tidak cukup kuat terhadap analisis kriptografi yang lebih canggih, membuatnya rentan terhadap metode pemecahan modern tanpa modifikasi tambahan.
9	(Imam Riadi et al., 2022)	Vigenere Cipher adalah algoritma kriptografi klasik berbasis polyalphabetic substitution cipher yang menggunakan kunci berulang untuk mengenkripsi dan mendekripsi teks, memanfaatkan tabel bujur sangkar Vigenere. Kekuatan utamanya adalah kemampuannya untuk membuat pola huruf yang lebih kompleks dibandingkan Caesar Cipher, sehingga

		lebih tahan terhadap analisis frekuensi. Namun, kelemahannya terletak pada kunci yang berulang yang rentan terhadap serangan analisis seperti metode Kasiski dan Friedman, terutama jika panjang kunci dapat ditebak. Meskipun memberikan keamanan lebih baik dibandingkan substitusi sederhana, tingkat keamanan Vigenere Cipher masih lebih rendah dibandingkan algoritma modern seperti AES atau RSA, dan karenanya tidak disarankan untuk aplikasi yang membutuhkan perlindungan data tinggi .
10	(Fatma et al., 2023)	Prinsip dasar dari Vigenere Cipher adalah menggunakan teknik substitusi polialfabetik, di mana setiap huruf dalam teks terbuka dienkripsi berdasarkan urutan kunci yang terdiri dari beberapa sandi Caesar yang berbeda. Kunci ini digunakan secara berulang selama proses enkripsi, sehingga setiap huruf dalam teks terbuka dapat dienkripsi dengan kunci yang berbeda-beda. Kekuatan dari Vigenere Cipher terletak pada kompleksitasnya yang meningkatkan tingkat keamanan dibandingkan dengan sandi Caesar sederhana. Namun, kelemahannya terletak pada rentan terhadap analisis frekuensi huruf dan serangan kasar lainnya karena pola pengulangan kunci yang dapat dieksploitasi untuk mendekripsi pesan terenkripsi. Tingkat keamanan dari Vigenere Cipher dapat bervariasi tergantung pada panjang kunci yang digunakan. Semakin panjang kunci yang digunakan, semakin sulit untuk melakukan dekripsi tanpa kunci yang tepat. Namun, jika panjang kunci terlalu pendek, Vigenere Cipher dapat menjadi rentan terhadap serangan kriptanalisis, seperti analisis frekuensi huruf dan serangan kasar.
11	(Azura et al., 2023)	Prinsip dasar Vigenere Cipher adalah menggunakan metode substitusi polialfabetik sederhana dengan mengonversi huruf alfabet dari A-Z menjadi 0-25, dilakukan dengan mengkombinasikan huruf alfabet dan angka serta melakukan perjumlahan atau pengurangan berdasarkan rumus yang telah ditentukan untuk mencari chipertext dan plaintext. Kekuatan Vigenere Cipher terletak pada kemampuannya untuk meningkatkan keamanan data, seperti dalam aplikasi rekam medis, namun kelemahannya
		adalah pada tingkat keamanan yang relatif rendah dibandingkan dengan algoritma kriptografi modern yang lebih kompleks. Tingkat keamanan Vigenere Cipher dianggap relatif rendah karena sifat polialfabetiknya yang sederhana, rentan terhadap serangan kriptanalis jika digunakan tanpa pengamanan tambahan atau kunci yang mudah ditebak.
12	(Rista & Samuel Sitio, 2021)	Prinsip dasar RC4 adalah algoritma stream cipher yang menggunakan kunci simetris untuk mengenkripsi dan mendekripsi data. Algoritma ini bekerja dengan cara menghasilkan aliran kunci pseudorandom yang kemudian digunakan dalam operasi XOR dengan data yang akan diamankan. Kekuatan RC4 terletak pada kecepatan dan efisiensinya dalam mengenkripsi data serta kemampuannya untuk diimplementasikan dalam berbagai aplikasi. Namun, kelemahannya terletak pada kerentanan terhadap serangan kriptoanalisis, terutama dalam menghadapi serangan terkait dengan kunci yang lemah dan pola kekunci yang dapat diprediksi. Secara umum, tingkat keamanan RC4 dapat dianggap cukup kuat untuk penggunaan umum, tetapi seringkali direkomendasikan untuk digunakan dengan kunci yang lebih panjang dan menghindari penggunaan yang terlalu sering pada data yang sama.
13	(Febriyani & Arfriandi, 2021)	Mengimplementasikan algoritma RC4 dalam mengamankan dokumen digital, dengan prinsip dasarnya sebagai algoritma stream cipher yang menggunakan kunci simetris untuk mengenkripsi dan mendekripsi data dengan cepat. RC4 memiliki kecepatan dan efisiensi dalam proses enkripsi, namun rentan terhadap serangan kriptoanalisis, terutama terkait dengan kunci yang lemah dan pola kekunci yang dapat diprediksi. Meskipun demikian, dengan penggunaan kunci yang panjang dan variasi yang baik, tingkat keamanan RC4 masih dapat dianggap memadai untuk aplikasi umum. Dalam penelitian yang dilakukan, pengujian CrackStation tidak dapat memecahkan ciphertext yang dihasilkan oleh algoritma RC4, menunjukkan bahwa implementasinya berhasil dalam mengamankan dokumen digital.

