BUSINESS REQUIREMENTS DOCUMENT (BRD)

Pengembangan Aplikasi Kriptografi AES-256 Berbasis Streamlit

1. Pendahuluan

1.1 Latar Belakang

Banyak dokumen penting disimpan dalam bentuk file digital tanpa perlindungan kriptografi yang memadai, sehingga menimbulkan risiko kebocoran data. Penggunaan aplikasi enkripsi yang ada seringkali masih berbasis terminal (*command line*), yang menyulitkan pengguna non-teknis.

1.2 Tujuan Proyek

- Merancang aplikasi web sederhana untuk enkripsi dan dekripsi file menggunakan algoritma AES-256.
- Memberikan antarmuka yang ramah pengguna melalui framework Streamlit sehingga proses keamanan data dapat dilakukan tanpa perintah terminal.

2. Cakupan Bisnis (Business Scope)

Aplikasi ini ditujukan untuk pengguna personal yang ingin mengamankan file lokal (seperti dokumen PDF, teks, atau media) sebelum disimpan atau dibagikan.

3. Persyaratan Fungsional (Functional Requirements)

Aplikasi harus memenuhi fungsi-fungsi utama berikut:

- **FR-01: Pemilihan Mode Operasi** Sistem harus menyediakan opsi radio button untuk memilih antara mode "Encrypt" (Enkripsi) atau "Decrypt" (Dekripsi).
- **FR-02: Manajemen Unggah File** Sistem harus memungkinkan pengguna mengunggah file uji dengan berbagai ukuran dan tipe (PDF, .txt, .jpg, .mp4).
- **FR-03: Keamanan Berbasis Password** Sistem wajib menyediakan field input password sebagai dasar pembentukan kunci AES-256.
- **FR-04: Proses Enkripsi** Sistem harus menghasilkan kunci melalui PBKDF2-HMAC-SHA256 dengan salt, lalu mengenkripsi file menggunakan mode AES-GCM.
- **FR-05: Proses Dekripsi** Sistem harus mampu memisahkan salt/nonce, menghitung ulang kunci, dan mengembalikan file ke bentuk semula jika password benar.
- **FR-06: Penanganan Kesalahan (Error Handling)** Jika password salah atau data korup, sistem harus menampilkan pesan kesalahan dan tidak menghasilkan file plaintext.
- **FR-07: Pengunduhan Hasil** Sistem harus menyediakan tombol unduh untuk file berekstensi .enc (setelah enkripsi) atau file asli (setelah dekripsi).

4. Persyaratan Non-Fungsional (Non-Functional Requirements)

- **Keamanan (Security):** Menggunakan AES-256 bit yang tahan terhadap serangan *brute-force* dan menyediakan autentikasi integritas data.
- **Kegunaan (Usability):** Antarmuka harus sederhana agar layak sebagai solusi harian bagi pengguna umum.
- **Performa:** Waktu pemrosesan enkripsi dan dekripsi harus berada pada rentang yang dapat diterima (di bawah 6 detik untuk file hingga 18 MB).

5. Alur Kerja Sistem (System Workflow)

1. **Input:** Pengguna memilih mode, mengunggah file, dan memasukkan password.
2. **Proses:** Sistem menjalankan fungsi PBKDF2 dan AES-GCM.
3. **Output:** Sistem menyediakan file hasil proses untuk diunduh melalui browser.

6. Kriteria Penerimaan (Acceptance Criteria)

- Seluruh file uji (kecil hingga besar) dapat dienkripsi dan didekripsi dengan benar tanpa kerusakan data.
- File terenkripsi tidak dapat dibaca secara langsung tanpa proses dekripsi yang valid.
- Percobaan dekripsi dengan password salah dipastikan gagal mengeluarkan data asli.