**IMPLEMENTASI KOMBINASI CHACHA20 DAN MODIFIKASI AES MELALUI *ADDROUNDKEY* PADA**

**STUDI KASUS KEAMANAN *FILE***

**Proposal Tugas Akhir Mata Kuliah Penulisan Proposal**

## (CAK4EAB2)

Disusun oleh:

## EMILIA RAMONA 1203210017

****

**PROGRAM STUDI SARJANA INFORMATIKA DIREKTORAT KAMPUS SURABAYA**

**UNIVERSITAS TELKOM SURABAYA TAHUN 2025**

# 

# KATA PENGANTAR

Assalamu’alaikum Warrahmatullahi Wabarakatuh, puja puji syukur ke hadirat Allah SWT yang telah memberikan nikmat dan karunia-Nya yang sangat luar biasa kepada hamba – hambanya. Tidak lupa shalawat serta salam kita curahkan atas bimbingan nabi kita nabi Muhammad SAW yang telah membawa cahaya islam ke dalam dunia ini dan menjadi panutan bagi setiap umatnya hingga akhir zaman.

Setelah melalui berbagai proses kerja keras, penyusunan skripsi yang berjudul “Implementasi Kombinasi ChaCha20 dan Modifikasi AES melalui *AddRoundkey* Pada Studi Kasus Keamanan *File*” akhirnya dapat terselesaikan. Selain sebagai salah satu syarat memperoleh gelar S-Kom, penulis berharap juga skripsi ini dapat bermanfaat bagi semua pihak yang berkepentingan. Oleh karena itu, penulis ingin mengungkapkan rasa terima kasih kepada pihak-pihak yang telah memberikan dukungan dan doa sehingga penulis dapat menyelesaikan skripsi ini tepat pada waktunya. Beberapa pihak tersebut antara lain:

1. **Kepada Mama** yang sangat penulis cintai yang tidak pernah lupa selalu memberikan dukungannya dan doa agar diberikan kemudahan dan kelancaran dalam penyusunan skripsi ini sehingga penulis dapat menyelesaikan studi Informatika di Universitas IT Telkom Surabaya.
2. **Kepada Alm.Ibu Suhartatik**, yang penulis cintai dan sayangi, yang telah memberikan motivasi untuk saya.
3. **Kepada Saudara Kembar**, yang selalu mendukung, terima kasih atas bantuan dan waktunya dalam memberikan masukan terkait susunan skripsi ini.
4. **Keluarga Besar penulis** yang telah memberikan motivasi dan kepercayaan besar sehingga penulis bisa mewujudkan impian untuk meraih gelar S-Kom.
5. **Dosen Pembimbing**, Pak Rizky Fenaldo Maulana, S.Kom., M.Kom. dan Tanzila Mustaqim, S.Kom., M.Kom. Yang telah memberikan solusi, waktu, dan bimbingan penuh kesabaran selama proses penyusunan skripsi ini.
6. **Teman-teman dekat**, termasuk Jus’an, Erica Dyah, Qori Emalia, Ardina Firdatana, dan Elma Saskia yang selalu memberikan semangat, mendengarkan keluh kesah, serta menemani dalam berbagai kondisi selama penulisan skripsi.
7. **Semua pihak lainnya**, yang tidak dapat disebutkan satu per satu, atas bantuan dan dukungannya selama proses ini.
8. **Diri penulis sendiri**, atas perjuangan dan kerja keras hingga akhirnya skripsi ini selesai tepat waktu.

Penulis menyadari bahwa skripsi ini masih jauh dari kesempurnaan. Oleh karena itu, saran dan kritik yang membangun sangat diharapkan untuk memperbaiki skripsi ini ke depannya.

Terima kasih.

### Wassalamu’alaikum Warrahmatullahi Wabarakatuh.

Surabaya, 24 Desember 2024 Penulis

Emilia Ramona

# DAFTAR ISI

Pada [Tabel II.4 Transformasi ShiftRows](#_bookmark29) merupakan hasil dari pergeseran pada tabel 1 baris ke 2 pergeseran 1 kali, baris ke 3 pergeseran 2, dan beris ke 4 pergeseran 3 kali.

* + - * 1. *MixColumns*

*MixColumns* adalah proses transformasi di mana setiap elemen dalam blok *cipher* dikalikan dengan matriks . Transformasi ini bertujuan untuk mencampur elemen- elemen dalam setiap kolom *state* berguna meningkatkan difusi data dan memperkuat keamanan enkripsi . Transformasi ini bekerja dengan membagi matriks atau *state* menjadi empat bagian, untuk setiap kolomnya (Widyawan & Imelda, 2021). Setiap kolom dalam matriks *state* diperlakukan sebagai *polinomial* dengan empat bagian

00000001 ( 1 diposisi ke 1 dari kanan), dimana elemen 1 ini menyatakan bahwa *polinomial* ini memiliki koefisien konstan.