14	(Nathues & Hoffmann, n.d.)	Vigenere cipher adalah metode enkripsi simetris yang menggunakan kata kunci untuk mengenkripsi dan mendekripsi pesan dengan menggabungkan teks asli dan kata kunci melalui penjumlahan modular, membuatnya lebih sulit dipecahkan dibanding cipher substitusi sederhana. Kekuatan utamanya terletak pada kata kunci yang panjang dan bervariasi, mengurangi efektivitas analisis frekuensi. Namun, kelemahannya muncul jika kata kunci pendek atau diketahui penyerang, memungkinkan metode seperti analisis koincidensi atau Kasiski untuk memecahkannya. Meskipun lebih aman daripada cipher substitusi sederhana, Vigenere cipher tetap rentan terhadap serangan kriptografi modern, terutama jika kata kuncinya pendek atau tidak acak.
15	(Bahri et al., 2023)	Vigenere cipher adalah metode enkripsi polialfabetik yang menggunakan Vigenere Square untuk mengubah setiap karakter plaintext berdasarkan karakter kunci,Kelebihannya termasuk penggunaan kunci berulang dan kerumitan polialfabetik, sedangkan kelemahannya adalah rentan terhadap metode Kasiski dan analisis frekuensi jika kunci pendek atau digunakan berulang. Kombinasi Vigenere cipher dengan Route cipher, dikenal sebagai super enkripsi, meningkatkan keamanan dengan menambahkan lapisan transposisi ke substitusi, sehingga meskipun satu metode dipecahkan, pesan tetap terlindungi. Penelitian menunjukkan implementasi super enkripsi menggunakan PHP efektif dalam meningkatkan keamanan pesan digital.

4.1 Prinsip Dasar

Prinsip dasar dari kriptografi klasik Vigenere Cipher dan kriptografi modern RC4 berbeda dalam hal metode enkripsi dan kunci yang digunakan. Metode enkripsi Pada kriptografi klasik Vigenere Cipher merupakan metode substitusi polialfabetik di mana setiap huruf teks terbuka digantikan oleh huruf lain berdasarkan kunci yang terdiri dari sebuah kata atau frasa. Cara kerjanya adalah dengan menggeser setiap huruf teks terbuka berdasarkan posisi huruf pada kunci. Misalnya, jika huruf pada teks terbuka adalah *p* dan huruf pada kunci adalah *k*, maka enkripsinya adalah $c = (p+k) \bmod 26$, dimana *c* adalah huruf terenkripsi(Dimas Krisna Maulana : 2023). Dan Kunci yang digunakan pada Vigenere Cipher adalah kunci simetris yang dapat digunakan untuk pengkodean pesan.(Dwi Rahmasari Kinasih Gusti : 2020)

