JURNAL MEDIA INFORMATIKA [JUMIN]
Volume 4, Nomor 1, Desember 2022, Page 63-69
ISSN ISSN 2808-005X
Available Online at http://ejournal.sisfokomtek.org/index.php/jumin

Penerapan Enkripsi Dan Deskripsi Menggunakan Algoritma Data Encryption Standart (DES) Dengan Pemograman Matlab

Jenni Hartati Sinaga[1], Maya Pangaribuan[2], Fazly[3], Iqbal Rivaldo[4], Indra Gunawan[5]

[1,2,3,4]Program Studi Teknik Informatika , STIKOM Tunas Bangsa Pematangsiantar
Email :[1]jennisinaga31@gmail.com*

Abstrak- Algoritma Data Encryption Standard (DES) adalah algoritma kriptografi yang termasuk dalam algoritma simetrik, dengan menggunakan kunci yang sama untuk enkripsi dan dekripsi. DES untuk enkripsi data menggunakan *Graphica*l User Interface Matlab.Graphic User Interface (GUI) merupakan Matlab script file yang dibut untuk menunjukkan analisasuatu permasalahan.Matlab menyediakan toolnya dan dapat dilihat dengan mengetikkan 'guide' pada MATLAB command window. Algoritma DES dengan menggunakan software MATLAB mengefesienkan pengguna dalam melakukan proses enkripsi dan dekripsi data.

Kata Kunci: DES, MATLAB, GUI, Enkripsi, Deskripsi.

Abstract- The Data Encryption Standard (DES) algorithm is a cryptographic algorithm that belongs to the symmetric algorithm, using the same key for encryption and decryption. DES for data encryption uses the Matlab Graphical User Interface. The Graphical User Interface (GUI) is a Matlab script file that is created to show the analysis of a problem. Matlab provides the tools and can be viewed by typing 'guide' in the MATLAB command window. The DES algorithm using MATLAB software streamlines the user in encrypting and decrypting data.

Kywords: DES, MATLAB, GUI, Encryption, Decryption.

1.PENDAHULUAN

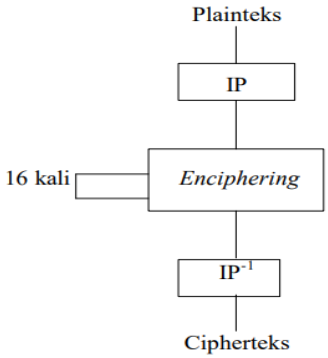
Untuk efisiensi suatu program, sering orang akan mencri sesuatu yang dapat memberikan hasil yang baik, sederhana, dan familiar untuk digunakan, serta mudah untuk input data atau melihat hasilnya. Masalah keamanan merupakan salah satu aspek terpenting pada sebuah system informasi.Kemajuan teknologi internet sebagai penghantar media informasi telah diadopsi oleh hampir semua orang.Dimana informasi menjadi suatu yang sangat berharga.Informasi menentukan hampir setiap elemen dalam kehidupan manusia.Informasi sangat penting artinya karena tanpa informasi, hampir semuanya tidak dapat dilakukan dengan baik.Contohnya, jika kita membeli tiket penerbangan dan membayarnya menggunakan kartu kredit, informasi mengenai diri kita disimpan dan dikumpulkan serta digunakan oleh pihak bank dan penerbangan.Demikian juga halnya dengan membeli obat di apotek, kita harus mendapatkan resep dari dokter dan memberikan resep tersebut kepada pelayan apotek.Hal tersebut juga merupakan salah satu informasi yang disampaikan oleh dokter kepada pihak apotek mengenai jenis obat yang dibutuhkan.

Karena berharganya suatu informasi ,maka informasi menjadi target serangan oleh para cracker.Karenanya,keamanan suatu informasi menjadi sesuatu informasi yang dijaga dengan baik.Pengamanan informasi pada prinsipnya berfungsi untuk melindungi informasi agar siapapun yang tidak berhak tidak dapat membaca , mengubahnya, atau menghapus informasi tersebut.Untuk permasalahan-permasalahan keamanan keaman tersebut diperlukan suatu metode untuk menjaga keamanan informasi.Salah satu metodenya adalah Enkripsi.

