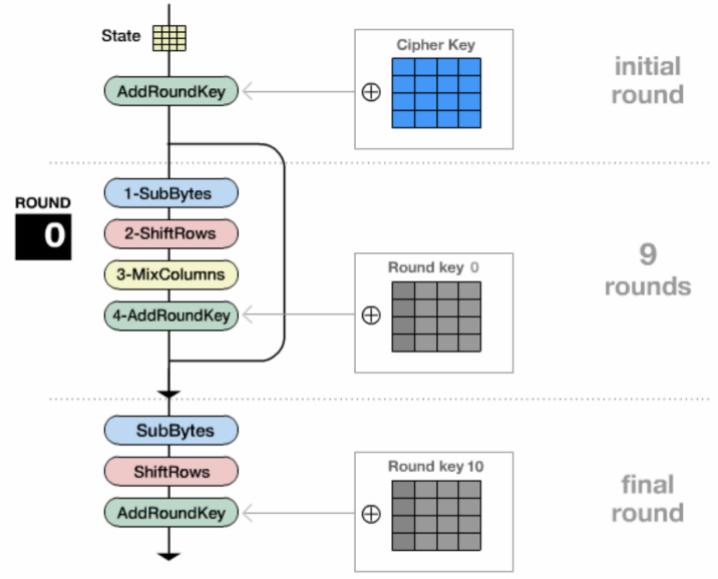
Project Tengah Semester
ET234501 Kriptografi
Tahun Ajaran 2024/2025 Genap

Mini-AES



Gambar 13.1 Diagram proses enkripsi

Sifat: Kelompok (4-5 orang) Link

AES (Advanced Encryption Standard) adalah algoritma kriptografi blok yang kuat namun kompleks. Untuk keperluan pembelajaran, Mini-AES dirancang sebagai versi ringkas yang tetap mempertahankan struktur inti AES seperti *SubBytes*, *ShiftRows*, *MixColumns*, dan *AddRoundKey*, namun dengan ukuran blok dan kunci yang lebih kecil. Project ini bertujuan untuk memberikan pemahaman praktis tentang bagaimana cipher modern bekerja dalam bentuk yang sederhana.

A. Spesifikasi Dasar (Total 100 poin)

1. Implementasi Mini-AES 16-bit **(35 poin)**
   - Representasi plaintext dan key: 16-bit (4 nibble) **(2,5)**
   - Operasi meliputi:
     - SubNibbles (menggunakan S-Box 4-bit) **(8)**
     - ShiftRows **(5)**
     - MixColumns (dengan matriks sederhana pada $GF(2^4)$) **(10)**
     - AddRoundKey **(7)**
   - Jumlah round: 3 **(2,5)**
   - Bahasa pemrograman bebas (Python direkomendasikan)

2. Key Expansion (Round Key Generator) **(20 poin)**
    - Key awal: 16-bit **(10)**
    - Algoritma key expansion sederhana untuk menghasilkan round keys **(10)**

3. Program **(30 poin)**
    - Menerima Input: Plaintext (16-bit) dan key (16-bit) **(5)**
    - Mengeluarkan Output: Ciphertext (16-bit) **(5)**
    - Minimal 3 test case dengan expected output benar **(10)**
    - Tampilkan *output* proses tiap round **(5)**
    - Memiliki GUI, menggunakan Tkinter, Streamlit (web-based), dsb **(5)**

4. Dokumentasi **(15 poin)** – Github
    - Spesifikasi algoritma Mini-AES **(5)**
    - Flowchart Mini-AES dan Key Expansion **(5)**
    - Implementasi program
    - Penjelasan TestCase
    - Analisis: kelebihan dan keterbatasan Mini-AES **(5)**

B. Spesifikasi Tambahan (Max. 20 poin)

1. Implementasi Dekripsi Mini-AES **(7 poin)**
    - Tambahkan fungsi dekripsi
    - Implementasi inverse operations:
        - Inverse S-Box
        - Inverse MixColumns
        - Inverse ShiftRows
    - Output dekripsi harus menghasilkan kembali plaintext awal

2. Analisis Keamanan dan Avalanche Effect **(5 poin)**
    - Uji sensitivitas terhadap perubahan 1-bit di plaintext atau key
    - Jelaskan efek avalanche (bit perubahan pada ciphertext)

3. Mode Operasi Blok (ECB/CBC) **(6 poin)**
    - Tambahkan implementasi mode operasi blok:
        - ECB (Electronic Codebook)
        - CBC (Cipher Block Chaining) lengkap dengan simulasi IV (Initialization Vector).
    - Mendukung input teks lebih panjang dari 16-bit (contoh: 64-bit diproses sebagai 4 blok).
    - Proses enkripsi/dekripsi harus mempertahankan mode terpilih.

4. Export dan Import File **(2 poin)**
    - Simpan **input/output dan log proses** ke file TXT/CSV
    - Load file untuk proses enkripsi/dekripsi

Submission:

1. Buatlah Repository Github untuk Kriptografi
2. Tuliskan dokumentasi menggunakan Github Markdown
3. Push program yang telah dibuat ke Github
4. Kumpulkan Link Github di MyITS Classroom sesuai dengan deadlinenya

Selamat mengerjakan! ☺