

Analisis Perbandingan Kinerja Enkripsi Algoritma RC4 Dan AES

Feri Kusuma Wardhana*¹, Ardi Kurniawan², Bintang Radityo Seto³, Indrawan Ady Saputro⁴

¹²³⁴Informatika, STMIK AMIKOM Surakarta

¹²³⁴Sukoharjo, Indonesia

Email: ¹feriwardhana41@gmail.com, ²kurniawanardi091@gmail.com,
³bintangradityo84@gmail.com, ⁴indrawanadys@dosen.amikomsolo.ac.id

Abstract

Cryptography has a function to secure data by hiding messages in a form that cannot be seen without the correct key. There are several algorithms used to perform encryption including AES, DES, RC4, RSA and others. This research addresses the comparison of encryption performance between RC4 and AES algorithms on various file types, such as MP3, AVI, DOCX, MP4, and IMG. The research problem involves evaluating speed, encryption file size, and data security. The research objective is to understand the differences in encryption time, file size, and security between RC4 and AES. The research method includes problem identification, data collection, and result analysis using RC4 and AES algorithms. Results show that RC4 has better encryption speed, while AES takes longer. The file size encrypted with RC4 remains the same, while AES produces a different size. In conclusion, the choice between RC4 and AES should consider the balance between security and efficiency, with special consideration regarding encryption time and file size.

Keywords: Cryptography, Secure data, encryption, RC4, AES.

Abstraksi

Kriptografi memiliki fungsi untuk melakukan pengamanan data dengan menyembunyikan pesan dalam bentuk yang tidak dapat dilihat tanpa kunci yang benar. Algoritma yang digunakan untuk melakukan enkripsi ada beberapa antara lain AES, DES, RC4, RSA dan lainnya. Penelitian ini membahas perbandingan performa enkripsi antara algoritma RC4 dan AES pada berbagai jenis file, seperti MP3, AVI, DOCX, MP4, dan IMG. Masalah penelitian melibatkan evaluasi kecepatan, ukuran file enkripsi, dan keamanan data. Tujuan penelitian adalah memahami perbedaan dalam waktu enkripsi, ukuran file, dan keamanan antara RC4 dan AES. Metode penelitian mencakup identifikasi masalah, pengumpulan data, dan analisis hasil menggunakan algoritma RC4 dan AES. Hasil menunjukkan bahwa RC4 memiliki kecepatan enkripsi lebih baik, sementara AES memerlukan waktu lebih lama. Ukuran file enkripsi dengan RC4 tetap sama, sedangkan AES menghasilkan ukuran yang berbeda. Kesimpulannya, pemilihan antara RC4 dan AES harus mempertimbangkan keseimbangan antara keamanan dan efisiensi, dengan pertimbangan khusus terkait waktu enkripsi dan ukuran file.

Kata Kunci: Kriptografi, Keamanan Data, Enkripsi, RC4, AES.

1. PENDAHULUAN

Keamanan data merupakan sebuah proses untuk melindungi sebuah data dari akses yang tidak memiliki sebuah akses, tidak memiliki penggunaan atau perubahan yang tidak diinginkan. Salah satu pengamanan data adalah dengan kriptografi bisa menyembunyikan sebuah pesan menjadi sebuah data lain sehingga dapat diterapkan untuk mengamankan sebuah jenis file [1]. Kriptografi adalah ilmu dan seni mengamankan komunikasi serta melindungi informasi dari akses yang tidak sah atau modifikasi oleh pihak-pihak yang tidak berwenang. Kriptografi berfungsi untuk menyembunyikan makna dari suatu pesan agar hanya penerima yang dituju yang dapat membacanya dengan jelas. Secara lebih luas, kriptografi juga mencakup berbagai teknik dan algoritma untuk mengamankan data, mengenkripsi, dan mendekripsi informasi [2].

