JURNAL MEDIA INFORMATIKA [JUMIN]
Volume 4, Nomor 2, Juni 2023, Page 97-101
ISSN 2808-005X (media online)
Available Online at http://ejournal.sisfokomtek.org/index.php/jumin

Analisis Keamanan Data Dengan Menggunakan Kriptografi Modern Algoritma Advance Encryption Standar (AES)

Selli Oktavani[1], Fahrizal Rizky[2], Indra Gunawan[3]
[1,2,3] Teknik Informatika, STIKOM TUNAS Bangsa Pematang Siantar,Sumatera Utara
Email: [1]Sellyoktaviani585@gmail.com, [2]Fahrizalrizki1207@gmail.com, [3]indra@amiktunasbangsa.ac.id
Email Korespondensi : [1]Sellyoktaviani585@gmail.com

Abstrak− Perkembangan teknologi informasi dan komunikasi yang sangat pesat menyebabkan munculnya kemajuan. Teknologi informasi memegang peranan penting dalam berbagai bidang kehidupan, baik secara langsung maupun tidak langsung. Teknologi informasi tidak dapat dipisahkan dari berbagai aspek kehidupan manusia. Memungkinkan komunikasi dan pertukaran informasi atau data. Dengan kemajuan teknologi informasi, sangat diperlukan untuk melindungi data terhadap kerahasiaan informasi yang dipertukarkan. Kriptografi adalah studi tentang cara untuk melindungi informasi. Keamanan ini disediakan dengan mengenkripsi informasi dengan kunci khusus. Informasi ini sebelum enkripsi disebut plaintext. Setelah dienkripsi dengan kunci yang disebut ciphertext. Sangat penting untuk memastikan keamanan informasi Anda agar tidak disalahgunakan atau jatuh ke tangan yang tidak berhak. Informasi ini dapat berupa kata sandi, nomor kartu kredit, atau informasi pribadi lainnya. Perkembangan teknologi informasi dan komunikasi yang sangat pesat menyebabkan munculnya kemajuan. Teknologi informasi memegang peranan penting dalam berbagai bidang kehidupan, baik secara langsung maupun tidak langsung. Teknologi informasi tidak dapat dipisahkan dari berbagai aspek kehidupan manusia. Memungkinkan komunikasi dan pertukaran informasi atau data. Dengan kemajuan teknologi informasi, sangat diperlukan untuk melindungi data terhadap kerahasiaan informasi yang dipertukarkan. Kriptografi adalah studi tentang cara untuk melindungi informasi. Keamanan ini disediakan dengan mengenkripsi informasi dengan kunci khusus. Informasi ini sebelum enkripsi disebut plaintext. Setelah dienkripsi dengan kunci yang disebut ciphertext. Sangat penting untuk memastikan keamanan informasi Anda agar tidak disalahgunakan atau jatuh ke tangan yang tidak berhak. Informasi ini dapat berupa kata sandi, nomor kartu kredit, atau informasi pribadi lainnya.

Kata Kunci: Kriptografi, AES, Keamanan data, Plainteks, Kunci

Abstract− The very rapid development of information and communication technology led to the emergence of progress. Information technology plays an important role in many areas of life, both directly and indirectly. Information technology is inseparable from many aspects of human life. Enables communication and exchange of information or data. With the advancement of information technology, it is indispensable to protect data against the confidentiality of the information exchanged. Cryptography is he study of ways to protect information. This security is provided by encrypting the information with a special key. This information before encryption is called plaintext. Once encrypted with a key called ciphertext. It is very important to ensure the security of your information so that it is not misused or falls into unauthorized hands. This information can be a password, credit card number, or other personal information. The very rapid development of information and communication technology led to the emergence of progress. Information technology plays an important role in many areas of life, both directly and indirectly. Information technology is inseparable from many aspects of human life. Enables communication and exchange of information or data. With the advancement of information technology, it is indispensable to protect data against the confidentiality of the information exchanged. Cryptography is the study of ways to protect information. This security is provided by encrypting the information with a special key. This information before encryption is called plaintext. Once encrypted with a key called ciphertext. It is very important to ensure the security of your information so that it is not misused or falls into unauthorized hands. This information can be a password, credit card number, or other personal information.