Enkripsi merupakan hal yang sangat penting dalam kriptografi supaya data yang dikirimkan bisa terjaga kerahasiannya. Pesan asli (plaintext) diunah menjadi kode-kode yang tidak dimengerti. Enkripsi bisa diartikan dengan chipper atau kode. Sama halnya dengan kita yang tidak mengerti sebuah kata, kita akan dapat melihatnya di dalam kamus atau daftar istilah-istilah. Berbeda halnya dengan enkripsi, untuk mengubah plaintext ke bentuk chiphertext, kita harus menggunakan algoritma yang dapat mengkodekan data yang kita inginkan.

Submitted: 1**5/11/2022**; Accepted: 25**/11/2022**; Published: 15**/12/2022**

JURNAL MEDIA INFORMATIKA [JUMIN]
Volume 4, Nomor 1, Desember 2022, Page 63-69
ISSN ISSN 2808-005X
Available Online at http://ejournal.sisfokomtek.org/index.php/jumin

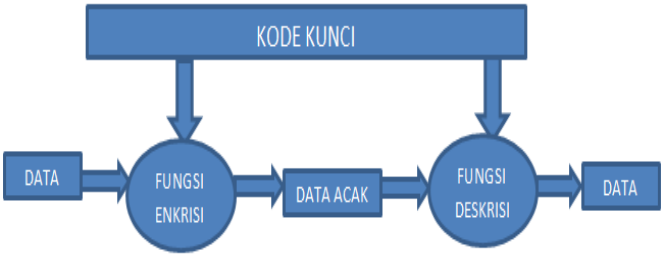


Algoritma enkripsi yang paling banyak dipakai di dunia adalah Data Encryption Standard (DES) yang diadopsi oleh NIST (Nasional Institue of Standard and Techonology) sebagai standar pengolahaan informasi Federal AS.Secara umunm, DES terbagi menjadi tiga kelompok saling berinteraksi satu dengan yang lainnya.

Berdasarkan tujuan dalam penelitian ini diuraikan dalam pokok-pokok yang ingin memahami proses penyandian dengan Data Encryption Standard (DES), mengetahui dan bagaimana merancang sebuah model algoritma DES untuk enkripsi data menggunakan *Graphica*l User Interface Matlab,dan mengetahui hasil algoritma DES pada keamanan pesan.

2.METODOLOGI PENELITIAN

Data dienkripsi dalam blok-blok 64 bit menggunkan kunci 56 bit, DES mentransformasikan input 64 bit dalam beberapa tahap enkripsi kedalam output 64 bit. Dengan demikian, DES termasuk dalam block chipher dengan tahapan pemakaian kunci yang sama untuk dekripsinya.



Gambar 1. Pemakaian Kunci Pada Des

Secara umum skema Data Encryption Standard (DES) memiliki dua fungsi input , yaitu:

a. Plaintext untuk dienkripsi dengan panjang 64 bit.
b. Kunci dengan panjang 56 bit

Proses initial permutasi (IP) Plaintext ada tiga:

1. Plaintext 64-Bit diproses di Initial Permutasi (IP) dan menyusun kembali bit untuk menghasilkan permutasi input.
2. Langkah untuk melakukan perulangan kata dari plaintext sebanyak 16 dengan meakukan fungsi permutasi subtitusi, yang mana output akhir dari hal tersebut berisi 64-Bit (fungsi dari plaintext dan kunci), masuk ke swap, dan menghasilkan preoutput.
3. Preoutput diproses, dan permutasi di-invers dari initial permutasi yang akan menghasilkan chiphertext 64-Bit.