Proses *MixColumns* juga dapat direpresentasikan sebagai operasi perkalian matriks, di mana setiap kolom matriks dikalikan dengan matriks tertentu dalam *Galois Field* (Cristy & Riandari, 2021).

* + - 1. **Proses *dekripsi* AES :**

Proses *dekripsi* merupakan kebalikan dari proses enkripsi. *Transformasi bytes* yang digunakan dalam *dekripsi* mencakup *AddRoundKey*, *InvShiftRows*, *InvSubBytes,* dan *InvMixColumns*. Pada iterasi pertama *dekripsi*, dilakukan *transformasi AddRoundKey, Inverse ShiftRows, dan Inverse SubBytes. Ciphertex*t kemudian akan mengalami transformasi *AddRoundKey* .

* + - * 1. *InvShiftRows*

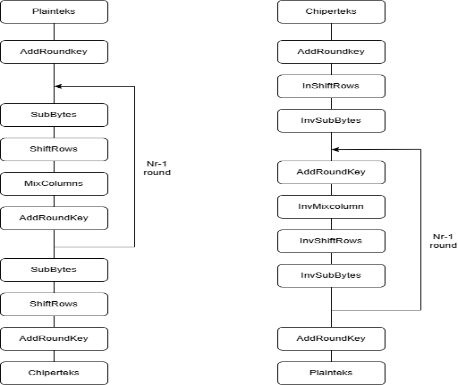
Transformasi *byte* yang merupakan kebalikan dari proses *ShiftRows*. Dalam transformasi ini, bit-bit pada *state* digeser ke arah kanan, berbeda dengan *ShiftRows* yang melakukan pergeseran bit ke arah kiri.

* + - * 1. *InvSubBytes*

Transformasi *byte* yang menjadi kebalikan dari *SubBytes*. Dalam proses ini, setiap elemen pada *state* dipetakan menggunakan tabel substitusi *Inverse* S-Box.

* + - * 1. *InvMixColumns*

Setiap kolom dalam *state* dikalikan dengan matriks khusus yang digunakan dalam proses perkalian pada algoritma AES (Syahputra Sianipar et al., 2024)



*Gambar II.4 Proses AES*

Pada [Gambar II.4 Proses AES](#_bookmark31) sebelah kiri menunjukkan tahapan proses enkripsi pada algoritma AES Modifikasi. Proses dimulai dengan memasukkan plainteks, kemudian melalui serangkaian langkah seperti *AddRoundkey*, SubBytes, ShiftRows, MixColumns, dan diakhiri dengan *AddRoundkey* tambahan. Langkah ini diulang sebanyak Nr−1 ronde untuk meningkatkan keamanan data, menghasilkan cipherteks di akhir proses. Flowchart sebelah kanan menjelaskan tahapan proses *dekripsi*, yang merupakan kebalikan dari proses enkripsi. Proses dimulai dengan memasukkan cipherteks, kemudian melalui langkah-langkah seperti *AddRoundkey*, Inverse ShiftRows, Inverse SubBytes, dan Inverse MixColumns. Setelah semua ronde selesai, data dikembalikan ke bentuk plainteks asli.

### Chacha20

Algoritma ChaCha20 adalah salah satu jenis *stream cipher* yang dikembangkan sebagai varian dari algoritma Salsa20. Algoritma ini berbasis desain yang serupa dengan Salsa20, namun ChaCha20 meningkatkan tingkat *diffusion* pada setiap ronde untuk memperkuat keamanan proses enkripsi (Anindita & 18219086, 2023). Chacha20 beroperasi pada unit data 32-bit menggunakan kunci 256-bit. Algoritma ini menghasilkan *output* berupa *stream* kunci sepanjang 512-bit, yang kemudian akan di XOR kan dengan *plainteks* untuk menghasilkan *chiperteks*(Alyas & Abdullah, 2021b). ChaCha20 dimulai dengan membuat *state* 512-bit, yang berupa *array* yang berukuran 16x32-bit. State ini disusun dari empat konstanta 32 bit, kunci rahasia sepanjang 256-bit, penghitung blok 32-bit, serta nonce sepanjang 96-bit (Kim & Wong, 2023).

matriks 4x4 dengan 16 elemen 32-bit. Matriks ini diinisialisasi dengan empat konstanta 32-bit, kunci 256-bit yang dibagi menjadi 8 bagian, penghitung 32 blok 32-bit, dan Nonce 96-bit. Elemen-elemen ini digunakan untuk menghasilkan *keystream* yang kemudian di XOR kan dengan *plainteks* untuk menghasilkan *chiperteks*. Di mana *const* (konstanta) ini berisi empat nilai tetap 32-bit, *key* (kunci) yang terbagi 8 bagian 32-bit dari kunci rahasia 256-bit, *counter* (penghitung), dan Nonce (nilai acak) yang berukuran 96-bit.