Mengevaluasi beragam teknik enkripsi simetris dan melakukan perbandingan pada aspek-aspek tertentu, seperti efek yang diperoleh melalui variasi kunci atau teks biasa, merupakan fokus analisis yang telah dilakukan [3]. Sebuah penelitian telah dilakukan untuk menyelidiki kombinasi antara Rc4 dan AES, dengan banyak teori yang diuraikan untuk potensi pengembangan algoritma baru dalam konteks ini.

Proteksi data melibatkan penerapan algoritma kriptografi, termasuk teknik modern seperti substitusi dan transposisi. Dua algoritma yang sering digunakan dalam konteks ini adalah AES dan RC4 [4]. Penelitian sebelumnya telah secara luas mengulas strategi pengamanan informasi menggunakan algoritma kriptografi ini [5]. Saat ini, banyak yang memilih algoritma AES sebagai solusi untuk menjaga kerahasiaan data, memastikan bahwa hanya pihak tertentu yang berwenang dapat mengakses atau mengetahui isinya [6]. AES, sebagai salah satu algoritma kriptografi modern, berperan dalam mengenkripsi dan mendekripsi informasi dalam bentuk blok ciphertext simetris, menjadikannya pilihan utama untuk pengamanan data yang bersifat rahasia [7].

Terdapat suatu proses yang melibatkan algoritma Advanced Encryption Standard (AES) dalam praktik enkripsi dan dekripsi. Ada empat tipe transformasi bytes yang terlibat dalam proses ini. Pada tahap awal enkripsi, input yang telah disalin ke dalam state mengalami konversi byte yang disebut sebagai AddRoundKey. Proses konversi byte melibatkan iterasi dari SubBytes, ShiftRows, MixColumn, dan AddRoundKey sebanyak Nr kali, di mana Nr menunjukkan jumlah putaran. Proses ini dikenal sebagai fungsi pembulatan [8].

Metode RC4 dirancang oleh Ron Rivest pada tahun 1987. Keunggulan dari RC4 terletak pada kombinasi kecepatan dan kesederhanaan algoritmanya dalam menangani berbagai aplikasi, sehingga memudahkan implementasinya baik dalam perangkat keras maupun perangkat lunak [9].

Selain opsi penerapan algoritma AES, keamanan data dapat diperkuat dengan memanfaatkan algoritma RC4 [10]. RC4 merupakan algoritma kriptografi berbentuk stream cipher yang digunakan untuk menginput data atau informasi pada saat tertentu,

biasanya dalam bentuk byte. Meskipun RC4 memiliki kelebihan, terdapat kelemahan yang perlu diwaspadai, seperti Bit-Flipping Attack (BFA) yang berpotensi memungkinkan seorang penyerang mendapatkan plaintext tanpa mengetahui kunci enkripsi [4].

Proses pengamanan dalam kriptografi membutuhkan sebuah algoritma enkripsi. Algoritma enkripsi memiliki banyak macam dan ragamnya antara lain algoritma DES, 3DES, AES, RSA, ECC, dan Algoritma enkripsi Rc4 [11]. Penelitian terkait algoritma enkripsi RC4 diterapkan pada proses pemesanan transaksi online untuk menyembunyikan data transaksi pelanggan. Hasil dari penelitian tersebut menunjukkan bahwa algoritma RC4 dapat diterapkan dan memiliki performa yang baik serta waktu pemrosesan data dari algoritma RC4 dipengaruhi oleh Panjang kunci [12]. Penelitian lainnya mengimplementasikan algoritma RC4 untuk file .docx, .pdf, .xls, .txt mendapatkan hasil bahwa waktu dan hasil dari enkripsi pesan menunjukkan tingkat keamanan yang lebih baik [13]. Algoritma RC4 adalah cipher aliran yang kerap digunakan secara luas untuk sistem keamanan, misal: protokol Secure Socket Layer (SSL) [14]. Algoritma kriptografi ini sederhana serta mudah diimplementasikan [15]. Rc4 diciptakan oleh Ron Rivest di laboratorium RSA. Penelitian lainnya [16] tentang pengamanan data menggunakan algoritma AES, algoritma tersebut dapat menjaga data dari serangan pasing dengan hasil persentasi 50% dengan panjang teks sekitar 16 karakter. Penelitian lainnya [17] tentang AES menerapkan algoritma AES kedalam aplikasi SMS untuk membuat enkripsi pesan agar tidak dibaca oleh orang lain. Algoritma AES juga diterapkan pada keamanan jaringan internet of things dan menghasilkan tingkat keamanan yang lebih baik [18]. AES ini terdiri dari tiga penyandian blok yaitu AES-128, AES-192, dan AES-256, pertama kali dipublikasikan pada tahun 1998 [19]. Menurut Amita Pandey [20], konsep dasar dari Kriptografi adalah sebagai berikut :

