MAKALAH KEAMANAN PERANGKAT LUNAK

TEMA : “DES *(Data Encryption Standard)*”



Nama Anggota Kelompok 1:

Ridho Surya

Novriandhandy

Elki Tri Okta

Yani Cardova 1910031802015

TEKNIK INFORMATIKA

STMIK Amik Riau

2022/2023

**KATA PENGANTAR**

Puji syukur atas kehadiran Allah SWT yang mana telah melimpahkan rahmat dan karunianya sehingga kami Kelompok 1 TI Mobile 6 B dapat menyelesaikan makalah ini demi memenuhi tugas matakuliah KPL (Kemanan Perangkat Lunak) dengan dosen pengampu bapak Syahrul Imardi, M.T.

Kami penulis sangat berharap semoga makalah yang kami susun dapat bermanfaat bagi para pembaca dan menambah pengetahuan baru mengenai DES *(Data Encryption Standard)* yang akan dibahas di makalah ini nantinya.

Bagi kami penyusun makalah masih merasa bahwa banyak kekurangan saat menyusun makalah karena keterbatasan pengetahuan dan juga pengalaman. Oleh karena itu kami sebagai penulis beserta penyusun sangat berterimakasih apabila ada pembaca yang memberi kritik serta saran yang membangun demi kesempurnaan makalah ini.

Pekanbaru 19 April 2022

Penyusun

(Kelompok 1)

**BAB I**

**PENDAHULUAN**

**1.1 Latar Belakang**

Kemananan sangat dibutuhkan dalam komputer baik dari segi aplikasi maupun untuk keamanan data pribadi saat menggunakan aplikasi. Keamanan juga sangat penting karena berisi data dan informasi yang sensitif maka jika itu hilang atau disalah gunakan bisa saja menimbulkan kerugian bagi pemiliknya. Tujuannya ialah untuk membantu user/pengguna bisa mencegah terjadinya penipuan, ataupun bisa mendeteksi jika ada usaha untuk penipuan pada sebuah sistem dengan berbasis informasi (Gramedia 2019). Ketika suatu ancaman keamanan pada pengguna terdeteksi maka itu akan cepat teratasi dan kerugian pada pengguna mungkin bisa di minimalisirkan. Menurut (Sutiono S.Kom, M.Kom, M.T.I 2022) Keamanan komputer menjadi salah satu hal utama yang perlu diperhatikan oleh para pengguna komputer. Pasalnya, dengan adanya keamanan komputer / *cybersecurity*, segala jenis penipuan yang akan merugikan para pengguna dapat dicegah dan dideteksi dini menggunakan sebuah sistem yang berbasis informasi. Segala bentuk transaksi dan pencarian informasi saat menjelajah di komputer harus di waspadai oleh pengguna maka jangan membuka tautan sembarangan ataupun memasuki sebuah situs yang tidak resmi.

Enkripsi salah satu cara untuk mengamankan data yang banyak digunakan. Ketika kita melakukan transaksi data maka data tersebut tidak dapat dipahami oleh pihak ketiga. Pada engkripsi biasanya menggunakan kode-kode tertentu yang mana merubah data asli menjadi kode yang sulit dipahami oleh orang lain. Untuk mengembalikan kode enkripsi menjadi data awal maka diperlukan kunci-kunci tertentu seperti penerapan algoritma yang dapat memecahkan kode-kode enkripsi. Tujuan dari makalah ini yaitu membahas mengenai salah satu penggunaan enkripsi yaitu DES *(Data Encryption Standard).* Oleh karena itu makalah ini akan membahas mengenai tema tersebut dan diharapkan akan menembah wawasan para pembaca mengenai enkripsi DES *(Data Encryption Standard).*

**1.2 Maksud dan Tujuan**

Adapun maksud dan tujuan kami dalam pembuatan makalah yaitu:

1. menambah pengetahuan mengenai DES *(Data Encryption Standard)*
2. menambah pengetahuan bahwa enkripsi itu sangat penting

**1.3 Metode Penulisan**

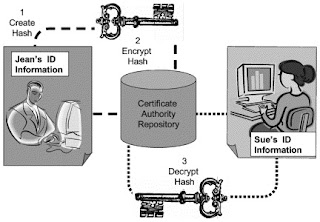
Penyusunan makalah ini kami lakukan dengan cara menganalisa dan membaca dari berbagai sumber yang telah di terbitkan oleh para ahli melalui jurnal maupun internet.