Submitted: 1**5/11/2022**; Accepted: 25**/11/2022**; Published: 15**/12/2022**

JURNAL MEDIA INFORMATIKA [JUMIN]
Volume 4, Nomor 1, Desember 2022, Page 63-69
ISSN ISSN 2808-005X
Available Online at http://ejournal.sisfokomtek.org/index.php/jumin

Proses dari kunci 56-bit:

1). Kunci melawati fungsi dari permutasi.
2). Penggeseran kunci untuk memilih perulangan permutasi kunci sebanyak 16 kali yang menghasilkan subkey(Ki) yang di proses dengan kombinasi permutasi.
3). Perbedaan dari subkey(Ki) akan dilakukan penggeseran kunci yang menghasilkan kombinasi plaintext 64-bit dengan kunci 56-bit.
   a. initial permutasi (IP)
      initial permutasi (IP) dan inveres permutasi akan kita pelajari fungsinya pada permutasi dan inveres dengan mempertimbangkan 64-bit yang akan diberi input "M":
      M1 M2 M3 M4 M5 M6 M7 M8 M9 M10 M11 M12 M13 M14 M15 M16 M17 M18 M19 M20 M21 M22 M23 M24 M25 M26 M27 M28 M29 M30 M31 M32 M33 M34 M35 M36 M37 M38 M39 M40 M41 M42 M43 M44 M45 M46 M47 M48 M49 M50 M51 M52 M53 M54 M55 M56 M57 M58 M59 M60 M61 M62 M63 M64

      Mx adalah bilangan binary, kemudian dilakukan permutasi x = IP (M)

3. HASIL DAN PEMBAHASAN

Program ini digunakan untuk melakukan proses perubahan data dari bentuk asli ke bentuk baru (**enkripsi**) dan proses pengembalian data dari bentuk baru ke bentuk asli (**deskripsi**). Proses cypher digunakan menggunakan metode transposisi adalah dengan mengubah posisi karakter-karakternya dengan cara tertentu. Pada bagian ini akan digunakan 2 cara, yaitu:

1. Metode Zig-Zag Menggunakan N Baris.
   Pada metode ini, pada prinsipnya pesan yang akan dikirimkan ditulis per baris sebanyak baris yang ditentukan (sesuai dengan nilai **n**-nya). Sebelumnya karakter disusun dalam posisi baris dan kolom dengan urutan penyusunan:
   - Baris ke-1 dengan penyusunan karakter dengan menggunakan jeda ke-1 = 2*n dan jeda 2= 0.
   - Baris ke-2 dengan penyusunan karakter dengan menggunakan jeda ke-1 sebelummnya dikurangi 2 dan jeda ke-2 sebelumnya dengan 2.
   - Demikian seterusnya sampai dengan baris ke-**n**

     Ilustrasi:
     Plaintext = a1 a2 a3 a4 ... an
     Dikirim menggunakan metode zig-zag: n baris
     Pesan yang akan dikirimkan ditulis per baris dari pola:

     a1 an+3 dst

     a2 an+2

     ... an+1

     an

     sehingga cyphertext menjadi = a1 an+3 a2 an+2 ... dst

2. Metode Permutasi
   Prinsip metode ini adalah plaintext dibagi menjadi beberapa kolom sesuai dengan banyaknya permutasi yang akan digunakan, kemudian masing-masing kolom dikenai proses transpose sehingga menjadi baris

Submitted: 1**5/11/2022**; Accepted: 25**/11/2022**; Published: 15**/12/2022**

JURNAL MEDIA INFORMATIKA [JUMIN]
Volume 4, Nomor 1, Desember 2022, Page 63-69
ISSN ISSN 2808-005X
Available Online at http://ejournal.sisfokomtek.org/index.php/jumin

kemudian cyphertext dihasilkan dengan menyusun barisan karakter yang sesuai dengan urutan permutasi yang diinginkan.

Ilustrasi:

Permutasi yang digunakan misalnya a1 a2 a3 ... an

Maka plaintext dibagi menjadi n kolom

Kolom 1	kolom 2	kolom3	**...**	kolom n

Kemudian diubah menjadi baris

Kolom 1
Kolom 2
Kolom 3
...

a1	a2	a3	**...**	an

l;.dengan menggunakan MATLAB, maka permasalahan tersebut dapat diselesaikan:

Permasalahan 1:

Fungsi enchyper dan dechyper menggunakan proses transposisi dengan formula zig-zag.

a. Fungsi enchyper

Fungsi enchyper diberi nama ***function enkripsi***

```
function c=enkripsi (x,baris)
n=size(x,2);
jeda1=2*baris-2;
jeda2=0;
c=[];
for i=1:baris
    k=i;
    c=[c x(k)];
    while k<=n
        k=k+jeda1;
        if k<=n & jeda1~=0
            c=[c x (k)];
        end
    end
    jeda1=jeda1-2;
    jeda2=jeda2+2;
end
```

sebagai contohnya, function di atas dapat dijalankan

```
>> function c=dekrip(x,baris)
    n=size(x,2);
    jeda1=2*baris-2;
```