1. Plain text : Pesan asli yang ingin sampaikan sebagai teks biasa
2. Chiper text : Pesan yang tidak bisa dipahami oleh siapapun yang dideniiskan sebagai teks sandi
3. Enkripsi :Proses mengubah teks biasa menjadi teks sandi yang membutuhkan dua . yaitu algoritma enkripsi dan kunci
4. Deskripsi : Proses Mengubah teks sandi menjadi teks biasa
5. Key : Sebuah kombinasi numerik atau alfa numerik teks atau symbol khusus disebut sebagai kunci

Pada penelitian ini melakukan perbandingan performa dari proses enkripsi file bentuk .avi, .mp4, .mp3, .docx berbeda penelitian sebelumnya yang hanya melakukan proses enkripsi hanya menggunakan file sejenis serta tidak membandingkan performa pemrosesan antara algoritma Rc4 dan AES.

2. METODE PENELITIAN

Tahap penelitian yang dilakukan pada penelitian ini adalah melakukan identifikasi masalah, pengumpulan data, melakukan enkripsi, hasil enkripsi dan kesimpulan. Alur penelitian tersaji pada Gambar 1.

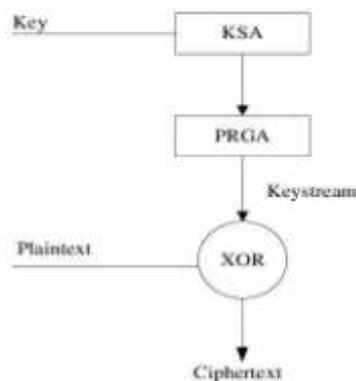


Gambar 1. Alur Penelitian

Algoritma Enkripsi yang digunakan dalam penelitian ini adalah Algoritma RC4 dan AES. Berikut ini alur dan pembahasan terkait dengan algoritma enkripsi RC4 dan AES :

A. Algoritma RC4

Algoritma RC4 atau disebut dengan Rivest Code 4 adalah merupakan salah satu algoritma yang masuk dalam algoritma simetris. Algoritma Stream chipper yang melakukan enkripsi diantara kombinasi dari plainteks dengan menggunakan sebuah bit wise or. Panjang kunci dari algoritma RC4 sendiri adalah dari 1 sampai dengan 256 yang digunakan menganisialisasi tabel yang sepanjang 256 byte. Proses yang terjadi dalam Algoritma RC4 disajikan pada gambar 2.



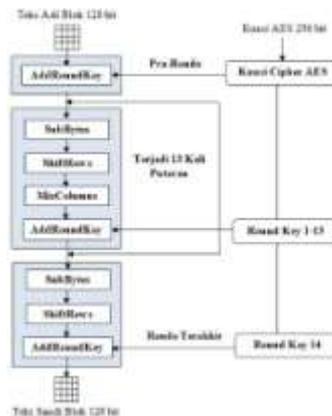
Gambar 2. Blok Diagram Algoritma RC4

Langkah-langkah umum untuk proses enkripsi dengan algoritma RC4:

