Algoritma AES-128

Pada algoritma AES-128 (Advanced Encryption Standard 128-bit), operasi enkripsi dilakukan dengan menggunakan blok data berukuran 128 bit (16 byte) yang diproses dalam bentuk matriks 4x4 (disebut "state"). Algoritma AES-128 bekerja dengan 10 putaran (rounds) enkripsi untuk menghasilkan teks terenkripsi. Berikut adalah langkah-langkah dasar dalam proses enkripsi AES-128 dengan fokus pada operasi matriks yang terlibat.

1. State Matrix

Data input dalam AES-128 dibagi menjadi blok 128-bit (16 byte), yang kemudian diorganisasi menjadi matriks 4x4, di mana setiap elemen adalah satu byte (8 bit). Matriks ini disebut state matrix dan diatur secara kolom.

Setiap elemen adalah satu byte dari blok data yang akan dienkripsi.

2. Langkah-langkah Enkripsi AES-128

AES-128 terdiri dari 10 putaran, dan setiap putaran melibatkan beberapa operasi pada state matrix. Berikut adalah langkah-langkahnya:

1. AddRoundKey (Key Expansion)

- Pada awalnya (sebelum ronde pertama), blok data (state matrix) akan dipadukan dengan **kunci** melalui operasi XOR.
- Setelah itu, kunci akan diperluas untuk menghasilkan kunci yang digunakan di setiap putaran enkripsi.

2. SubBytes

- Setiap byte dalam state matrix digantikan dengan byte yang sesuai dari **S-box**, yang merupakan tabel substitusi. Operasi ini mengganti nilai byte sesuai dengan fungsi non-linier.

3. ShiftRows

- Operasi ini berfungsi untuk menggeser baris-baris dalam matriks state:
    - Baris pertama (S1) tidak digeser.
    - Baris kedua digeser 1 posisi ke kiri.
    - Baris ketiga digeser 2 posisi ke kiri.
    - Baris keempat digeser 3 posisi ke kiri.
    -

4. MixColumns

- Operasi ini mengubah kolom-kolom dalam state matrix. Setiap kolom dianggap sebagai polinomial derajat 3 dan dikalikan dengan matriks tetap tertentu. Tujuan dari langkah ini adalah untuk mendistribusikan bit-bit dalam blok dan meningkatkan kekuatan enkripsi.

Rumus untuk MixColumns dalam AES adalah:

Matriks tetap yang digunakan untuk MixColumns adalah:

2	3	1	1
1	2	3	1
1	1	2	3
3	1	1	2

5. AddRoundKey (Final Round)

- Pada ronde terakhir, proses ini dilakukan sekali lagi dengan menambahkan (XOR) **key** ke state matrix, namun tanpa melakukan langkah MixColumns.

Struktur dan Proses Matriks

Berikut gambaran visual langkah-langkah yang terlibat dalam satu putaran enkripsi AES-128:

1. **Input**: Blok data 128 bit (state matrix)
2. **Proses Putaran**:
    - **AddRoundKey**: XOR blok data dengan kunci (state = state $\oplus$ key).
    - **SubBytes**: Substitusi dengan S-box.
    - **ShiftRows**: Geser baris-baris.
    - **MixColumns**: Kombinasi kolom-kolom (kecuali di putaran terakhir).
3. **Putaran Akhir**: Hanya AddRoundKey, SubBytes, dan ShiftRows tanpa MixColumns.
4. **Output**: Blok data terenkripsi.