Nuniek Fahriani

Penerapan Kriptografi DES Untuk Keamanan Data Teks Pada File PDF Menggunakan Bahasa Pemrograman Phyton

Quick Submit
Quick Submit
Universitas Muhammadiyah Surabaya

Document Details

Submission ID
trn:oid:::1:3103032986

Submission Date
Dec 5, 2024, 1:51 PM GMT+7

Download Date
Dec 5, 2024, 1:52 PM GMT+7

File Name
Jurnal_Nuniek.docx

File Size
760.1 KB

11 Pages

2,804 Words

16,545 Characters

19% Overall Similarity

The combined total of all matches, including overlapping sources, for each database.

Top Sources

0% Internet sources
19% Publications
0% Submitted works (Student Papers)

Integrity Flags

0 Integrity Flags for Review

No suspicious text manipulations found.

Our system's algorithms look deeply at a document for any inconsistencies that would set it apart from a normal submission. If we notice something strange, we flag it for you to review.

A Flag is not necessarily an indicator of a problem. However, we'd recommend you focus your attention there for further review.

Top Sources

0% Internet sources
19% Publications
0% Submitted works (Student Papers)

Top Sources

The sources with the highest number of matches within the submission. Overlapping sources will not be displayed.

1 Publication
Seminar Nasional Multidisiplin Ilmu 2017, Sylvia Vianty Ranita, Zubaidah Hanum. ... 4%

2 Publication
Priyansh Kumar Dubey, Ajay Jangid, B. R. Chandavarkar. "An Interdependency be... 2%

3 Publication
Obaida M. Al-hazaimeh, Moyawiah A. Al-Shannaq, Mohammed J. Bawaneh, Khalid... 2%

4 Publication
Joko Susanto , Ilhamsyah , Tedy Rismawan. "APLIKASI ENKRIPSI DAN DEKRIPSI U... 2%

5 Publication
Edi Jaya Kusuma, Oktaviana Rena Indriani, Christy Atika Sari, Eko Hari Rachmawa... 1%

6 Publication
"Proceedings of International Conference on Smart Computing and Cyber Securit... 1%

7 Publication
Muhammad Hasan Thoriq Almuwaffaq Thoriq, Asep Id Hadiana Asep, Puspita Nu... 1%

8 Publication
Wahyu Ariandi, Susi Widyastuti, Lutfi Haris. "Implementasi Block Cipher Electroni... 1%

9 Publication
"Emerging Technologies in Data Mining and Information Security", Springer Scie... 1%

10 Publication
Yoga Pratama, Tata Sutabri. "Analisis Kriptografi Algoritma Blowfish pada Keama... 1%

11 Publication
Zil Fadli, Taslim Taslim. "IMPLEMENTASI PENGAMANAN BASIS DATA DENGAN TEK-... 1%

12 Publication

Pachi Pulusu Chanakya, Balaram Khamari, Manmath Lama, Arun Sai Kumar Peke... 1%

13 Publication

Anang Widiantoro, Dwi Songgo Panggayudi. "Design and Development of Sun En... 0%

14 Publication

Ega pratama. "Implementasi Algoritma Elgamal dan kode HILL Untuk Keamanan ... 0%

15 Publication

Ela Mahudi, Yosef Cahyo Setianto Poernomo, Ahmad Ridwan. "STUDI ANALISA DA... 0%

16 Publication

Satria Agust, Gatot Subroto, Muhammad Candra. "Pentingnya Stepping the 5 Stai... 0%

17 Publication

"Communication and Intelligent Systems", Springer Science and Business Media ... 0%

18 Publication

Made Hanindia Prami Swari, Hendra Maulana, I Putu Susila Handika, I Kadek Susi... 0%

19 Publication

Moranain Mungkin, Habib Satria, Zulkifli Bahri, Ahmad Ridwan. "Testing the Relia... 0%

20 Publication

Muhammad Efendi, Volvo Sihombing, Sahat Parulian. "Implementation and Use o... 0%

21 Publication

P. Gamba, F. Dell'Acqua, G. Lisini. "Improving Urban Road Extraction in High-Reso... 0%

22 Publication

Novelius Buulolo, Anita Sindar. "Analisis dan Perancangan Keamanan Data Teks ... 0%

JURNAL XXXXX

Penerapan Kriptografi DES Untuk Keamanan Data Teks Pada File PDF Menggunakan Bahasa Pemrograman Phyton

Nuniek Fahriani
Informatika, Fakultas Teknik, Universitas Muhammadiyah Surabaya,
Jl. Sutorejo No. 59 Surabaya
e-mail: nuniekfahriani@ft.um-surabaya.ac.id,

Diajukan:……; Direvisi: ...; Diterima: ...