1. Inisialisasi S-box, S-box adalah sebuah array dimana berukuran 256 elemen(8-bit), Pada S-box pada setiap elemennya diberi nomor dari 0 hingga 255 secara berurutan contoh misalkan $S[0]=0, S[1]=1, S[2]=2, S[3]=3, S[4]=4, \dots, S[255]=255$. Selanjutnya, akan diacak s-box berdasarkan kunci dari enkripsi yang digunakan
2. Kocok S-box(Penjadwalan Kunci), Sebuah hal terjadi sebuah konversi kunci enkripsi ke dalam bentuk dari array byte, dan jika Panjang kunci lebih pendek dari 256 byte maka akan diulangi hingga panjangnya sama dengan 256 byte, kemudian akan melakukan pengocokan S-box dengan menginterasi semua elemen s dengan cara menukar elemen $S[i]$ dengan elemen $S[i]$ yang kemudian didasarkan dengan kunci sesuai, pada sebuah proses ini hanya akan dilakukan sekali sebelum melakukan sebuah enkripsi.
3. Variable persiapan untuk melakukan enkripsi, Mulai dari awal data yang akan dilakukan enkripsi, untuk daya setiap byte yang akan dienkrispikan adalah sebuah tingkatan dari pointer $S1 (S1+1)\%256$ dan setelah kemudian nilai yang diambil dari nilai S-box merupakan indeks $S1$ simpan dalam variable i tadi, kemudian pada tingkatan pointer $S2(S2=(S2+S\text{-box}[i]\%256)$ dan kemudian nilai akan diambil dari S-box pada indeks $S2$, tersimpan dalam sebuah variable j yang tadi, kemudian setelah itu akan tukar nilai S-box pada indeks i dan j tadi, kemudian akan terjadi menghitung K stream atau sebuah kunci acak dengan mengambil sebuah elemen dari S-box dari S-box yang baru saja dapat diacak tadi dengan sebuah indeks, kemudian akan melakukan sebuah operasi XOR sebuah byte data dengan K stream untuk agar menghasilkan byte data terenkripsi.
4. Enkripsi penyelesaian, Saat semua dari data byte tadi dienkrripsi, keluaran dari daya hasil enkripsi adalah data yang sudah terenkripsi.

B. Algoritma AES

AES adalah sebuah standar enkripsi yang dimana merupakan jenis kunci simetris. AES ini terdiri dari tiga penyandian blok yaitu AES-128, AES-192, dan AES-256 pertama kali dipublikasikan pada tahun 1998. Berikut ini alur proses dari Algoritma AES dapat dilihat pada gambar 3.



Gambar 3. Alur Proses Enkripsi Algoritma AES

Proses-proses dalam melakukan enkripsi menggunakan Algoritma AES dapat sebagai berikut :

1. Input data, plainteks tersebut akan dipecah menjadi blok-blok dari data yang tentu saja sesuai dengan ukuran blok AES , yaitu 128 bit(16 byte).
2. Ekspansi Kunci, kunci enkripsi yang akan digunakan harus sesuai dengan ukuran sebuah yang diizinkan oleh AES (128- bit,192-bit,256-bit), jika sebuah kunci yang diberikan itu kurang atau tidak sesuai dengan dari ukuran yang tadi maka kunci tersebut akan di-expand yang menggunakan algoritma khusus untuk menghasilkan kunci yang sesuai.
3. Putaran awal , pada putaran awal ini , plainteks akan di-xor dengan kunci enkripsi awal
4. Putaran utama, proses enkripsi pada putaran utama terdiri dari sebuah beberapa Langkah ,termasuk subbyte , shifrowsmixcolumns, dan addroundkey . Langkah tersebut melibatkan sebuah substitusi atau perhitungan dan permutasian data dnegan menggunakan sebuah kunci dari enkripsi.
5. Final round, dan ini adalah putaran terakhir yang dengan menggunakan sebuah Langkah-langkah yang bisa dibilang sangat mirip dengan putaran utama , akan tetapi tidak adal langkah sebuah mixcolumns.
6. Output, setelah selesai terjadi pada final round, ciphertext dihasilkan

