KERANGKA ACUAN KERJA (KAK)

TUGAS INDIVIDU: PENGEMBANGAN APLIKASI KRIPTOGRAFI SEDERHANA

Mata Kuliah : Keamanan Data

Program Studi : Sarjana Data Science

Fakultas : Informatika, Universitas Telkom Bandung

Dosen Pengampu : Sidik Prabowo (SPO)

1. Latar Belakang

Dalam mata kuliah Keamanan Data, pemahaman tentang kriptografi menjadi fondasi utama untuk melindungi data sensitif di era digital. Tugas individu ini dirancang untuk menerapkan konsep kriptografi secara praktis melalui pengembangan aplikasi sederhana. Mahasiswa diharapkan memilih satu algoritma kriptografi simetris atau asimetris dari opsi yang disediakan, menjelaskan mekanismenya, dan mengimplementasikannya dalam bentuk program Python yang dapat dijalankan. Penggunaan alat bantu AI/LLM (seperti Grok atau ChatGPT) diperbolehkan untuk asistensi dalam penulisan kode, debugging, atau klarifikasi konsep, selama mahasiswa mencantumkan sumber dan memahami prosesnya. Tujuan tugas ini adalah mengintegrasikan teori kriptografi dengan keterampilan pemrograman data science, sejalan dengan kurikulum program studi yang menekankan analisis dan keamanan data.

2. Tujuan

- Memahami prinsip dasar kriptografi dan penerapannya dalam keamanan data.
- Mengembangkan kemampuan analisis alur kerja algoritma kriptografi.
- Menerapkan implementasi program sederhana untuk enkripsi dan dekripsi data.
- Mendorong kreativitas dalam desain aplikasi yang user-friendly, dengan potensi integrasi data science (misalnya, handling teks atau file data).

3. Ruang Lingkup

- Mahasiswa wajib memilih satu dari 5 opsi algoritma kriptografi pada tabel 1 berikut yang setara kompleksitasnya. Pilihan ini dirancang untuk relevansi dengan Data Science, seperti enkripsi dataset tabular, streaming data, atau key exchange untuk model ML. Setiap opsi memerlukan pemahaman matematika dasar (e.g., modular arithmetic) dan implementasi dengan library Python seperti `*cryptography*` atau `*pycryptodome*`.

TABEL 1 ALTERNATIF PILIHAN ALGORITMA

No	Algoritma	Jenis	Kompleksitas (1-5)	Fokus Utama	Integrasi Data Science
1	AES-256 (CBC mode)	Simetris Block	5	Enkripsi data massal	Enkripsi dataset CSV/Excel secara batch
2	ChaCha20-Poly1305	Simetris Stream	4	Enkripsi authenticated	Streaming enkripsi data real-time (IoT)
3	RSA-2048 (OAEP)	Asimetris	5	Key exchange & signing	Enkripsi metadata atau API keys
4	Serpent-256 (CBC)	Simetris Block	5	Alternatif AES	Benchmark keamanan pada big data
5	Camellia-256 (CBC)	Simetris Block	4	Kompatibilitas internasional	Enkripsi file terstruktur (JSON/XML)

Detail Singkat Opsi Algoritma:

- AES-256 (CBC mode): Block cipher simetris standar NIST. Alur: Plaintext dibagi block 128-bit, di-XOR dengan IV, diproses 14 ronde substitusi/permutasi. Kompleksitas tinggi (handle padding, IV, key derivation PBKDF2).
- ChaCha20-Poly1305: Stream cipher AEAD. Alur: Keystream dari 20 ronde ARX, XOR dengan plaintext; Poly1305 untuk MAC. Lebih cepat untuk mobile, fokus nonce unik.
- RSA-2048 (OAEP): Asimetris berbasis faktorisasi prima. Alur: Generate kunci public/private; enkripsi C = (M^e mod n) dengan OAEP. Cocok hybrid dengan AES untuk data besar.
- Serpent-256 (CBC): Alternatif AES (finalis kompetisi AES). Alur: 32 ronde bit-slicing dengan S-box kompleks. Dorong komparasi keamanan.
- Camellia-256 (CBC): Block cipher ISO Jepang. Alur: 24 ronde Feistel network dengan FL layers. Mudah adaptasi dari AES, untuk kompatibilitas global.