Abstrak

Pada seni kriptografi banyak teknik enkripsi yang bisa dmanfaatkan, diantaranya adalah teknik "Data Encryption Standard (DES)" yang tergolong jenis cipher blok yang menggunakan kunci simetris yang dapat mengenkripsi pesan sebanyak 64 bit. Terdapat tiga tahapan operasi untuk teknik data encryption standard-DES, tahap satu dengan menjalankan perubahan letak atau permutasi, selanjutnya dilakukan rotasi, dan langkah ketiga adalah melakukan fungsi substitusi. Pada penelitian ini bahasa permograman yang digunakan adalah bahasa python. Objek yang menjadi sebagai plainteks (teks asli) adalah file dokumen PDF (portable document format). Program python yang dijalankan dapat melakukan enkripsi sekaligus melakukan kompresi ukuran PDF (portable document format) menjadi lebih kecil. Dengan hasil file plainteks awal sebesar 7.55 KB (7.732 bytes). Sesudah dilakukan enkripsi menjadi 1.99 KB (2.039 bytes). Selanjutnya adalah proses dekripsi mengembalikan lagi ke dalam teks yang bisa dibaca dengan ukuran file sebesar 1.30 KB (1.336 bytes).

Kata kunci— *DES, Kriptografi, Enkripsi, Dekripsi, PDF, Phyton*

Abstract

In cryptography, there are many encryption techniques that can be utilized, including the "Data Encryption Standard (DES)" technique which is classified as a block cipher type that uses a symmetric key that can encrypt messages as much as 64 bits. There are three stages of operation for the standard-DES data encryption technique, the first stage is by changing the location or permutation, then the rotation is carried out, and the third step is performing the substitution function. In this study the programming language used is Python. The object used as plaintext (original text) is a PDF (portable document format) document file. The python program that is run can encrypt as well as compress the size of the PDF (portable document format) to be smaller. With the resulting initial plaintext file of 7.55 KB (7,732 bytes). After encryption is done, it becomes 1.99 KB (2,039 bytes). Next is the decryption process to return it to readable text with a file size of 1.30 KB (1,336 bytes).

Keywords— *DES, Kriptography, Enkription, Dekription, PDF, Phyton*

1. Pendahuluan

Pada masa sekarang perkembangan teknologi bergerak sangat cepat, sehingga membuat suatu informasi dapat diterima atau dikirim dengan sangat cepat. Bahkan teknologi berbasis IoT "(*Internet of Thing*)" menjadi salah satu konsep yang cukup digunakan untuk mentransfer data melalui jaringan yang berkomunikasi dengan berbagai perangkat keras dan perangkat lunak [1]. Dengan adanya berbagai media untuk saling bertukar data atau informasi, dan masa sekarang teknologi informasi merupakan bagian yang sangat penting dalam kehidupan manusia. Namun, dengan kebebasan bertukar data pada periode ini, keamanan data juga menjadi isu yang sangat penting yang harus diperhatikan, apalagi jika data atau informasi yang sedang dikirimkan ke orang lain merupakan data yang sangat rahasia, dan dikirim menggunakan jaringan komputer yang terhubung ke jaringan luas (internet). Hal tersebut menjadi masalah jika ada yang melakukan akses ilegal terhadap data dan mengambil semua data atau informasi yang sedang dikirim. Keamanan didalam sistem informasi sangat dibutuhkan. Jenis data dapat berupa file dokumen, file video, file audio maupun file gambar [2].

turnitin Page 5 of 15 - Integrity Submission Submission ID trn:oid:::1:3103032986