3. HASIL DAN PEMBAHASAN

Sistem yang dirancang untuk menunjang penelitian dalam enkripsi dan deskripsi algoritma AES dan Algoritma RC4. Program untuk melakukan enkripsi menggunakan Bahasa pemrograman python dimana untuk mengerjakannya menggunakan IDE Visual Studio code. Pengujian ini atau aplikasi ini digunakan pada sistem operasi windows 10. Dalam aplikasi ini dapat dilihat pengamatan waktu dari proses enkripsi dan deskripsi dari algoritma AES dan algoritma RC4. Hasil yang didapat dari aplikasi ini dapat terpengaruh

dari spesifikasi dari perangkat keras yang digunakan ini. Untuk pengujian sistem ini sendiri , langkah yang diambil untuk mempermudah dalam analisis kecepatan dalam algoritma kriptografi yang di analisis . langkahnya adalah

1. Sampel yang digunakan berbeda-beda jenis dari file mp4 ,mp3,docx, kemudian .avi
2. Mengukur waktu yang dibutuhkan untuk melakukan enkripsi dan deskripsi
3. Melakukan / menghitung ukuran dari file yang telah di enkripsi maupun yang sudah dideskripsi.

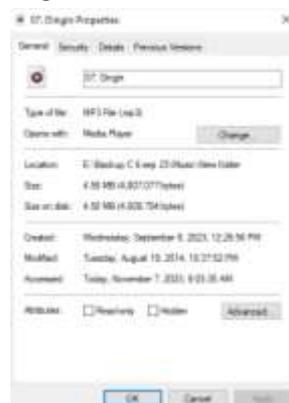


Gambar 4. Aplikasi Enkripsi Algoritma RC4 dan AES

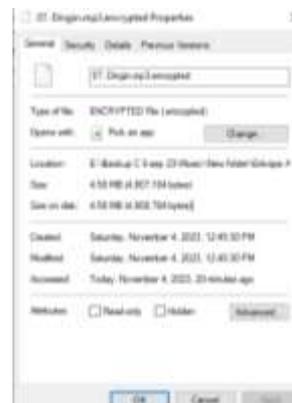
Simulasi perbandingan algoritma enkripsi RC4 dan AES dilakukan pada beberapa file yang beragam sehingga bisa melihat perbedaan ukuran file yang nanti dienkripsi yaitu file mp3, .avi, .docx, .mp4, .img.

3.1. Perbandingan ukuran file asli dengan data enkripsi

Berdasarkan hasil perbandingan ukuran file asli memiliki ukuran data yang sama dengan algoritma RC4 sedangkan enkripsi menggunakan algoritma AES menghasilkan ukuran data yang berubah dan berbeda dengan file aslinya. Pada gambar 5 dan gambar 6 menunjukkan ukuran file asli mengalami perubahan ukuran setelah dilakukan enkripsi menggunakan algoritma AES.



Gambar 5. File Asli MP3

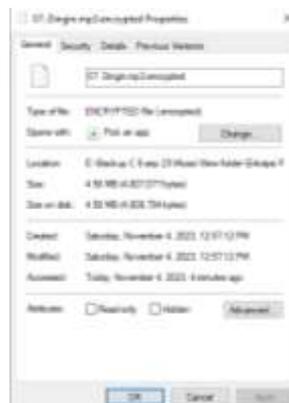


Gambar 6. File MP3 yang di enkripsi

Berikut ini pada gambar 7 dan gambar 8 menunjukkan bahwa ukuran file setelah dilakukan enkripsi dengan Algoritma RC4 ukuran file tidak mengalami perubahan ukuran file.



Gambar 7. File Asli MP3



Gambar 8. File MP3 yang di enkripsi

3.2. Hasil dari Perbandingan Algoritma AES dan RC4

Pada proses membandingkan algoritma menggunakan 5 jenis file yang berbeda yaitu jenis file MP3, AVI, DOCX, MP4 dan file IMG. Hasil dari perbandingan didapatkan bahwasanya enkripsi dengan menggunakan algoritma RC4 menghasilkan ukuran byte yang sama dengan file aslinya. Sedangkan hasil dari algoritma AES menghasilkan nilai byte yang berbeda dengan file aslinya. Berikut ini hasil perbandingan dari kedua algoritma yang tersaji pada tabel 1.