Submitted: 1**5/11/2022**; Accepted: 25**/11/2022**; Published: 15**/12/2022**

JURNAL MEDIA INFORMATIKA [JUMIN]
Volume 4, Nomor 1, Desember 2022, Page 63-69
ISSN ISSN 2808-005X
Available Online at http://ejournal.sisfokomtek.org/index.php/jumin

```
        jeda2=0;
        pos=0;
        for i=1:baris
            k=1;
            pos=pos+1;
            deciper(k)=[x(pos)];
            while k<=n
                k=k+jeda1;
                if k<=n & jeda1~=0
                                                    pos=pos+1;
                                                    deciper(k)={x(pos)];

                end
                k=k+jeda2;
                if k<=n & jeda2~=0
                                                    pos=pos+1;
                                                    deciper(k)=[x(pos)];

                end
            end
            jeda1=jeda1-2;
            jeda2=jeda2-2;
        end
        c=[];
        for i=1:n
            c=]c deciper (i)];
        end
>> baris = 5
Baris =

     5
>> c = enkripsi(x,baris)

c=
M UDAHARIAMHMMA
```

b. Fungsi Dechyper

Fungsi dechyper diberi nama ***function dekrip***

```
    function c=dekrip(x,baris)
    n=size(x,2);
    jeda1=2*baris-2;
    jeda2=0;
    pos=0;
    for i=1:baris
        k=1;
        pos=pos+1;
        deciper(k)=[x(pos)];
        while k<=n
            k=k+jeda1;
```


Submitted: 1**5/11/2022**; Accepted: 25**/11/2022**; Published: 15**/12/2022**

JURNAL MEDIA INFORMATIKA [JUMIN]
Volume 4, Nomor 1, Desember 2022, Page 63-69
ISSN ISSN 2808-005X
Available Online at http://ejournal.sisfokomtek.org/index.php/jumin

```
                    if k<=n & jeda1~=0
                        pos=pos+1;
                        deciper(k)={x(pos)];
                    end
                    k=k+jeda2;
                    if k<=n & jeda2~=0
                        pos=pos+1;
                        deciper(k)=[x(pos)];
                    end
                end
                jeda1=jeda1-2;
                jeda2=jeda2-2;
            end
            c=[];
            for i=1:n
                c=]c deciper (i)];
            end
```

jika function diatas dijalankan dengan input yang merupakan hasil enkripsi di atas maka diperoleh:

```
>> x= 'M UDAHARIAMHMMA'
x=
M UDAHARIAMHMMA

>>baris = 5
Baris =
     5
>>d=dekrip (x,baris)
d=

MUHAMMAD ARHAMI
```

4. KESIMPULAN

Kriptografi atau keamanan data bisa dipecahkan menggunakan dengan cara manual maupun dengan aplikasi komputer. Salah satunya dengan aplikasi komputer dengan pemograman Matlab. Teknik mengnkripsi sangat efektik karena dapat menjaga kerahasiaan data khususnya data dan juga memerlukan waktu yang sangat lama untuk dapat menemukan kunci yang benar. Algoritma DES banyak melakukan oprasi permutasi dan substitusi dalam bentuk matriks sehingga, software MATLAB membantu proses enkripsi dan dekripsi DES dilaksanakan dengan cepat, tepat, dan efisien.

REFERENCES

[1] R. Kusnadi and M. Jannah, "Penerapan Jaringan Syaraf Tiruan Untuk Memprediksi Jumlah Bagasi Lion Air dan Batik Air di Bandar Udara Kualanamu Dengan Metode Backpropagation," vol. 3, no. 3, pp. 293–302, 2021.

Submitted: 1**5/11/2022**; Accepted: 25**/11/2022**; Published: 15**/12/2022**

[2] A. Juanda and F. A. Sianturi, "Sistem Pendukung Keputusan Pemilihan Karyawan Tetap pada Trinity Teknologi Nusantara Dengan Metode Moora," *JIKOMSI [Jurnal Ilmu Komputer dan Sistem Informasi]*, vol. 3, no. 3, pp. 277–282, 2021.