Diantara ilmu yang mempelajari tentang keamanan data, yaitu kriptografi [3]. Banyak algoritma enkripsi yang dapat digunakan untuk enkripsi, salah satu nya adalah algoritma "*Data Encryption Standard* (DES)" [4] [5] [6]. DES dikembangkan 1973 oleh "*National Institute of Standards and Technology*-NIST" [7]. Awalnya, algoritma *Data Encryption Standard* (DES) mendapat kritikan keras karena dua alasan. Yang pertama, karena DES memiliki panjang kunci yang pendek (56 bit) yang membuat suatu *cipher* menjadi mudah untuk dipecahkan menggunakan metode *brute-force*. Kedua, kekhawatiran juga terjadi kepada rahasia desain dibelakang mekanisme internal *Data Encryption Standard* (DES). Pada penelitian ini, fokus proses kriptografi untuk keamanan pada data file PDF (*portable document format*).

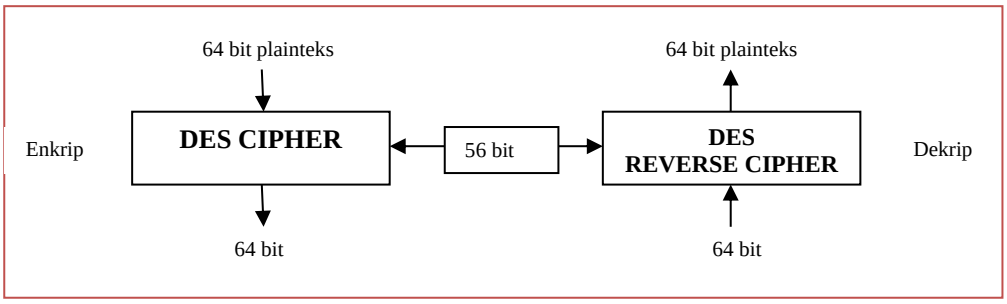
Proses algoritma *Data Encryption Standard* (DES) adalah teks yang awalnya dapat dibaca dengan mudah oleh siapapun bisa menjadi tulisan yang tidak dapat dibaca tanpa menggunakan kunci enkripsi yang telah dibuat oleh pembuat enkripsi tersebut. Menggunakan algoritma cipher blok dengan enkripsi kunci simetris. Ada tiga tahapan yang dilakukan pada proses algoritma *Data Encryption Standard* (DES): fase kunci, fase mengenkripsi perhitungan 64 bit, fase kebalikan dengan mendekripsikan perhitungan 64 bit [8] [9]. Terdapat penelitian yang dibuat oleh Gunawan Putrodjojo, Julhan H. Purba, dan Junawano Candra [4]. Dalam penelitian tersebut, mereka menggunakan algoritma DES untuk enkripsi file txt. Aplikasi dibuat dengan bahasa pemrograman Visual Studio 2015 menggunakan *compiler Visual Studio Basic*. Dari apa yang ditulis menyimpulkan bahwa keamanan informasi atau teks dapat ditingkatkan dengan menggunakan proses enkripsi – dekripsi dengan teknik DES. Algoritma kriptografi (kripto sistem) memiliki cara kerja menyandikan suatu pesan-plainteks (teks asli) menjadi suatu kode rahasia berupa *cipherteks* [10].

2. Metode Penelitian

Metode untuk keamanan data file PDF (*portable document format*) dengan menggunakan algoritma *Data Encryption Standard* (DES) diterapkan menggunakan bahasa pemrograman *phyton*. Algoritma simetris di kriptografi yang paling banyak digunakan untuk melakukan proses enkripsi data atau informasi diantaranya yaitu teknik DES yang masuk kategori jenis *blockcipher* dengan kunci simetris yang dapat mengenkripsi pesan sebanyak 64 bit. Kunci simetri berarti hanya 1 (satu) *key* yang dipakai untuk proses enkripsi maupun dekripsi. Terdapat beberapa elemen pembangun dari algoritma *Data Encryption Standard* (DES) ini, yaitu aritmatika modular, jaringan feistel, S-Box, jumlah iterasi DES, dan panjang kunci *Data Encryption Standard* (DES) [11].