Tabel 1. Perbandingan ukuran file enkripsi antara Algoritma RC4 dan AES :

No	Jenis File	Ukuran File Asli	Enkripsi dengan Algoritma RC4	Enkripsi dengan Algoritma AES
1	MP3	4.807.077 bytes	4.807.077 bytes	4.807.104 bytes
2	AVI	323.032.092 bytes	323.032.092 bytes	323.032.112 bytes
3	DOCX	3.204.893 bytes	3.204.893 bytes	3.204.912 bytes
4	MP4	86.435.836 bytes	86.435.836 bytes	86.435.856 bytes
5	IMG	80.811 bytes	80.811 bytes	80.832 bytes

Dalam menganalisis data perbandingan ukuran file enkripsi antara algoritma RC4 dan AES, kita dapat mengamati beberapa hal berikut:

- Terlihat bahwa ukuran file enkripsi dengan AES sedikit lebih besar daripada ukuran file enkripsi dengan RC4. Ini bisa disebabkan oleh overhead yang diperlukan oleh algoritma AES untuk menyertakan informasi keamanan tambahan.
- Seperti pada kasus MP3, ukuran file enkripsi dengan AES juga sedikit lebih besar. Ini dapat menjadi indikasi bahwa AES memerlukan lebih banyak overhead untuk memberikan tingkat keamanan yang lebih tinggi.

- Seperti pada kasus sebelumnya, perbedaan ukuran file enkripsi antara RC4 dan AES pada jenis file DOCX juga sangat kecil. Kembali, terdapat perbedaan kecil dalam ukuran file enkripsi, menunjukkan bahwa AES memerlukan sedikit lebih banyak ruang untuk memberikan keamanan tambahan. Ukuran file enkripsi dengan AES kembali sedikit lebih besar daripada RC4, meskipun perbedaannya kecil. Dalam menganalisis data perbandingan kinerja proses waktu enkripsi antara algoritma RC4 dan AES pada berbagai jenis file, kita dapat memperhatikan beberapa aspek kunci:
- Pada jenis file MP3, terlihat bahwa AES membutuhkan waktu yang lebih lama untuk proses enkripsi dibandingkan dengan RC4. Kemungkinan ini terjadi karena AES adalah algoritma yang lebih kompleks dan melibatkan proses enkripsi yang lebih rumit.
- Untuk jenis file AVI, hasilnya serupa dengan MP3, di mana AES kembali memerlukan waktu lebih lama dibandingkan RC4. Ini dapat disebabkan oleh kompleksitas dan keamanan yang lebih tinggi dari algoritma AES.
- Pada jenis file DOCX, perbedaan waktu enkripsi antara RC4 dan AES sangat kecil. Ini mungkin menunjukkan bahwa kompleksitas file ini tidak memberikan keuntungan signifikan kepada AES dalam hal waktu enkripsi.
- Mirip dengan MP3 dan AVI, AES juga memerlukan lebih banyak waktu untuk jenis file MP4. Kemungkinan besar, ini disebabkan oleh sifat kompleks algoritma AES yang dirancang untuk memberikan tingkat keamanan yang lebih tinggi.
- Pada jenis file IMG, kedua algoritma memiliki waktu enkripsi yang sama (0 detik). Ini bisa terjadi karena file tersebut mungkin memiliki sifat tertentu yang membuat enkripsi dengan kedua algoritma menjadi sangat cepat atau mungkin file tersebut tidak dienkripsi sama sekali.

Hasil dari perbandingan waktu proses enkripsi pada kedua algoritma didapatkan bahwasanya enkripsi dengan menggunakan algoritma RC4 memiliki pemrosesan waktu yang lebih baik daripada algoritma AES. Sedangkan hasil dari algoritma AES memiliki waktu yang lebih lambat daripada RC4. Algoritma RC4 memiliki kecepatan lebih baik daripada algoritma AES yang tersaji pada tabel 2.