Fitur Aplikasi: Program harus mencakup:

- Input teks/file sederhana (e.g., CSV, xls, etc).
- Proses enkripsi/dekripsi dengan key management dasar.
- Output hasil yang jelas (e.g., hex-encoded ciphertext).
- Batasan:
    - Program dibatasi pada implementasi dasar (CLI cukup; GUI opsional).
    - Ukuran file input maksimal 1 MB.
    - Tidak termasuk analisis performa lanjutan kecuali diminta.

4. Metodologi Pengerjaan

Pengerjaan tugas dibagi menjadi tiga tahap utama. Waktu pengerjaan estimasi: 2 minggu

- **Tahap 1: Penelitian dan Penjelasan Algoritma (Hari 1-3)**

Aktivitas :

- Pilih 1 algoritma dari 5 opsi pada tabel 1 dan pelajari literatur dasar (misalnya, dari buku "Cryptography and Network Security" oleh Stallings atau sumber online seperti NIST guidelines).
- Jelaskan alur/cara kerja algoritma secara rinci, termasuk:
    - Prinsip Dasar: Jenis kriptografi (simetris/asimetris), kunci, dan tujuan (kerahasiaan, integritas, autentikasi).
    - Alur Kerja (Flowchart): Gambarkan langkah-langkah enkripsi/dekripsi dengan diagram sederhana (gunakan tools seperti Draw.io atau kode Mermaid untuk visualisasi).
    - Contoh Manual: Hitung enkripsi/dekripsi untuk input sederhana (misalnya, teks "HELLO" atau block data dengan kunci tertentu).

Output : Laporan teks (1-2 halaman) dengan diagram alur.

Bantuan AI : Gunakan LLM untuk generate flowchart atau contoh perhitungan, tapi verifikasi manual.

- **Tahap 2: Desain Aplikasi (Hari 4-7)**

Aktivitas :

- Rancang struktur program: Input (teks/kunci), proses (enkripsi/dekripsi), output.
- Tentukan library: Gunakan Python standar untuk cipher sederhana; `cryptography` untuk AES/RSA (install via pip jika di luar environment kuliah).
- Buat pseudocode atau sketsa fungsi utama, termasuk integrasi Data Science (e.g., Pandas untuk baca file).

Output : Dokumen desain (pseudocode + ERD sederhana jika ada database mini untuk simpan kunci).

Bantuan AI : gunakan LLM untuk membantu generate pseudocode berdasarkan deskripsi alur.

- **Tahap 3: Implementasi dan Pengujian (Hari 8-14)**

Aktivitas:

- Tulis kode Python lengkap (lihat snippet contoh di lampiran KAK untuk inspirasi).
- Uji dengan berbagai input (normal, edge case seperti kunci kosong atau file besar).
- Dokumentasikan kode dengan komentar.

Output: File .py executable + laporan pengujian (screenshot hasil).

Bantuan AI: Gunakan LLM untuk debug error atau optimasi kode, cantumkan prompt yang digunakan.

5. Deliverables dan Penilaian

Deliverables:

1. Laporan PDF/Word (5-10 halaman): Latar belakang, penjelasan algoritma (dengan diagram), desain, kode, hasil pengujian, dan refleksi (termasuk penggunaan AI).
2. File kode .py (dengan README.txt untuk instruksi).
3. Demo singkat (video 2-3 menit).

Kriteria Penilaian (Total 100%):

TABEL 2 KRITERIA PENILAIAN

Kriteria	Bobot	Deskripsi
Penjelasan Algoritma & Alur	30%	Kelengkapan, akurasi, dan visualisasi (termasuk pemilihan opsi yang tepat).
Desain & Implementasi Kode	40%	Kebenaran logika, user-friendly, error handling, dan integrasi library.
Pengujian & Dokumentasi	20%	Contoh kasus, screenshot, komentar kode.
Inovasi & Refleksi (termasuk AI usage)	10%	Kreativitas + etika penggunaan AI.

6. Jadwal dan Dukungan

- Deadline: [Isi tanggal, misalnya 6 November 2025].
- Konsultasi: Hubungi dosen via email/Zoom setiap Jumat (14:00-15:00 WIB).
- Sumber Belajar Tambahan:
    - Online: Crypto101.io, Python Cryptography docs, NIST SP 800-38A untuk mode CBC.