Kriptografi *Advanced Encryption Standard* (AES)

Nasa Ngainur Rohmah
Program Studi D3 Teknik Informatika, FMIPA, Universitas Sebelas Maret,

Abstrak. Advanced Encryption Standard (AES) adalah algoritma kriptografi yang menjadi algoritma standar enkripsi kunci simetris saat ini. AES-128 menggunakan kunci yang berukuran 128 bit untuk mengenkripsi dan mendekripsi blok pesan yang memiliki ukuran 128 bit. Proses enkripsi melibatkan 10 ronde enkripsi pada matriks heksadesimal 4x4, yang setiap ronde melibatkan 4 transformasi dasar, yaitu subbytes, shiftrows, mixcolumns, dan addroundkey. Selain itu, proses dekripsi melibatkan inversi semua transformasi dasar pada algoritma AES kecuali addroundkey, dengan urutan transformasi invshiftrows, invsubbytes, addroundkey, dan invmixcolumns. AES-128 sangat aman dan sulit ditebak oleh serangan brute force, yang berarti membuat kunci yang sangat besar dan sulit ditebak oleh serangan yang mencoba mengakses informasi terkait dengan kunci. AES-128 secara luas digunakan untuk mengenkripsi data pribadi pada komputer, perangkat penyimpanan eksternal, dan penyimpanan cloud.

Abstract. Advanced Encryption Standard (AES) is a cryptographic algorithm that is the current standard symmetric key encryption algorithm. AES-128 uses a key of 128 bits to encrypt and decrypt message blocks of 128 bits. The encryption process involves 10 rounds of encryption on a 4x4 hexadecimal matrix, each round involving 4 basic transformations, namely subbytes, shiftrows, mixcolumns, and addroundkey. In addition, the decryption process involves inverting all the basic transformations in the AES algorithm except addroundkey, with the transformation sequence in shiftrows, invsubbytes, addroundkey, and invmixcolumns. AES-128 is highly secure and difficult to guess by brute force attacks, which means it creates keys that are very large and difficult to guess by attacks trying to access information associated with the key. AES-128 is widely used to encrypt personal data on computers, external storage devices, and cloud storage.

1. Pendahuluan

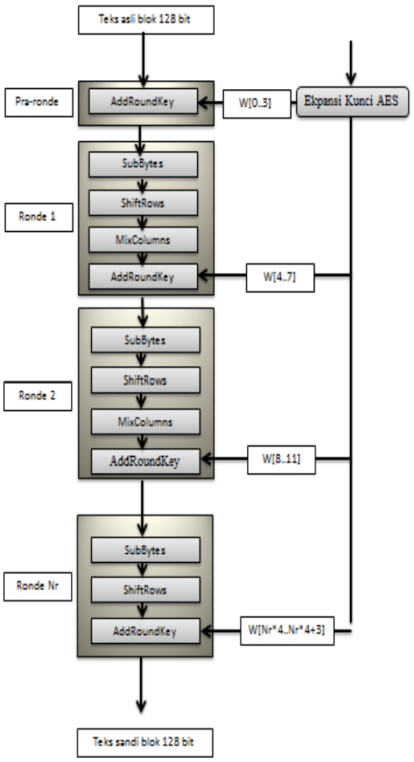
Perkembangan teknologi informasi dan komunikasi saat ini telah memungkinkan manusia untuk berkomunikasi dan saling bertukar data dan informasi tanpa dihalangi oleh jarak dan waktu. Tuntutan akan keamanan untuk kerahasiaan informasi yang saling dipertukarkan semakin meningkatkan, yang mengarah pada peningkatan keamanan data yang lebih baik untuk melindungi data yang ditransmisikan atau dikirimkan melalui suatu jaringan komunikasi. Kriptografi adalah ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan data dan informasi seperti keabsahan data, integritas data, dan autentifikasi data.

Sistem kriptografi adalah suatu fasilitas untuk mengkonversikan pesan jelas (plainteks) ke pesan yang telah disandikan (cipherteks). Proses konversi ini disebut enkripsi (encryption). Sebaliknya, menerjemahkan cipherteks menjadi plainteks disebut dengan dekripsi (decryption). Proses enkripsi dan dekripsi menggunakan satu atau beberapa kunci kriptografi. Pada tahun 2000, National Institute of Standards and Technology (NIST) sebagai agensi departemen perdagangan AS menetapkan sebuah standard kriptografi yang baru yaitu Algoritma Rijndael dan ditetapkan sebagai Advanced Encryption Standard (AES) (Munir, 2006).