**BAB II**

**PEMBAHASAN**

**2.1 Pengertian DES *(Data Encryption Standard)***

DES, atau juga dikenal sebagai Data Encryption Algorithm (DEA) oleh ANSI dan DEA-1 oleh ISO, merupakan algoritma kriptografi simetris yang paling umum digunakan saat ini. Secara umum, DES termasuk ke dalam sistem kriptografi simetri dan tergolong jenis cipher blok. DES beroperasi pada ukuran blok 64 bit. DES mengenkripsikan 64 bit plainteks menjadi 64 bit cipherteks dengan menggunakan 56 bit kunci internal (internal key) atau lupa-kunci (subkey). Kunci internal dibangkitkan dari kunci eksternal (external key) yang panjangnya 64 bit (Donzelio Antonio Meko 2018) .Algoritma DES (Data Encryption Standard) adalah algoritma cipher blok yang digunakan untuk keamanan informasi dengan menggunakan metode simetrik dalam mengenkripsi dan dekripsi data ataupun informasi (widiarti Rista Maya, dkk 2022). DES (*Data Encryption System*) dimulai dengan mengubah plaintext dan key kedalam bentuk biner. Setiap hasil putaran digabungkan kembali dan diinput kedalam tabel Permutation Compression 2 (PC-2) dan terjadi kompresi data CiDi 56 bit menjadi CiDi 48 bit (Nuvelius Buulolo dkk 2020). Jadi dapat disimpulkan DES *(Data Encryption Standard)* merupakan algoritma kriptografi simetris yang sangat umum digunakan dan tergolong chiper blok yang beroperasi dalam 64 bit yang memiliki 56 bit kunci internal dan sub kunci.



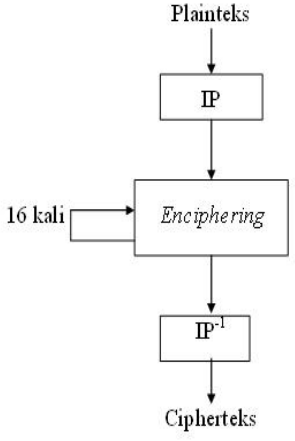
Gambar 1. Priyaprakharmrigank.blogspot.com

**2.2 Sejarah singkat DES *(Data Encryption Standard)***

Sekitar tahun 1960 IBM melakukan riset mengenai kriptografi yang bernama Lucifer. 1971 Lucifer dijual ke salah satu perusahaan di London. IBM mencoba mendaftarkan algoritmanya di tahun 1977 algoritma tersebut dijadikan sebagai DES (Data Encryption Standard). Pada tahun 1998, 70 ribu komputer di internet berhasil menjebol satu kunci DES dengan waktu sekitar 96 hari. Bahkan pada tahun 1999 berhasil dibobol dalam waktu kurang dari 22 hari. Pada tanggal 16 juni 1998 ada sebuah kelompok yang menamakan dirinya Electronic Frontier Foundation (EFF) telah berhasil memecahkan DES dalam waktu 4-5 hari menggunakan komputer yang dilengkapi dengan Integrated Circuit Chip DES Cracker. Di akhir tragedi ini, DES dianggap sudah tak aman lagi sehingga ia dicampakkan begitu saja dan digantikan oleh AES (Anvanced Encryption Standard). Jadi kesimpulan DES *(Data Encryption Standard)* didirikan oleh IBM dengan nama Lucifer yang kemudian dijual ke london setelah itu Amerika sedang membutuhkan kunci enkripsi makaditawarkan DES *(Data Encryption Standard)* namun karena sistem keamanan yang tidak lagi baik dari kasusnya yang mudah di bobol maka DES *(Data Encryption Standard)* tidak digunakan lagi dan digantikan oleh AES (*Anvanced Encryption Standard*).

**2.3 Panjang Kunci dan Ukuran Blok DES**

Panjang kunci ekternal = 64 bit (sesuai ukuran blok), tetapi hanya 56 bit yang dipakai (8 bit paritas tidak digunakan). Setiap blok (plainteks atau cipherteks) dienkripsi dalam 16 putaran. Setiap putaran menggunakan kunci internal berbeda. Kunci internal (56-bit) dibangkitkan dari kunci eksternal. Setiap blok mengalami permutasi awal (IP), 16 putaran enciphering, dan inversi permutasi awal (IP-1 ).



Gambar 2 Skema Global Algoritma DES

**2.4 Metode DES *(Data Encryption Standard)***

DES termasuk ke dalam sistem kriptografi simetri dan tergolong jenis cipher blok. DES dirancang untuk melakukan enchiper dan dechiper data yang berisi 56 bit dibawah kendali 56 bit kunci internal atau upakunci. Dalam melakukan dechiper harus dilakukan dengan menggunakan kunci yang sama dengan saat proses enchiper tetapi sat melakukan dechiper pemberian halaman berubah sehingga proses dechiper merupakan kebalikan dari proses enchiper.