Sementara metode enkripsi pada kriptografi modern RC4 adalah algoritma enkripsi yang berbasis pada aliran (stream) yang memproduksi deretan byte acak (keystream). Algoritma ini menggunakan kunci untuk menginisialisasi keadaan internal, dan dari keadaan ini, sebuah keystream yang panjangnya setara dengan teks terbuka dihasilkan. Teks terbuka kemudian dienkripsi dengan menggunakan XOR (exclusive OR) antara teks terbuka dan keystream. Dan Kunci yang digunakan pada RC4 adalah urutan bit (biasanya dalam bentuk byte) yang digunakan untuk menghasilkan keystream. Kunci ini harus rahasia dan disepakati di antara pihak yang terlibat dalam komunikasi. Algoritma RC4 stream cipher terbagi menjadi dua tahap, yaitu key setup dan stream generation. Dalam key setup, ada tiga proses yakni Inisialisasi S-Box, penyimpanan key dalam key byte array, dan permutasi pada S-Box. Sedangkan pada stream generation, nilai pseudorandom dihasilkan untuk kemudian digunakan dalam operasi XOR untuk menghasilkan ciphertext atau plaintext tergantung pada konteksnya(Febriyani & Arfriandi, 2021).

Perbedaan mendasar antara Vigenere Cipher dan RC4 adalah pada teknik enkripsi dan penggunaan kunci. Vigenere Cipher menggunakan teknik substitusi polialfabetik dengan kunci berulang, sedangkan RC4 menggunakan algoritma aliran dengan keystream yang dihasilkan dari kunci untuk melakukan enkripsi data.

4.2 ***Kekuatan dan Kelemahan***

Vigenere Cipher memiliki beberapa kekuatan dalam keamanan jaringan komputer seperti dalam implementasi, vigenere cipher relatif mudah diimplementasikan dan dipahami karena metode vigenere cipher menyembunyikan pesan berupa teks melalui teknik substitusi dengan mengubah setiap huruf menjadi huruf lain berdasarkan kunci yang digunakan. Vigenère cipher adalah salah satu algoritma kriptografi klasik yang menggunakan metode substitusi abjad majemuk. Substitusi abjad-majemuk mengenkripsi setiap huruf yang ada menggunakan kunci yang berbeda.(Hidayah et al., 2023)

Vigenere Cipher dapat mengatasi kelemahan analisis frekuensi yang ada pada cipher substitusi sederhana seperti Caesar Cipher. Ini karena Vigenere Cipher menggunakan kunci polialfabetik yang membuat pola pergeseran huruf lebih kompleks.

Selanjutnya terdapat pula kelemahan dari vigenere cipher seperti rentan terhadap analisis kasar, meskipun lebih kuat daripada cipher substitusi sederhana, Vigenere Cipher masih rentan terhadap analisis kasar (brute-force attack) jika panjang kunci tidak terlalu panjang dan pola berulang, jika panjang kunci relatif pendek dan berulang, pola pergeseran huruf dapat ditemukan dengan metode kriptanalisis yang lebih canggih.