Keywords: Kriptografi, AES, Data security, Plainteks, Key

1. PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi yang sangat pesat menyebabkan munculnya kemajuan teknologi informasi. Teknologi informasi memainkan peran penting dalam banyak bidang kehidupan, baik secara langsung maupun tidak langsung. Teknologi informasi tidak dapat dipisahkan dari banyak aspek kehidupan manusia. Memungkinkan komunikasi dan pertukaran informasi atau data. Dengan kemajuan teknologi informasi, sangat diperlukan untuk melindungi data terhadap kerahasiaan informasi yang dipertukarkan[1].

Kriptografi adalah ilmu yang berhubungan dengan teknik-teknik untuk menjaga keamanan data dan komunikasi. Dalam era digital saat ini, keamanan data menjadi sangat penting mengingat banyaknya serangan terhadap sistem komputer dan jaringan. Salah satu algoritma kriptografi modern yang paling umum digunakan adalah Advanced Encryption Standard (AES). AES adalah algoritma kriptografi simetris yang dikembangkan oleh National Institute of Standards and Technology (NIST) Amerika Serikat. Algoritma ini dirancang untuk mengamankan informasi dengan menggunakan kunci rahasia yang sama untuk enkripsi dan dekripsi[2],[3]. AES telah diadopsi secara luas oleh banyak organisasi dan digunakan dalam berbagai aplikasi, termasuk keamanan jaringan, perlindungan data di perangkat lunak, serta penyimpanan data yang aman[4].

Submitted: **20/04/2023**; Accepted: **10/05/2023**; Published: **01/06/2023**

JURNAL MEDIA INFORMATIKA [JUMIN]
Volume 4, Nomor 2, Juni 2023, Page 97-101
ISSN 2808-005X (media online)
Available Online at http://ejournal.sisfokomtek.org/index.php/jumin

Juga, data berada di jaringan komputer yang terhubung ke jaringan lain. Tidak mengherankan bahwa orang yang tidak berwenang mendapatkan akses ke informasi rahasia dan berharga, yang meningkatkan risiko. Dalam hal ini, pengirim pesan berpotensi dirugikan. Hal sama berlaku untuk organisasi. Informasi yang dikandungnya diubah secara menyesatkan oleh penerima pesan.

Oleh karena itu, untuk menghindari hal tersebut, penulis menggunakan algoritma enkripsi AES untuk proses enkripsi dan deskripsi data. Enkripsi telah menjadi bagian integral dari sistem keamanan jaringan.Salah satu metode enkripsi data adalah Advance Encryption Standard (AES)[5],[3]. Dengan pemikiran tersebut, penulis mencoba melakukan analisis keamanan data menggunakan algoritma enkripsi AES dengan judul Analisis Keamanan Data Menggunakan Advance Encryption Standard AES). Algoritma AES mengoperasikan data dalam blok-blok tetap dengan ukuran 128 bit. Blok data tersebut diubah secara berulang menggunakan serangkaian substitusi dan transposisi bit[6]. AES menggunakan kunci enkripsi dengan panjang 128, 192, atau 256 bit, yang ditentukan oleh versi AES yang digunakan. Semakin panjang kunci yang digunakan, semakin tinggi tingkat keamanan yang dapat dicapai.[7]