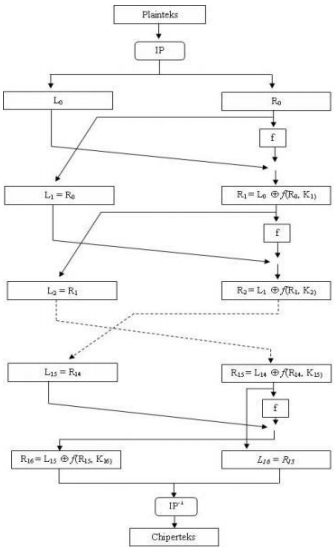
Sejumlah data yang akan di enchiper disebut sebagai permutasi awal atau initial permutation (IP). Komputasi key – dependent didefinisikan sebagai fungsi f sebgai fungsi chipper dan function KS sebagai key schedule. Deskripsi dari komputasi diberikan pertama, bersama dengan detail bagaimana algoritma digunakan dalam proses enchiper. Selanjutnya, penggunaan algoritma untuk proses dechiper dideskripsikan. Pada akhirnya, sebuah definisi chipper fungsi f diberikan dalam bentuk fungsi primitive yang disebut fungsi seleksi Si dan fungsi permutasi P.

**2.5 Skema Global DES**

* Pada awalnya, blok plainteks dipermutasi dengan matriks permutasi awal (initial permutation atau IP). Hasil dari permutasi awal tersebutkemudian di enchiper sebanyak 16 kali atau 16 putaran. Setiap putarannya menggunakan kunci internal yang berbeda. Hasil dari proses enchiper kembali dipermutasi dengan matrikspermutasi balikan (invers initial permutation atau IP-1 ) menjadi blok cipherteks.
* Dalam proses enchiper, blok plainteks terbagi menjadi dua bagian yaitu bagian kiri (L) dan bagian kanan (R), yang masing masing memiliki panjang 32 bit. Pada setiap putaran i, blok R merupakan masukan untuk fungsi transformasi fungsi f. Pada fungsi f, blok R dikombinasikan dengan kunci internal Ki. Keluaran dari fungsi ini di XOR kan dengan blok L yang langsung diambil dari blok R sebelumnya. Ini merupakan 1 putaran DES. Secara matematis, satu putaran DES dinyatakan sebagai berikut :

Li = Ri – 1

Ri = Li – 1 + f(Ri – 1, Ki)



**BAB III**

**KESIMPULAN**

**3.1 Kesimpulan**

Kami membahas secara rinci setiap poin dalam makalah ini yang mana kami dapatkan dari para ahli, jurnal, dan situs *internet.* Berikut kesimpulan dari makalah ini yaitu:

1. **Pengertian DES *(Data Encryption Standard)***

merupakan algoritma kriptografi simetris yang sangat umum digunakan dan tergolong chiper blok yang beroperasi dalam 64 bit yang memiliki 56 bit kunci internal dan sub kunci.

1. **Kesimpulan Sejarah**

DES *(Data Encryption Standard)* didirikan oleh IBM dengan nama Lucifer yang kemudian dijual ke london setelah itu Amerika sedang membutuhkan kunci enkripsi makaditawarkan DES *(Data Encryption Standard)* namun karena sistem keamanan yang tidak lagi baik dari kasusnya yang mudah di bobol maka DES *(Data Encryption Standard)* tidak digunakan lagi dan digantikan oleh AES (*Anvanced Encryption Standard*).

1. **Panjang Kunci dan Ukuran Blok DES**

Panjang kunci ekternal = 64 bit (sesuai ukuran blok), tetapi hanya 56 bit yang dipakai (8 bit paritas tidak digunakan). Setiap blok (plainteks atau cipherteks) dienkripsi dalam 16 putaran. Setiap putaran menggunakan kunci internal berbeda. Kunci internal (56-bit) dibangkitkan dari kunci eksternal. Setiap blok mengalami permutasi awal (IP), 16 putaran enciphering, dan inversi permutasi awal (IP-1 ).

1. **Metode DES (*Data Encryption* *Standard*)**

DES dirancang untuk melakukan enchiper dan dechiper data yang berisi 56 bit dibawah kendali 56 bit kunci internal atau upakunci.

1. **Skema Global DES**

Blok plainteks dipermutasi dengan matriks permutasi awal (initial permutation atau IP). Hasil dari permutasi awal tersebut kemudian di enchiper sebanyak 16 kali atau 16 putaran. Dalam proses enchiper, blok plainteks terbagi menjadi dua bagian yaitu bagian kiri (L) dan bagian kanan (R), yang masing masing memiliki panjang 32 bit.

**DAFTAR PUSTAKA**

https://www.studentterpelajar.com/2021/03/pengertian-algoritma-des.html