Dalam keamanan kriptografi modern, RC4 memiliki reputasi yang unik karena kekuatan operasi XOR yang kompleks. Namun demikian, seperti halnya banyak

algoritma, RC4 juga perlu dipertimbangkan untuk digunakan. Salah satu kelebihan utama dari RC4 adalah pada teknik operasi XOR yang dilakukan tidak hanya dengan kunci, tetapi juga melibatkan proses pemindahan bit dari posisi kiri ke kanan untuk mengacak posisi biner yang dihasilkan. Proses ini terjadi berantai pada setiap blok plain dan cipher, menambah tingkat keamanan dalam operasi enkripsi. Namun, RC4 juga memiliki beberapa kelemahan yang signifikan. Salah satunya adalah rentan terhadap teknik serangan know-plaintext attack, di mana penyerang menggunakan pengetahuan tentang teks terbuka untuk mendekripsi pesan. Selain itu, RC4 juga mudah diserang dengan teknik ciphertext-only attack, di mana penyerang hanya memiliki akses ke ciphertext tanpa pengetahuan tentang teks terbuka. Kedua serangan ini dapat mengancam keamanan data yang dienkripsi menggunakan algoritma RC4.

4.2 Tingkat Keamanan

Perbandingan tingkat keamanan antara kriptografi klasik Vigenere Cipher dan kriptografi modern RC4 dalam penggunaan pada jaringan komputer, terdapat beberapa perbedaan utama dari vigenere cipher yaitu keamanan vigenere cipher, meskipun Vigenere Cipher mengatasi analisis frekuensi yang mudah dilakukan pada cipher substitusi sederhana, ia tetap rentan terhadap analisis kasar jika panjang kunci tidak cukup panjang. Pola berulang pada kunci dapat dieksploitasi untuk mencoba menebak teks terbuka. Kekuatan Vigenere Cipher lebih cocok digunakan untuk keamanan sederhana dan tidak cocok untuk keamanan modern di lingkungan jaringan komputer. Keamanannya terbatas oleh panjang kunci dan repetisi pola kunci.

Perbandingan utama dari RC4 yaitu keamanan RC4 memiliki sejumlah kelemahan keamanan yang signifikan. Salah satunya adalah kerentanannya terhadap serangan terhadap kunci terkait (key-scheduling algorithm) yang dapat membocorkan informasi tentang keystream dan akhirnya mengungkapkan teks terbuka. Kekuatan RC4 dikenal karena kecepatan dan fleksibilitasnya, tetapi telah diketahui memiliki masalah keamanan yang serius. Beberapa serangan terhadap RC4 telah dikembangkan, dan algoritma ini tidak lagi direkomendasikan untuk keamanan data yang tinggi dalam pengaturan modern.

Kedua nya dibandingan dan menghasilkan bahwa secara umum, kriptografi modern seperti RC4, meskipun dapat digunakan dengan kunci yang panjang dan dianggap lebih kompleks daripada Vigenere Cipher, memiliki masalah keamanan yang signifikan. Dalam penggunaan pada jaringan komputer, penting untuk memilih algoritma kriptografi yang aman, terbukti, dan disarankan oleh standar keamanan terkini. Vigenere Cipher dan RC4, meskipun menarik dari segi sejarah dan implementasi, umumnya tidak memenuhi standar keamanan modern dan oleh karena itu kurang disarankan untuk digunakan dalam jaringan komputer yang membutuhkan keamanan yang tinggi.

5. KESIMPULAN DAN SARAN

Dari hasil penelitian, dapat disimpulkan bahwa Vigenere Cipher dan RC4 memiliki kekuatan dan kelemahan masing-masing dalam keamanan jaringan komputer. Vigenere Cipher mudah diimplementasikan dan dapat mengatasi kelemahan analisis frekuensi yang mudah dilakukan pada cipher substitusi sederhana, namun masih rentan terhadap serangan brute-force dan analisis pola jika panjang kunci tidak cukup panjang. Sedangkan RC4 adalah algoritma stream cipher yang cepat dan fleksibel, namun memiliki kelemahan keamanan yang signifikan, seperti kerentanan terhadap serangan terhadap kunci terkait dan kualitas keystream yang tidak ideal. Dalam perbandingan umum, kriptografi modern seperti RC4 memiliki masalah keamanan yang signifikan meskipun dapat digunakan dengan kunci yang panjang dan dianggap lebih kompleks daripada Vigenere Cipher. Dalam penggunaan dalam jaringan komputer, penting untuk memilih algoritma kriptografi yang aman, terbukti, dan disarankan oleh standar keamanan terkini. Vigenere Cipher dan RC4, meskipun menarik dari segi sejarah dan implementasi, umumnya tidak memenuhi standar keamanan modern dan kurang disarankan untuk digunakan dalam jaringan komputer yang membutuhkan keamanan yang tinggi.