2. METODE PENELITIAN

Dalam jurnal ini menggunakan metode penelitian kualitatif ini merupakan metode penelitian yang mempelajari observasi terhadap objek. Metode ini dalam bentuk analisis dan kesimpulan yang bergantung pada analisis penelitian.Teknik pengumpulan data dipadukan dengan menekankan pentingnya simpulan umum dari suatu permasalahan. Internet searching merupakan teknik pengumpulan data melalui bantuan teknologi yang berupa alat atau mesin pencari di internet dimana segala informasi dari berbagai era tersedia di dalamnya. Selain internet searching, pengamatan tentang kriptografi dan penerapannya terhadap keamanan data juga dilakukan dengan metode pendekatan studi pustaka. Studi pustaka yaitu merupakan teknik pengumpulan data dengan mempelajari berbagai buku referensi serta hasil penelitian yang sudah ada sebelumnya yang sejenis, yang berguna untuk mendapatkan landasan teori mengenai masalah masalah yang akan diteliti.[8]

3. HASIL DAN PEMBAHASAN

Pada tahun 1997, US National Institute of Standards and Technology (NIST) menerbitkan Advanced Encryption Standard (AES) untuk menggantikan Data Encryption Standard (DES). AES dikembangkan dengan tujuan memastikan tata kelola di berbagai domain. Algoritma AES dirancang dengan blok cipher minimum blok input 128-bit dan mendukung tiga ukuran kunci (tiga ukuran kunci): 128-bit, 192-bit, dan 256-bit[9],[10].

Kriptografi adalah studi tentang cara untuk melindungi informasi. Keamanan ini disediakan dengan mengenkripsi informasi dengan kunci khusus. Informasi ini sebelum enkripsi disebut plaintext. Setelah dienkripsi dengan kunci yang disebut ciphertext. Sangat penting untuk memastikan keamanan informasi Anda agar tidak disalahgunakan atau jatuh ke tangan yang tidak berwenang. Informasi ini dapat berupa kata sandi, nomor kartu kredit, atau informasi pribadi lainnya.

Upaya menjaga kerahasiaan informasi sudah ada sejak lama. Kaisar Romawi Julius Caesar menggunakan metode enkripsi sederhana untuk menggeser setiap huruf dari pesan dengan nilai tertentu. Metode ini sangat aman pada saat itu, tetapi sangat mudah diselesaikan dengan kekuatan komputasi saat ini sehingga tidak dapat digunakan saat ini. Berbagai algoritma kriptografi telah dibuat oleh kriptografer, dan berbagai upaya telah dilakukan oleh cracker untuk menyelesaikannya dengan sukses. Ini memfasilitasi pembuatan algoritme yang lebih aman secara kriptografis[3].

3.1 Analisis Proses Enkripsi Advanced Encryption Standard(AES)

Proses enkripsi algoritma AES pada ronde 0 dan 1. Misalnya plainteks kunci yang digunakan yaitu contoh kasus seperti berikut yang sudah ada ditambahkan data dammy:

Plainteks : “UNIKOM9807645317”
Kunci : “ADMIN09512345678”

Langkah pertama yang dilakukan adalah mengubah plainteks dan kunci diatas menjadi bentuk hexadecimal dimana proses selanjutnya semua akan menggunakan bentuk hexadecimal. Hasil konversi akan menjadi seperti ini:

Plainteks : “40 45 44 49 20 41 4C 59 41 4E 54 4F 32 30 31 36”
Kunci : “52 49 4A 4E 44 41 45 4A 31 32 33 34 35 36 37 38”

Setelah menkonversi plainteks dan kunci ke dalam hexadecimal, maka kita akan susun plainteks dan kunci ke dalam bentuk matriks 4x4 seperti gambar dibawah:

44	20	41	32
45	41	4E	30
44	4C	54	31

Submitted: **20/04/2023**; Accepted: **10/05/2023**; Published: **01/06/2023**

JURNAL MEDIA INFORMATIKA [JUMIN]
Volume 4, Nomor 2, Juni 2023, Page 97-101
ISSN 2808-005X (media online)
Available Online at http://ejournal.sisfokomtek.org/index.php/jumin

49	59	4F	36
52	44	31	35
49	41	32	36
4A	45	33	37
4E	4C	34	38

Sebelum masuk initial round 0, kita terlebih dahulu mencari round key agar tiap - tiap ronde. Pada ronde 0, subKey-nya sama dengan kunci yang pertama kali diinput. Pada ronde 0 plainteks akan melalui proses AddRounKey dimana tahap ini terjadi perhitungan XOR antara plainteks dengan kunci.