Langkah – Langkah Algoritma ChaCha20 :

* + - 1. *Inisialisasi* State

Algoritma ChaCha20 dimulai dengan membangun sebuah state internal berbentuk matriks 4x4 (32-bit) (Barbero et al., 2022) . Matriks ini terdiri dari:

* + - * 1. Baris pertama: Berisi 4 konstanta tetap (128-bit), yang digunakan untuk mengenali algoritma.
        2. Baris kedua dan ketiga: Berisi kunci rahasia 256-bit (8 elemen 32-bit), yang digunakan untuk proses enkripsi.
        3. Baris keempat: Berisi kombinasi 64-bit counter dan 64-bit nonce (masing-masing terdiri dari 2 elemen 32-bit).
      1. *Quarter Round*

Operasi ini memodifikasi 4 elemen dari matriks ( a, b, c, d ) (Almukhlifi & Vora, 2020)

𝑎 += 𝑏; 𝑑 ^ = 𝑎; 𝑑 <<<= 16;

𝑐 += 𝑑; 𝑏 ^ = 𝑐; 𝑏 <<<= 12;

𝑎 += 𝑏; 𝑏 ^ = 𝑎; 𝑑 <<<= 8;

𝑐 += 𝑑; 𝑏 ^ = 𝑐; 𝑏 <<<= 7;

* + - 1. *Double Round*

*Double Round* adalah kombinasi dari dua *Quarter Round* yang dijalankan secara berurutan. Setiap iterasi *Double Round* mencakup:

* + - * 1. Operasi pada kolom matriks *(Column Round):*

melakukan operasi Quarter Round pada setiap kolom matriks 4x4. Tujuannya adalah untuk mencampur data antar elemen dalam kolom, sehingga meningkatkan difusi data secara vertikal.

* + - * 1. Operasi pada diagonal matriks (Diagonal Round):

Setelah operasi pada kolom selesai, langkah berikutnya adalah menerapkan Quarter Round pada elemen-elemen diagonal dalam matriks.

Proses Double Round dilakukan sebanyak 10 iterasi, menghasilkan total 20 ronde Quarter Round untuk setiap blok data yang diproses.

* + - 1. Finalisasi State
      2. *Keystream Generation*

Setelah 20 ronde selesai*, state* akhir ditambahkan kembali ke

*state* awal menggunakan penjumlahan modul0 232 :

# BAB III METODOLOGI PENELITIAN

### Sistematika Penyelesaian Masalah

Penelitian ini bersifat kuantitatif dengan tujuan mengevaluasi performa algoritma AES modifikasi dan kombinasi ChaCha20 dan AES modifikasi. Penilaian performa ini dilakukan berdasarkan waktu enkripsi, waktu *dekripsi*, kecepatan enkripsi, dan kecepatan *dekripsi*, yang akan dianalisis menggunakan data hasil pengujian pada berbagai jenis *file* dengan format PDF, Word dan TXT, yang hasilnya berbentuk tabel untuk mempermudah analisis perbandingan.

### Alat dan Bahan

### Alat

1. Perangkat Keras (Hardware) Laptop dengan spesifikasi :
   1. Prosesor : Intel *Core* I5
   2. RAM : 8 GB
   3. Penyimpanan : 256 GB SSD atau lebih
2. Perangkat Lunak (*Software*)
   1. *Python* :

Menggunakan *library cryptography, pycryptodome*, dan *library* lain yang mendukung algoritma AES dan ChaCha20. Berikut beberapa pustaka yang digunakan :

* + - PyCryptodome : Digunakan Iplementasi algoritma AES dan ChaCha20
    - Cryptography : Implementasi kemanan tambahan (jika nanti dibutuhkan )
    - Numpy : Digunakan untuk analisis data (perhitungan entropi)
    - Time : Mencatat waktu eksekusi algoritma, baik untuk enkripsi maupun dekripsi.
  1. *Text* Editor :

Visual Studio Code dan *Jupyter Notebook*

* 1. Sistem Operasi : Windows

### Bahan

1. Data set *file* :
   1. *File* PDF : Ukuran *file* 100 KB – 100 MB
   2. *File* Word : Ukuran *file* 100 KB – 100 MB
   3. *File* TXT : Ukuran *file* maksimal 300 *byte*
2. Literatur :

Jurnal atau artikel ilmiah tentang AES, ChaCha20 dan *Double Encrypt* (tahun 2020-2024)

1. *Spreadsheet* Analisis Data :

Format CSV (Comma Separated Values)