Text

Assalamualikum Wr...Wb...

Mukadimah

Baik, mungkin untuk mempersingkat waktu, dan tanpa mengurangi rasa hormat saya, kata-kata penghormatan saya, yang saya hormati :

1. Ibu Cut mutia SST.,MT selaku dosen pembimbing utama skripsi saya
2. Yang saya hormati Ibu Cukri rahmi niani SP.d,.M.Si selaku dosen pembimbing 2 saya,
3. Dan yang saya hormati bapak abdullrahman ridho sst mt
4. dan ibuk hayatun magfirah sst mt, selaku dosen penguji 1 dan 2 saya
5. Dan yang saya banggakan teman seperjuangan saya yang telah berhadir di seminar proposal saya kali ini.

Baik, Mungkin langsung saja ke topik pembahasan saya kali ini, yaitu dengan judul "**Perancangan dan Implementasi Keamanan Data Kependudukan Desa Namo Buaya Menggunakan Metode Enkripsi AES 128-bit berbasis Web"**

- **Baca latar belakang**

Adapun alasan saya mengambil judul ini tidak lepas dari minimnya ilmu pengetahuan teknologi yang memungkinkan data kependudukan desa namo buaya dapat di curi, sehingga dapat merugikan beberapa pihak. di karnakan akses yang tidak sah dalam 1 perangkat komputer yang di pakai secara bergantian, maka dari itu saya berinisiatif ingin mengambil judul ini untuk menguatkan pengamanan data kependudukan pada desa namo buaya.

Kisi-kisi

Aspek Metode

1. Mengapa Anda memilih metode enkripsi AES 128-bit?

- AES 128-bit dipilih karena merupakan standar enkripsi yang diakui secara internasional, memiliki keseimbangan yang baik antara keamanan dan performa, serta telah banyak digunakan dan diuji dalam berbagai aplikasi.
- Kelebihan AES 128-bit adalah kecepatan enkripsi yang tinggi dan kekuatan keamanan yang cukup untuk melindungi data sensitif. Kekurangannya adalah jika kunci tidak dikelola dengan baik, dapat menjadi titik lemah dalam sistem keamanan.

2. Bagaimana cara kerja metode enkripsi AES 128-bit?

- Proses enkripsi AES 128-bit melibatkan substitusi byte, pergantian baris, pencampuran kolom, dan penambahan kunci pada setiap putaran (round). Terdapat total 10 round dalam AES 128-bit.
- Dekripsi melibatkan proses yang sama namun dengan langkah-langkah yang dibalik, mengembalikan ciphertext ke plaintext menggunakan kunci yang sama.

3. Mengapa memilih pendekatan berbasis web?

- Pendekatan berbasis web dipilih untuk memudahkan akses data secara terpusat dan real-time oleh aparat desa dan pihak terkait.

Aspek Implementasi

4. Bagaimana Anda menangani masalah privasi dan legalitas data kependudukan?

- Kebijakan privasi dan persetujuan pengguna diimplementasikan untuk memastikan bahwa data digunakan sesuai izin yang diberikan.

Aspek Relevansi

1. Mengapa penelitian ini penting untuk Desa Namo Buaya?

- Penelitian ini penting karena melindungi data sensitif warga dari potensi pencurian dan penyalahgunaan, serta meningkatkan efisiensi administrasi kependudukan.
- Dampak langsungnya adalah peningkatan kepercayaan warga terhadap pengelolaan data oleh desa.

Algoritma AES-128 bit

Plainteks (plaintext), adalah data atau informasi yang dapat dibaca dan dimengerti maknanya. Pesan yang tersimpan tidak hanya berupa teks, tetapi juga dapat berbentuk citra (image), suara/bunyi (audio), dan video, atau berkas biner lainnya.

Cipherteks (ciphertext), adalah bentuk pesan yang tersandi atau hasil dari penyamaran plainteks.

Contoh :

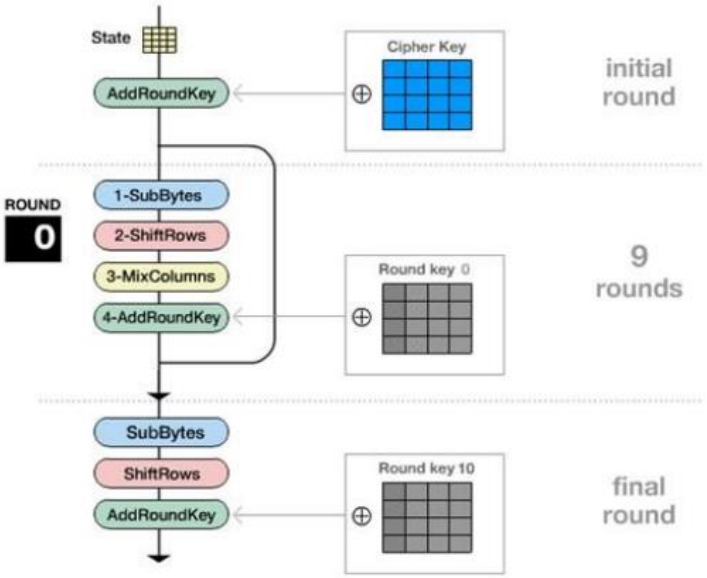
Plaintext : malam ini kita bantai mereka

Chipertext : *2b7e151628aed2a6abf7158809cf4f3c*

Enskripsi, adalah proses menyandikan plaintext menjadi ciphertext.

Deskripsi, adalah proses mengembalikan ciphertextmenjadi plaintext semula.

Proses Enkripsi:



- **Initial Round (AddRoundKey):** Kunci yang sudah di-generate akan di-"XOR" kan dengan blok teks biasa.
- **Rounds:** Dilakukan 9 putaran (rounds).
    - **SubBytes:** Setiap byte dalam matriks di-substitusi menggunakan tabel S-box, menghasilkan matriks baru yang disubstitusi.
    - **ShiftRows:** Setiap baris dalam matriks bergeser ke kiri. Posisi geser baris sesuai dengan nomor baris (baris pertama tidak digeser, baris kedua digeser satu byte ke kiri, dan seterusnya).
    - **MixColumns:** Operasi matriks di mana setiap kolom matriks dikalikan dengan matriks
    - **AddRoundKey:** Matriks blok 4x4 di-"XOR" kan dengan kunci putaran saat ini
- **Final Round:** Hanya terdiri dari tiga langkah:
    - **SubBytes**
    - **ShiftRows**
    - **AddRoundKey**

Jenis algoritma AES

	Panjang kunci	Panjang blok	Jumlah putaran
AES 128	4	4	10
AES192	6	4	12
AES 256	8	4	14

Panjang Kunci: **128-bit** (16 byte). 16 kotak 4 baris pada matrix
Panjang Kunci: **192-bit** (24 byte). 24 kotak 6 baris pada matrix
Panjang Kunci: **256-bit** (32 byte). 32 kotak 8 baris pada matrix

Jadi 128 terdapat 32 kharakter huruf , Setiap digit heksadesimal mewakili 4 bit,
192 terdapat 48 kharakter huruf , Setiap digit heksadesimal mewakili 4 bit,
256 terdapat 64 kharakter huruf , Setiap digit heksadesimal mewakili 4 bit,

Contoh : 8e73b0f7da0e6452c810f32b809079e562f8ead2522c6b7b = 48 kharakter huruf