Proses XOR terjadi terhadap masing - masing cell pada matriks diatas, contoh matriksTeks[1,1] XOR matriksKunci[1,1] dan matriksTeks[2,1] XOR matriksKunci[2,1], dan seterusnya. Dibawah ini akan diuji proses XOR antara baris ke-1 kolom ke-1 pada masing - masing matriks.

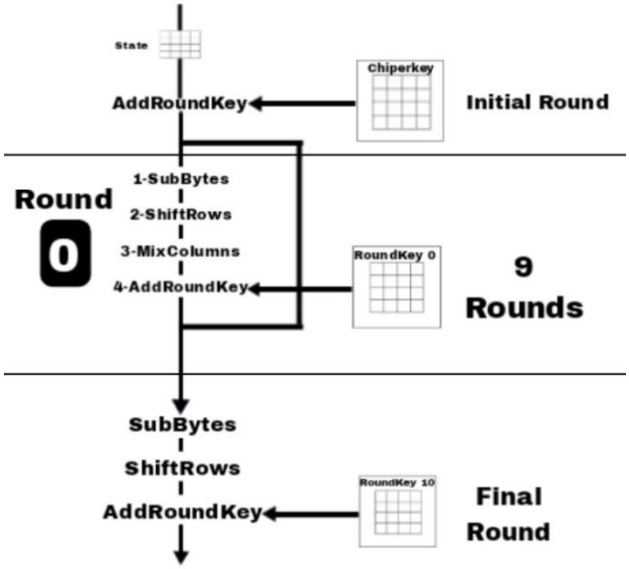
Baris pertama kolom pertama untuk matriks plainteks : 44
Baris ke-1 kolom ke-1 dari matriks kunci : 52

Untuk melakukan XOR langkah awalnya ubah bentuknya dari hexadesimal ke bentuk biner sehingga seperti dibawah ini:

Baris pertama kolom pertama dari matriks plainteks (biner 8 bit) : 01000100
Baris ke-1 kolom ke-1 dari matriks kunci (biner 8 bit) : 01010010

Proses enkripsi algoritma AES terdiri dari 3 langkah, yaitu:

1. Initial round, yaitu proses menyalin input ke dalam state yang akan menghadapi stransformasi AddRoundKey. Transformasi AddRoundKey: melakukan XOR antara state awal (plainteks) dengan cipher key.
2. Proses round function sebanyak Nr − 1 kali. Proses yang dilakukan pada setiap putaran adalah sebagai berikut :
   a) ***SubBytes*** :substitusi byte dengan tabel substitusi (S-box).
   b) ***ShiftRows*** : perpindahan baris-baris array state secara wrapping.
   c) ***MixColumns*** : pengacakan data di masing-masing kolom array state. AddRoundKey: peng-XOR-an antara state sekarang dengan round key.
3. Final round, yaitu proses untuk putaran terakhir. Putaran yang terakhir agak berbeda dengan putaran sebelumnya, yaitu state tidak mengalami transformasi MixColumns.



Gambar 1. Proses enkripsi algoritma AES

Pada umumnya enkripsi dengan algoritma AES sebagai berikut :

1. AddRoundKey : mengerjakan XOR antara state awal (plainteks) dengan cipher key. Tahap ini disebut juga initial round.

Submitted: **20/04/2023**; Accepted: **10/05/2023**; Published: **01/06/2023**

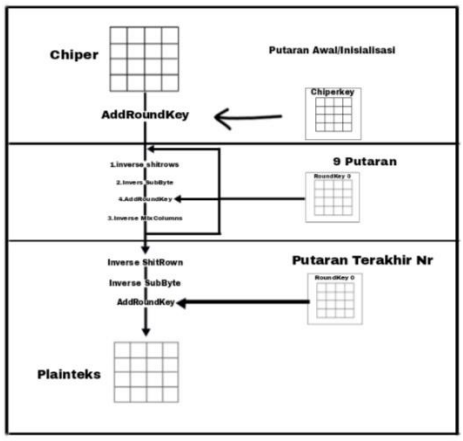
JURNAL MEDIA INFORMATIKA [JUMIN]
Volume 4, Nomor 2, Juni 2023, Page 97-101
ISSN 2808-005X (media online)
Available Online at http://ejournal.sisfokomtek.org/index.php/jumin