SARAN

Dalam mengambil keputusan tentang penggunaan kriptografi, perlu diperhatikan standar keamanan modern dan rekomendasi dari organisasi keamanan terkemuka. Selain itu, perlu diingat bahwa tidak ada kriptografi yang absolut aman, melainkan hanya mengurangi resiko keamanan. Oleh karena itu, penting untuk melakukan pembaruan dan pengujian kriptografi secara berkala.

Selain kriptografi, keamanan jaringan komputer dapat ditingkatkan dengan melakukan pengelolaan risiko, penggunaan firewall, pendeteksian serangan, dan pengamanan fisik. Selain itu, penting untuk melakukan edukasi dan latihan kepada pengguna terhadap ancaman keamanan.

DAFTAR PUSTAKA

Aisyiah, J., Priyambodo, B., Faridah, B., Yanuarima, A., Sudi, G. G., Pamungkas, K., & Alfina, R. (2023). Penerapan Algoritma Vigenere Cipher Untuk Keamanan Data Peresepan Obat. *Jurnal Informatika-COMPUTING*, *10*(1), 1–6. https://ejournal.unibba.ac.id/index.php/computing/article/view/1113

Alfan, M., Sutardi, S., & Pramono, B. (2021). Enkripsi Data Qr Code Menggunakan Metode Rc4 Pada Aplikasi Presensi Jurusan Teknik Informatika Universitas Halu Oleo. *SemanTIK*, *7*(2), 191. https://doi.org/10.55679/semantik.v7i2.8927

Azura, S., Tahir, M., Lestari, A. D., Sakia Mardiana, A., Turrofifah, A., Susanti, K. N., & Rohman, S. (2023). Penerapan Kemanan Data Text menggunakan Metode Kriptografi Vigener Chiper Berbasis Web. *Digital Transformation Technology (Digitech) | E*, *3*(1), 20–28.

https://doi.org/10.47709/digitech.v3i1.2311

Bahri, S., Jihan, F., & Rudianto, B. (2023). Implementasi Algoritma Super Enkripsi Vigenere Cipher Dan Route Cipher Pada Penyandian Pesan Teks. *Jurnal Matematika UNAND*, *12*(2), 168–175.

Belakang, L. (2023). *Metode algoritma rc4 (rivest code 4) untuk pengamanan database transaksi pada glory digital sablon*. *13*(1).

Busran, & Jeri Widodo Putra. (2021). Analisa Komputasi Algoritma Des Dengan Rc4 Untuk Keamanan Data. *Jurnal Teknoif Teknik Informatika Institut Teknologi Padang*, *9*(1), 20–23. https://doi.org/10.21063/jtif.2021.v9.1.20-23

Dimas Mayoni Aji Sasono, Muhlis Tahir, Fathricia Angel M. V., Mar'atul Azizah, Luluk Fariska Utami, & Nurul Septiana. (2023). Perbandingan Kriptography Klasik Caesar Cipher Dengan Kriptography Modern Aes Dalam Tingkat Keamanan Jaringan Komputer. *Jurnal Informasi, Sains Dan Teknologi*, *6*(1), 72–77. https://doi.org/10.55606/isaintek.v6i1.93

Fatma, Y., Reny Medikawati T, Yoze Rizki, & Bagas Tri Ramadana. (2023). Perbandingan algoritma kriptografi simon dan vigenere dalam mengamankan citra digital. *Jurnal CoSciTech (Computer Science and Information Technology)*, *4*(1), 299–305. https://doi.org/10.37859/coscitech.v4i1.4958