Tabel 2. Perbandingan Kinerja Proses Waktu Enkripsi antara Algoritma RC4 dan AES :

No	Jenis File	Lama waktu proses enkripsi dengan Algoritma RC4	Lama waktu proses enkripsi dengan Algoritma AES
1	MP3	0.01563 detik	0.03808 detik
2	AVI	1.39071 detik	1.78137 detik
3	DOCX	0.03116 detik	0.03125 detik
4	MP4	0.35939 detik	0.48441 detik
5	IMG	0.00000 detik	0.00000 detik

4. KESIMPULAN

Berdasarkan hasil pembahasan algoritma RC4 memiliki kecepatan enkripsi lebih cepat dibanding AES untuk berbagai jenis file seperti avi, mp3, doc, dan mp4. Meskipun ukuran file enkripsi dengan RC4 tetap, AES mengalami perubahan pada ukuran file aslinya. Meskipun AES memerlukan lebih banyak waktu untuk proses enkripsi, keamanan yang lebih tinggi membuatnya sering dipilih. Perbedaan ukuran file enkripsi menunjukkan bahwa AES memerlukan lebih banyak ruang penyimpanan untuk informasi keamanan tambahan. Dalam memilih antara RC4 dan AES, keputusan sebaiknya didasarkan pada keseimbangan antara keamanan dan efisiensi penggunaan ruang penyimpanan, dengan memahami bahwa kecepatan bukanlah satu-satunya pertimbangan.

DAFTAR PUSTAKA

- [1] Qammaddin and S. Sallu, "Keamanan Data Pembelajaran Online Jaringan Komputer Di Perguruan Tinggi," *Instruksional*, vol. 2, no. 1, p. 35, 2020, doi: 10.24853/instruksional.2.1.35-40.
- [2] I. Febriana and G. Aji, "Penerapan Teknik Kriptografi Pada Keamanan SMS Android," *JOEICT (Jurnal Educ. Inf. Commun. Technol.)*, vol. 1, no. 1, pp. 29–36, 2017.
- [3] P. KevalKetan and V. . Vijayarajan.V, "An Amalgam Approach using AES and RC4 Algorithms for Encryption and Decryption," *Int. J. Comput. Appl.*, vol. 54, no. 12, pp. 29–36, 2012, doi: 10.5120/8619-2483.
- [4] R. Sulaiman, "Combination and comparison of AES and RC4 cryptography in least significant bit (LSB) method in digital image to improve message security," *J. Inform.*, vol. 12, no. 2, p. 45, 2018, doi: 10.26555/jifo.v12i2.a8667.
- [5] S. C.P, S. T, and U. G, "A Study of Various Steganographic Techniques Used for Information Hiding," *Int. J. Comput. Sci. Eng. Surv.*, vol. 4, no. 6, pp. 9–25, 2013, doi: 10.5121/ijcses.2013.4602.
- [6] A. Prasetyo and R. Pradana, "PENERAPAN ALGORITME AES - 128 UNTUK PENGAMANAN FILE PADA SMKN 1 KOTA TANGERANG IMPLEMENTATION OF AES-128 ALGORITHM FOR FILE SECURITY AT SMKN 1 TANGERANG CITY," *SENAFTI*, vol. 2, no. September, pp. 324–331, 2023.
- [7] B. Schneier, J. Kelsey, D. Whiting, D. Wagner, C. Hall, and N. Ferguson, "Performance Comparison of the {AES} Submissions," *Second AES Candidate Conf. {NIST}*, pp. 15–34, 1999, [Online]. Available: <https://ieeexplore-ieee-org.glos.idm.oclc.org/document/5966408>
- [8] D. Calista, A. Farissi, and M. Diana Marieska, "Sistem Pengamanan Data Menggunakan Kriptografi AES dan Blockchain Berbasis Android," *J. JUPITER*, vol. 13, no. 2, pp. 220–226, 2021.
- [9] P. Jindal and B. Singh, "RC4 encryption - A literature survey," *Procedia Comput. Sci.*, vol. 46, no. Icict 2014, pp. 697–705, 2015, doi: 10.1016/j.procs.2015.02.129.
- [10] A. Farisi, "Analisis Kinerja Algoritma Kriptografi Kandidat Advanced Encryption Standard (AES) pada Smartphone," *JATISI (Jurnal Tek. Inform. dan Sist. Informasi)*,