2. Round : Putaran sebanyak Nr – 1 kali. Proses yang dikerjakan pada setiap putaran adalah:
   a) SubBytes : substitusi byte dengan menggunakan table substitusi (S- box).
   b) ShiftRows : perputaran baris-baris array state secara wrapping.
   c) MixColumns : mengacak data di masingmasing kolom array state.
   d) AddRoundKey : mengerjakan XOR antara state sekarang round key.
3. Final round: proses untuk putaran terakhir:
   a) SubBytes
   b) ShiftRows
   c) AddRoundKey Diskripsi proses enkripsi sebagai berikut :
4. Add Round Key
   Add Round Key adalah menyatukan chiper teks yang telah ada dengan chiper key yang chiper key dengan ikatantida XOR.
5. Sub Bytes
   Proses SubBytes () memetakan setiap byte dari array State dengan menggunakan table substitusi S-Box. Tidak menyerupai Des S-box yang berbeda pada setiap putaran, AES hanya memiliki satu buah S -Box.

3.2 Proses Dekripsi Algoritme AES

Proses dekripsi diimplementasikan dalam arah yang berlawanan dengan enkripsi untuk menghasilkan inverse cipher. Transformasi byte yang digunakan pada invers cipher adalah Inverse ShiftRows, Inverse SubBytes, Inverse MixColumns, dan AddRoundKey. Urutan proses dekripsi AES tidak merupakan kebalikan dari enkripsi, namun urutannya yang ditukarkan, walaupun penggunaan kuncinya sama.

Proses dekripsi algoritme AES terdiri dari 3 langkah seperti pada proses enkripsi seperti ditampilkan pada gambar



Gamabar 2. Proses dekripsi algoritme AES

4. KESIMPULAN

Berdasarkan hasil analisis,maka dapat disimpulkan :
Sistem dapat dimanfaatkan untuk proses enkripsi dan dekripsi file dengan berbagai ukuran dan jenis file, menggunakan algoritma AES. Proses yang dikerjakan pada setiap putaran adalah: SubBytes : substitusi byte dengan menggunakan table substitusi (S- box). ShiftRows : perputaran baris-baris array state secara wrapping. MixColumns : mengacak data di masingmasing kolom array state. AddRoundKey : mengerjakan XOR antara state sekarang *round key*. Final round: proses untuk putaran terakhir: SubBytes, ShiftRows, AddRoundKey Diskripsi proses enkripsi sebagai berikut : Add Round Key menyatukan chiper teks yang telah ada dengan chiper key yang chiper key dengan ikatantida XOR. Sub Bytes Proses SubBytes () memetakan setiap byte dari array State dengan menggunakan table substitusi S-Box. Tidak menyerupai Des S-box yang berbeda pada setiap putaran, AES hanya memiliki satu buah S -Box.

DAFTAR PUSTAKA

[1] Y. U. Alsabri, A. Zakir, and D. Irwan, “Penerapan Customer Relationship Management Pada Sistem Informasi Klinik Kecantikan Berbasis Website (Studi Kasus: Ms Glow Aesthetic Clinic),” vol. 4, 2022.