[3] S. K. Sari and J. Manurung, "Implementasi Jaringan Syaraf Tiruan Untuk Memprediksi Tingkat Pemahaman Siswa Pada Mata Pelajaran Ujian Akhir Sekolah (UAS) Di SD Mis An Nur Sukamandi Menggunakan Metode Backpropragation," vol. 3, no. 3, pp. 283–292, 2021.

[4] R. P. Fhonna and A. R. Marzuki, "Sistem Informasi Absensi Pegawai Pada Biro Kominfo Kantor Bupati Kabupaten Aceh Utara Berbasis Web," *Jurnal Ilmu Komputer dan Sistem Informasi (JIKOMSI)*, vol. 3, no. 3, pp. 333–340, 2021.

[5] A. Lestari and B. Sinaga, "Implementasi Metode Backpropagation Memprediksi Tingkat Pemahaman Siswa Pada Mata Pelajaran Pendidikan Agama Islam (PAI) di MTs . S Ummi Lubuk Pakam," *Jurnal Ilmu Komputer dan Sistem Informasi*, vol. 3, no. 3, pp. 251–276, 2021.

[6] Y. Perwira, "Sistem Pendukung Keputusan Pemilihan Guru Berprestasi di SMK Negeri 1 Pantai Labu Dengan Menggunakan Metode Technique For Order Of Preference By Similarity To Ideal Solution (Topsis)," vol. 3, no. 3, pp. 229–250, 2021.

[7] W. Vrayuda and Y. Perwira, "Penerapan Metode Analytical Hierarchy Process (AHP) Dalam Rekomendasi Subsidi Listrik (Studi Kasus: Desa Pulau Tagor Baru Kec. Galang)," *... Komputer dan Sistem Informasi ...*, vol. 3, no. 3, pp. 202–227, 2021, [Online]. Available: http://ejournal.sisfokomtek.org/index.php/jikom/article/view/117

[8] M. Siahaan and J. Manurung, "Perancangan Aplikasi Penyandian Teks Menggunakan Algoritma Triple DES," *Jurnal Ilmu Komputer dan Sistem ...*, vol. 3, no. 3, pp. 197–201, 2021, [Online]. Available: http://ejournal.sisfokomtek.org/index.php/jikom/article/view/116

[9] S. Dengan, C. Algoritma, and W. Hidayati, "Data Mining Penentuan Tenaga Perawat Di RSUD Sultan," vol. 1, no. 2, pp. 1–7, 2018.

[10] E. Febrivani and R. Winanjaya, "Penerapan Data Mining Asosiasi Pada Persediaan Obat," vol. 3, no. 3, pp. 354–365, 2021.

[11] G. Alfamart, D. Sartika, B. Ginting, M. Novaliani, and B. Sembiring, "Analisis Monte Carlo dalam Memprediksi Jumlah Penambahan," vol. 3, no. 3, pp. 348–353, 2021.

[12] I. P. Kusumawijaya, "Aplikasi Sistem Pakar Kerusakan Personal Computer Menggunakan Metode Certainty Factor," *ICIT Journal*, vol. 6, no. 2, pp. 183–194, 2020, doi: 10.33050/icit.v6i2.1115.

[13] G. Alfamart, D. Sartika, B. Ginting, M. Novaliani, and B. Sembiring, "Analisis Monte Carlo dalam Memprediksi Jumlah Penambahan," vol. 3, no. 3, pp. 348–353, 2021.

[14] A. M. Adli Abdillah, "Model Simulasi Antrian Matchmaking Dalam Permainan Massive Online Battle Arena Menggunakan Algoritma K-Nearest Neighbor," *Jikomsi*, vol. 3, no. 3, pp. 314–326, 2021.

[15] A. Sinaga, "Implementasi Algoritma Brute Force Dalam Pencarian Menu Pada Aplikasi Pemesanan Coffee (Studi Kasus : Tanamera Coffee)," vol. 3, no. 3, pp. 303–313, 2021.

Submitted: 1**5/11/2022**; Accepted: 25**/11/2022**; Published: 15**/12/2022**