Febriyani, F. S., & Arfriandi, A. (2021). Implementasi Algoritma RC4 pada Sistem Pengamanan Dokumen Digital Soal Ujian. *JISKA (Jurnal Informatika Sunan Kalijaga)*, *6*(3), 171–177. https://doi.org/10.14421/jiska.2021.6.3.171-177

Gusti, D. R. K., Santoso, K. A., & Kamsyakawuni, A. (2020). Vigenere Cipher Dengan Modifikasi Plaintext. *Majalah Ilmiah Matematika Dan Statistika*, *20*(1), 15. https://doi.org/10.19184/mims.v20i1.17219

Hidayah, V. M., Mulyana, D. I., & Bachtiar, Y. (2023). Algoritma Caesar Cipher atau Vigenere Cipher pada Pengenkripsian Pesan Teks. *Journal on Education*, *5*(3), 8563–8573. https://doi.org/10.31004/joe.v5i3.1647

Imam Riadi, Abdul Fadlil, & Fahmi Auliya Tsani. (2022). Pengamanan Citra Digital Berbasis Kriptografi Menggunakan Algoritma Vigenere Cipher. *JISKA (Jurnal Informatika Sunan Kalijaga)*, *7*(1), 33–45. https://doi.org/10.14421/jiska.2022.7.1.33-45

Nathues, A., & Hoffmann, M. (n.d.). *Implementation of RC4 Cryptography Algorithm for Data File Security Implementation of RC4 Cryptography Algorithm for Data File Security*. 0–6. https://doi.org/10.1088/1742-6596/1569/2/022080

Ngemba, H. R., Ulhaq, M. N. D., Hendra, S., Azhar, R., Alamsyah, A., & Laila, R. (2024). Implementasi Algoritma Rc4 Pada Sistem Informasi Koperasi Virtual Bawaslu Provinsi Sulawesi Tengah Virtual Bawaslu. *PROSISKO: Jurnal Pengembangan Riset Dan Observasi Sistem Komputer*, *11*(1), 98–103. https://doi.org/10.30656/prosisko.v11i1.8182

Noviyanti. P, & Mira. (2022). Analisa Algoritma Kriptografi Klasik Caesar Cipher Viginere Cipher dan Hill Cipher – Study Literature. *Journal of Information Technology*, *2*(1), 23–30. https://doi.org/10.46229/jifotech.v2i1.387

Nurmadjid, R. (2023). *Penerapan Kriptografi Rc4 Untuk Pengamanan Application of Rc4 Cryptography for Document Security*. *2*(September), 9–17.

Rista, & Samuel Sitio, A. (2021). Rista 1 , Arjon Samuel Sitio 2 [Implementasi Keamanan Data Keuangan di SMK Swasta Musda Perbaungan Menggunakan Metode RC4. *Jurnal Ilmu Komputer Dan Sistem Informasi (JIKOMSI)*, *3*(3), 60–66.

Utami Rukmaliani, Rosnita, M. A. (2020). Pengaruh Model Pembelajaran Inkuiri Terhadap Proses Siswa pada Mata Pelajaran IPA. *Jurnal EduFisika*, *01*(02), 1–10.

Yanuba, F. S., Tahir, M., Fadli, M. K., Nafasa, F. N., & Zahrah, S. A. (2023). *Implementasi Algoritma Kriptografi RC4 Untuk Keamanan Database Aplikasi Voting Pemilihan Ketua Umum Berbasis WEB*. *3*, 1–9.

Zawacki-Richter, O., Kerres, M., Bedenlier, S., Bond, M., & Buntins, K. (2019). Systematic Reviews in Educational Research: Methodology, Perspectives and Application. In *Systematic Reviews in Educational Research: Methodology, Perspectives and Application* (Issue November). https://doi.org/10.1007/978-3-658-27602-7