Submitted: **20/04/2023**; Accepted: **10/05/2023**; Published: **01/06/2023**

JURNAL MEDIA INFORMATIKA [JUMIN]
Volume 4, Nomor 2, Juni 2023, Page 97-101
ISSN 2808-005X (media online)
Available Online at http://ejournal.sisfokomtek.org/index.php/jumin

[2] F. A. Sianturi, "Perancangan aplikasi pengamanan data dengan kriptografi Advanced Encryption Standard (AES)," *J. Pelita Inform. Budi Darma*, vol. 4, no. 1, pp. 42–46, 2013.
[3] S. P. Lestari, H. N. Fadlan, R. Angelia Purba, and I. Gunawan, "REALISASI KRIPTOGRAFI PADA FITUR ENKRIPSI END-TO-END PESAN WHATSAPP," *J. Media Inform.*, vol. 4, no. 1, pp. 1–8, Nov. 2022, doi: 10.55338/jumin.v4i1.423.
[4] A. R. Faqih and A. A. Widya, "Implementasi Aplikasi E-Ticket pada Bumdes Desa Sumbermulyo Kec. Jogoroto Kab. Jombang sebagai Solusi Digitalisasi Pengelolaan Tiket.," vol. 2, 2023.
[5] F. A. Sianturi, "PERANCANGAN APLIKASI PENGAMANAN DATA DENGAN KRIPTOGRAFI ADVANCED ENCRYPTION STANDARD (AES)," 2013.
[6] A. N. Safitri and F. A. Sianturi, "Analisa Metode Trend Moment Untuk Peramalan Penjualan Stok Barang Pada Toko Sun Oleh-Oleh," *J. Ilmu Komput. Dan Sist. Inf. JIKOMSI*, vol. 3, no. 1.1, pp. 91–102, 2020.
[7] A. Afrisawati and S. Sahren, "ANALISIS PERBANDINGAN MENGGUNAKAN METODE MOORA DAN WASPAS PEMILIHAN BIBIT SAPI POTONG TERBAIK," *JURTEKSI J. Teknol. Dan Sist. Inf.*, vol. 6, no. 3, pp. 269–276, Aug. 2020, doi: 10.33330/jurteksi.v6i3.827.
[8] Y. Aziz, H. Hasdiana, and N. Nurjamiyah, "ANALISIS ASOSIASI RULE MINING DALAM REKOMENDASI SPAREPART PADA BENGKEL SERVICE 227 MENGGUNAKAN ALGORTIMA CT-PRO," *J. Media Inform.*, vol. 4, no. 1, pp. 31–39, Nov. 2022, doi: 10.55338/jumin.v4i1.403.
[9] E. Manalu, F. A. Sianturi, and M. R. Manalu, "Penerapan Algoritma Naive Bayes Untuk Memprediksi Jumlah Produksi Barang Berdasarkan Data Persediaan Dan Jumlah Pemesanan Pada Cv. Papadan Mama Pastries," *J. Mantik Penusa*, vol. 1, no. 2, 2017.
[10] F. A. Sianturi, "ANALISA PENGARUH LOG TRANSAKSI PADA SISTEM KOMPUTER MENGGUNAKAN ALGORITMA RECOVERY BERBASIS LOG: ANALISA PENGARUH LOG TRANSAKSI PADA SISTEM KOMPUTER MENGGUNAKAN ALGORITMA RECOVERY BERBASIS LOG," *J. Comput. Netw. Archit. High Perform. Comput.*, vol. 1, no. 1, pp. 6–9, Dec. 2018, doi: 10.47709/cnapc.v1i1.2.
[11] Agustan Latif, (2015), "IMPLEMENTASI KRIPTOGRAFI MENGGUNAKAN METODE ADVANCED ENCRYPTION STANDAR (AES) UNTUK PENGAMANAN DATA TEKS"
[12] Ratno Prasetyo , Asep Suryana, (2016), "APLIKASI PENGAMANAN DATA DENGAN TEKNIK ALGORITMA KRIPTOGRAFI AES DAN FUNGSI HASH SHA-1 BERBASIS DESKTOP"

Submitted: **20/04/2023**; Accepted: **10/05/2023**; Published: **01/06/2023**