BUSINESS REQUIREMENTS DOCUMENT (BRD)

1. Pendahuluan

1.1 Latar Belakang

Perkembangan teknologi informasi yang sangat pesat telah mendorong perubahan besar dalam cara manusia menyimpan, mengelola, dan memanfaatkan data digital. Salah satu bentuk data yang bersifat sangat pribadi dan sensitif adalah catatan harian digital, yang dapat berisi informasi personal, pemikiran individu, hingga data penting lainnya. Seiring meningkatnya ketergantungan terhadap aplikasi berbasis web, risiko kebocoran data dan akses tidak sah juga semakin meningkat.

Berdasarkan hasil *Systematic Literature Review (SLR)* yang telah dilakukan, diketahui bahwa algoritma kriptografi klasik seperti Caesar Cipher dan Vigenère Cipher memiliki kelemahan apabila digunakan secara tunggal. Namun, kombinasi kedua algoritma tersebut, khususnya dengan varian Vigenère Autokey melalui konsep *super encryption*, mampu meningkatkan tingkat keamanan data secara relatif. Pendekatan ini dinilai efisien secara komputasi dan sesuai untuk aplikasi berskala ringan seperti sistem penyimpanan catatan harian.

1.2 Tujuan Dokumen

Dokumen Business Requirements Document (BRD) ini disusun untuk mendefinisikan kebutuhan bisnis, kebutuhan sistem, serta batasan pengembangan aplikasi web catatan harian yang menerapkan kombinasi algoritma Caesar Cipher dan Vigenère Cipher (Autokey). Dokumen ini menjadi acuan utama bagi pengembang, pemangku kepentingan, dan pihak akademisi dalam memahami arah pengembangan sistem.

1.3 Ruang Lingkup

Ruang lingkup BRD ini meliputi:

- Identifikasi kebutuhan bisnis sistem keamanan data catatan harian
- Perumusan kebutuhan fungsional sistem
- Perumusan kebutuhan non-fungsional sistem
- Identifikasi stakeholder yang terlibat
- Batasan dan risiko sistem

2. Tujuan Bisnis

2.1 Tujuan Utama

Tujuan utama pengembangan sistem ini adalah menyediakan aplikasi web catatan harian yang memiliki tingkat keamanan penyimpanan data lebih baik dibandingkan penggunaan satu algoritma kriptografi klasik, tanpa mengorbankan performa sistem.

2.2 Tujuan Khusus

- Mengimplementasikan konsep *super encryption* berbasis kombinasi Caesar Cipher dan Vigenère Autokey.
- Menjaga kerahasiaan data teks pengguna dari akses tidak sah.
- Menyediakan solusi keamanan data yang bersifat *lightweight* dan efisien secara komputasi.

- Menjadi media implementasi dan pembelajaran kriptografi klasik dalam konteks sistem informasi.

3. Stakeholder

Stakeholder	Peran dan Kepentingan
Pengguna	Menggunakan aplikasi untuk menulis, menyimpan, dan membaca catatan harian secara aman
Pengembang Sistem	Merancang, membangun, dan menguji aplikasi sesuai kebutuhan bisnis
Akademisi/Peneliti	Mengkaji dan mengevaluasi penerapan kriptografi klasik kombinasi
Administrator Sistem	Mengelola sistem, server, dan keamanan aplikasi

4. Kebutuhan Bisnis

Kebutuhan bisnis yang harus dipenuhi oleh sistem antara lain:

- Sistem mampu memberikan perlindungan terhadap data teks pribadi pengguna.
- Sistem mendukung proses enkripsi dan dekripsi data secara efisien.
- Sistem tidak meningkatkan ukuran data secara signifikan setelah proses enkripsi.
- Sistem dapat dijadikan sebagai objek penelitian atau studi akademik.

5. Kebutuhan Fungsional

5.1 Manajemen Catatan Harian

- Sistem menyediakan fitur untuk membuat catatan harian baru.
- Sistem memungkinkan pengguna mengubah dan menghapus catatan harian.
- Sistem menyimpan catatan dalam bentuk terenkripsi.

5.2 Proses Enkripsi Data

- Sistem melakukan enkripsi data menggunakan Vigenère Cipher Autokey sebagai tahap pertama.
- Hasil enkripsi tahap pertama dienkripsi kembali menggunakan Caesar Cipher.
- Proses enkripsi dilakukan secara otomatis saat catatan disimpan.

5.3 Proses Dekripsi Data

- Sistem melakukan dekripsi data secara berurutan, dimulai dari Caesar Cipher kemudian Vigenère Autokey.
- Dekripsi hanya dapat dilakukan apabila kunci yang dimasukkan sesuai.

5.4 Manajemen Kunci

- Sistem mengharuskan pengguna memasukkan kunci enkripsi secara manual.
- Sistem tidak menyimpan kunci dalam bentuk teks asli.
- Sistem menolak proses dekripsi apabila kunci tidak valid.

6. Kebutuhan Non-Fungsional

6.1 Keamanan

- Sistem menjamin kerahasiaan data melalui penerapan kriptografi simetris.
- Data plaintext tidak disimpan di dalam basis data.

6.2 Performa

- Proses enkripsi dan dekripsi berjalan dengan waktu respons yang cepat.
- Ukuran ciphertext relatif sama dengan plaintext.

6.3 Usability

- Antarmuka aplikasi sederhana dan mudah digunakan.
- Pengguna tidak perlu memahami detail teknis algoritma kriptografi.

6.4 Reliability

- Sistem mampu melakukan proses enkripsi dan dekripsi secara konsisten tanpa kesalahan.

7. Batasan Sistem

- Sistem menggunakan algoritma kriptografi klasik dan tidak dimaksudkan sebagai pengganti kriptografi modern.
- Sistem menerapkan kriptografi simetris sehingga kunci harus dijaga kerahasiaannya.
- Fokus pengamanan terbatas pada data teks.

8. Risiko dan Mitigasi

Risiko	**Dampak**	**Strategi Mitigasi**
Kebocoran kunci	Data dapat diakses pihak tidak sah	Edukasi pengguna dan kebijakan pengelolaan kunci
Kesalahan input kunci	Data tidak dapat didekripsi	Validasi input dan pesan kesalahan
Keterbatasan karakter	Data tidak terenkripsi sempurna	Pengembangan algoritma extended

9. Kriteria Keberhasilan

- Sistem berhasil melakukan enkripsi dan dekripsi dengan benar.

- Sistem berjalan stabil dan responsif.
- Keamanan data meningkat berdasarkan analisis literatur.

10. Kesimpulan

Dokumen BRD ini menjelaskan secara rinci kebutuhan bisnis dan kebutuhan sistem untuk pengembangan aplikasi web catatan harian yang aman menggunakan kombinasi Caesar Cipher dan Vigenère Autokey. Berdasarkan hasil SLR, pendekatan *super encryption* ini dinilai layak sebagai solusi keamanan ringan serta relevan untuk kebutuhan akademik dan pembelajaran kriptografi klasik.