Advanced Encryption Standard (AES) secara garis besar beroperasi pada blok 128-bit atau 16 karakter, yang berarti dapat digunakan untuk enkripsi teks. File dokumen terdiri dari barisan teks yang tentu saja berukuran lebih dari 16 karakter, akan tetapi AES dapat digunakan untuk penyandian yaitu dengan melakukan enkripsi per blok (128 bit) secara paralel untuk memudahkan proses enkripsi maupun dekripsi digunakan software aplikasi MATLAB.

2. Landasan Teori

Algoritma Advanced Encryption Standard (AES) merupakan sistem penyandian blok yang bersifat non-Feistel karena menggunakan komponen yang selalu memiliki invers dengan panjang blok 128 bit. Proses enkripsi AES melibatkan transformasi terhadap state secara berulang dalam beberapa ronde, di mana state yang dihasilkan dari ronde sebelumnya menjadi masukan untuk ronde berikutnya. Proses enkripsi melibatkan 4 jenis transformasi, yaitu SubBytes, ShiftRows, MixColumns, dan AddRoundKey. Pada ronde terakhir, transformasi MixColumns tidak dilakukan. Algoritma dekripsi AES merupakan kebalikan dari algoritma enkripsi dan melibatkan transformasi invers dari transformasi dasar yang digunakan pada algoritma enkripsi AES, yaitu InvSubBytes, InvShiftRows, dan InvMixColumns. AddRoundKey merupakan transformasi yang bersifat self-invers dengan syarat menggunakan kunci yang sama.



proses enkripsi dan deskripsi AES

3. Hasil Penelitian dan Pembahasan

AES menggunakan beberapa tahap dalam proses enkripsi dan dekripsi. Tahap-tahap tersebut adalah:

1. Generation of round keys: Kunci ronde dihasilkan dari kunci utama menggunakan proses yang disebut key expansion. Proses ini menghasilkan kunci ronde yang digunakan pada setiap tahap ronde dalam enkripsi dan dekripsi.

2. Substitution of the bytes: Pada tahap ini, setiap byte pada state diubah menjadi byte lain menggunakan tabel substitusi yang disebut S-box. Setiap byte diubah menjadi byte lain yang berbeda, sehingga menghasilkan state yang berbeda.
3. Shifting the Rows: Pada tahap ini, setiap baris pada state digeser ke kiri sebanyak beberapa langkah. Baris pertama tidak digeser, baris kedua digeser satu langkah ke kiri, baris ketiga digeser dua langkah ke kiri, dan baris keempat digeser tiga langkah ke kiri.
4. Mix Column: Pada tahap ini, setiap kolom pada state diubah menggunakan operasi matematika tertentu. Setiap kolom diubah menjadi kolom lain yang berbeda, sehingga menghasilkan state yang berbeda.
5. Repeat Step 1 to 4: Tahap-tahap 1 hingga 4 diulang sebanyak 10 atau 14 kali tergantung pada panjang kunci yang digunakan. Setelah tahap terakhir, tahap Mixcolumn tidak dilakukan pada proses enkripsi, dan tahap ini dihilangkan pada proses dekripsi.

4. Kesimpulan

AES merupakan algoritma kriptografi yang menjadi standar algoritma enkripsi kunci simetris saat ini. Algoritma ini menggunakan kunci yang berukuran 128 bit untuk mengenkripsi dan mendekripsi blok pesan yang memiliki ukuran 128 bit. AES terbukti kebal menghadapi serangan konvensional (linear dan diferensial attack) yang menggunakan statistik untuk memecahkan sandi. Kesederhanaan AES memberikan keuntungan berupa kepercayaan bahwa AES tidak ditanami trapdoor. Namun, kesederhanaan struktur AES juga membuka kesempatan untuk mendapatkan persamaan aljabar AES yang selanjutnya akan diteliti apakah persamaan tersebut dapat dipecahkan.

5. Saran

AES merupakan algoritma kriptografi yang aman dan sulit ditebak oleh serangan brute force, yang berarti membuat kunci yang sangat besar dan sulit ditebak oleh serangan yang mencoba mengakses informasi yang terkait dengan kunci. Oleh karena itu, berbagai sistem pengamanan data dan informasi, seperti komputer, perangkat penyimpanan eksternal, dan penyimpanan cloud, menggunakan AES untuk mengenkripsi data pribadi mereka.

6. Referensi

[1] https://fmipa.unmul.ac.id/files/docs/20-31%20Jurnal%20Fresly.pdf

[2] https://www.section.io/engineering-education/aes-rsa-encryption/

[3] https://media.neliti.com/media/publications/65826-ID-enkripsi-dan-dekripsi-dengan-algoritma-a.pdf