PRAKTIK SISTEM KEAMANAN DATA
ALGORITMA DES

Disusun Oleh:

Bagas Aditya pramudana	(V3920012)
Dion Aji cahyono	(V3920018)
Isnan Nur Ahmad Wijayakusuma	(V3920029)
Ivan Fausta Dinata	(V3920030)
Kreshna Pura Adi Wicaksana)	(V3920032)

PROGRAM STUDI D-III TEKNIK INFORMATIKA (MADIUN)

FAKULTAS SEKOLAH VOKASI

UNIVERSITAS SEBELAS MARET

SURAKARTA

2021

Resume Jurnal

Jurnal 1

1 Judul

Implementasi Algoritma Data Encryption Standard Pada Penyandian Record Database

2 Latar Belakang Masalah

Masalah keamanan dan kerahasiaan suatu Data merupakan hal yang penting dalam suatu instansi atau pun perusahaan, sehingga perlu dilakukan pengamanan data terlebih dahulu agar tidak dapat dibaca atau dilacak oleh pihak-pihak yang tidak bertanggung jawab.

3 Tujuan Penelitian

Tujuan dari jurnal ini adalah untuk melakukan sebuah implementasi pengamanan pada sebuah record database untuk mempersulit para pihak-pihak yang ingin berbuat hal yang tidak baik atau hal yang merugikan.

4 Algoritma & Alur Penelitian

Algoritma yang digunakan adalah algoritma DES (Data Encryption Standard).

Alur penelitian :

Dengan Penyimpanan data menggunakan database,dan menggunakn salah satu algoritma kriptografi untuk mengekripsi data.kemudian Teks record di dalam database akan disandikan menjadi simbol-simbol .Record database yang akan dienkripsi yaitu record dari database. Dengan mengkonversi kunci ke biner, sehingga dihasilkan biner yang di sebut Proses Generate Key (Pembangkitan Kunci).

Char Kunci	Decimal	Biner
N	78	0100 1110
E	69	0100 0101
T	84	0101 0100
I	73	0100 1001
&	38	0010 0110
D	68	0100 0100
K	75	0100 1011
K	75	0100 1011

Kunci, terbagi menjadi dua bagian, kunci rahasia (private key) dan kunci umum (public key).

Proses Enkripsi :

Kelompokkan biner plain menjadi 64 bit setiap kelompok. Karena karakter yang dienkripsi hanya 8 karakter (64 bit) berarti memenuhi satu kelompok.

Proses Dekripsi :

Proses dekripsi diawali dengan memanfaatkan biner-biner cipher yang dibaggi menjadi dua kelompok.Dua blok ini kemudian di permutasikan berdasarkan tabel permutasi invers (IP1). Output dari dekripsi adalah blok L[0] dan R[0] sehingga didapatkan biner-biner plaintext seperti semula.

5 Hasil Penelitian & Kesimpulan

Kesimpulan yang dapat diambil dari resume ini yang pertama ialah penyandian record database menggunakan algoritma DES ini mampu mempersulit pihak-pihak lain yang iseng dan jahat untuk memahami dan mengerti isi dari record database ini, penyandian ini diawali dengan penentuan nama database dan pemilihan tabel yang dimana akan diberi sandi dan selanjutnya akan dipilih kan sandinya berdasarkan algoritma DES, dan juga tingkat keamanan algoritma ini cukup aman karena memiliki kunci yang besar yang pada internalnya terdapat 57 bit dan eksternal nya terdapat 64 bit.

Jurnal 2

1 Judul

Aplikasi Enkripsi Dan Dekripsi Menggunakan Visual Basic 2012 Dengan Algoritma Triple DES

2 Latar Belakang Masalah

Pada Era Globalisasi saat ini, arus informasi merupakan suatu hal yang memegang peranan penting. Bahkan ada yang mengatakan bahwasanya jika ada yang mampu menguasai jaringan informasi, maka dia akan mampu menguasai dunia. Sehubungan dengan hal tersebut, banyak juga pihak-pihak yang berusaha mencuri atau mengakses informasi yang pihak tersebut tidak memiliki hak untuk melakukan akses terhadap informasi itu.

3 Tujuan Penelitian

Tujuan dari jurnal ini yang pertama ialah mengetahui apasih kriptografi itu, selanjutnya yang kedua untuk mengetahui bagaimana proses enkripsi dan dekripsi yang dilakukan menggunakan metode Triple DES, dan yang ketiga ini digunakan untuk merancang sebuah aplikasi sistem proteksi untuk file dengan menggunakan metode visual basic 2012.

4 Algoritma & Alur Penelitian

Algoritma yang digunakan adalah 3DES (Triple Data Encryption Standard)
Alur Penelitian :

3DES menggunakan 3 kunci yang panjangnya 168- bit (masing-masing panjangnya 56-bit).selanjutnya melakukan Pemilihan kunci eksternal pada algoritma 3DES:

a. K1, K2, dan K3 adalah kunci-kunci yang saling bebas

$K1 \neq K2 \neq K3 \neq K1$

- Selanjutnya Text box lokasi file untuk memilih file yang akan dilakukan enkripsi.
- Button enkripsi berfungsi untuk mulaimemproses enkripsi file.

Proses Enkripsi File :

Proses enkripsi ini data yang asli akan dilakukan proses pengacakan dengan algoritma yang sudah ditentukan. Proses enkripsi dilakukan setelah menginputkan file yang akan dienkripsi dan menginputkan key pada textbox password.

Proses Dekripsi File :

Untuk mengembalikan file kembali ke bentuk semula memasukan kunci atau key kedalam textbox.dan password harus sama dengan password pada saat proses enkripsi maka program akan melakukan proses dekripsi file.

5 Hasil Penelitian & Kesimpulan

Kesimpulan pada jurnal ini ialah dengan menerapkan algoritma Triple DES ini membuat aplikasi atau file yang ada pada komputer kita menjadi lebih aman dan terjamin kerahasiaannya semisal file yang di maksud (Gambar,dokumen,pdf,folder,dll).dan dimana waktu pada enkripsi dan dekripsi nya ini dipengaruhi oleh kecepatan komputer yang digunakan dan ukuran setiap filenya.