- vol. 4, no. 2, pp. 199–208, 2018, doi: 10.35957/jatisi.v4i2.103.
- [11] P. Rahmadi and H. D. Yunita, "IMPLEMENTASI PENGAMANAN BASIS DATA DENGAN TEKNIK ENKRIPSI (Studi Kasus : PT . Sugar Group Companies)," *J. Cendekia*, vol. XIX, no. April, pp. 413–419, 2020, [Online]. Available: <https://jurnal.dcc.ac.id/index.php/JC/article/view/331>
- [12] K. A. Seputra and G. A. J. Saskara, "Kriptografi Simetris RC4 Pada Transaksi Online Booking Engine System," *J. Pendidik. Teknol. dan Kejuru.*, vol. 17, no. 2, pp. 286–295, 2020, [Online]. Available: <https://ejournal.undiksha.ac.id/index.php/JPTK/article/view/27096>
- [13] R. A. Umar and S. Hari, "Implementasi Algoritma Rc4 Untuk Keamanan File Berbasis Web Pada Sdit Ar Rahman," *Semin. Nas. Mhs. Fak. Teknol. Inf.*, vol. 1, no. 1, pp. 377–385, 2022, [Online]. Available: <https://senafiti.budiluhur.ac.id/index.php/senafiti/index>
- [14] M. Safaei Pour, C. Nader, K. Friday, and E. Bou-Harb, "A Comprehensive Survey of Recent Internet Measurement Techniques for Cyber Security," *Comput. Secur.*, vol. 128, p. 103123, 2023, doi: 10.1016/j.cose.2023.103123.
- [15] D. Hulu, B. Nadeak, and S. Aripin, "Implementasi Algoritma AES (Advanced Encryption Standard) Untuk Keamanan File Hasil Radiologi di RSUD Imelda Medan," *KOMIK (Konferensi ...)*, vol. 4, pp. 78–86, 2020, doi: 10.30865/komik.v4i1.2590.
- [16] A. Permana and E. Jaelani, "Implementasi Algoritma AES 128 Bit sebagai Pengaman Teks di Aplikasi Note Berbasis Android," *JEJARING J. Teknol. dan ...*, vol. 5, no. November, pp. 9–17, 2020, [Online]. Available: <https://journal.uniku.ac.id/index.php/jejaring/article/view/6716%0Ahttps://journal.uniku.ac.id/index.php/jejaring/article/viewFile/6716/3272>
- [17] C. Kirana and E. Sugianto, "Penerapan Algoritma AES dan Konversi SMS ke dalam Bahasa KHEK pada Aplikasi Enkripsi Berbasis Mobile Application," *Khazanah Inform. J. Ilmu Komput. dan Inform.*, vol. 5, no. 1, pp. 68–77, 2019, doi: 10.23917/khif.v5i1.7453.
- [18] A. Rachmayanti and W. Wirawan, "Implementasi Algoritma Advanced Encryption Standard (AES) pada Jaringan Internet of Things (IoT) untuk Mendukung Smart Healthcare," *J. Tek. ITS*, vol. 11, no. 3, 2022, doi: 10.12962/j23373539.v11i3.97042.
- [19] H. A. Sagala, "Perancangan Aplikasi Audit Internal Dengan Menerapkan Algoritma AES 128 Bit Untuk Pengamanan Data," vol. 2, no. 2, pp. 75–86, 2023, [Online]. Available: <https://ejurnal.seminar-id.com/index.php/jogtc>
- [20] S. Suhandinata, R. A. Rizal, D. O. Wijaya, P. Warren, and S. Srinjiwi, "Analisis Performa Kriptografi Hybrid Algoritma Blowfish Dan Algoritma Rsa," *JURTEKSI (Jurnal Teknol. dan Sist. Informasi)*, vol. 6, no. 1, pp. 1–10, 2019, doi: 10.33330/jurteks.v6i1.395.