2.1 Tahapan Operasi DES

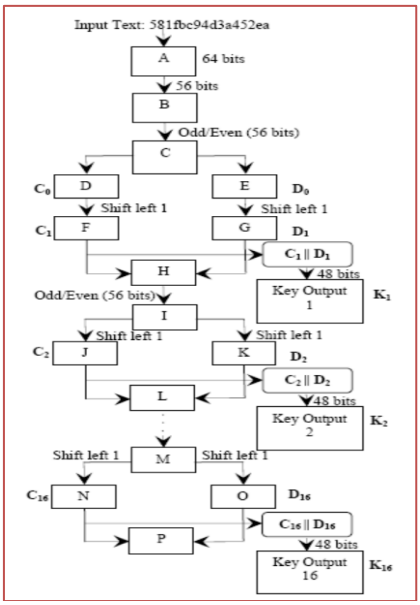
Terdapat tiga tahapan operasi pada algoritma *Data Encryption Standard* (DES), tahap awal dengan melalui permutasi selanjutnya dilakukan rotasi, dan langkah ketiga adalah melakukan fungsi substitusi. Diantara posisi awal dan akhir proses transposisi, algoritma ini menjalankan 16 iterasi dari sebuah fungsi [12]. Teknik enkrip dan dekrip dari algoritma *Data Encryption Standard* (DES) digambarkan dalam gambar 1 dibawah ini :



Gambar 1 Enkripsi dan Dekripsi Pola Teknik DES

2. 2 Generate Key DES

Algoritma DES hanya menggunakan 56 bit dari total 64 bit untuk tujuan konversi dan bit sisanya digunakan untuk pengecekan keseimbangan pada proses datanya. DES bekerja dengan tipe besaran 64-bit [13] penjelasan dapat diamati proses *generate key* pada gambar 2 dibawah :



Gambar 2 Generate Key *Data Encryption Standard* (DES) [14]

Data Encryption Standard (DES) mengenkrip 64-bit teks aslinya dan menjadikan 64-bit teks yang tidak dapat dibaca, melalui *key* 56-bit didalam yang dibangkitkan dari *key* diluar mencapai 64-bit. Sedangkan tahapan untuk melakukan *generate key*, kunci diluar yang menjadi proses untuk menghasilkan 16 kunci didalam yakni : kunci diluar dengan 64-bit disubstitusikan oleh matriks permutasi kompresi PC-1. Dengan ketentuan, permutasi per bit ke-8 (*parity bit*) dari 8 *byte* dilewati. Hasilnya berubah 56-bit, selanjutnya akan berbagi bagian, yakni *left* (C0) dan *right* (D0) dengan panjang masing-masing 28 bit. Bit kiri dan kanan bergeser pada setiap iterasinya satu atau dua bit. Pola enkripsinya, bit digeser ke kiri (*left shift*). Pola dekripsinya, bit digeser ke kanan (*right shift*). Ci akan disatukan dan disubstitusikan dengan permutasi matriks PC-2, dan berubah 48-bit. Prosedur itu diulang 16 kali. Sehingga proses enkripsi *Data Encryption Standard* (DES) dapat mempersulit peretas untuk melakukan dekripsi data yang sedang diamankan dengan teknik DES [15] [16].

2. 3 Skema Global DES

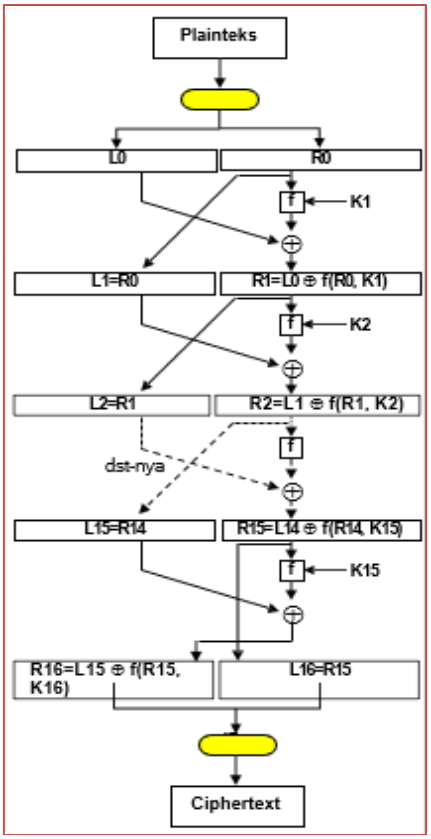
Terdapat kerangka global dalam teknik keamanan data dengan DES dan lebih jelasnya di tabel dibawah ini :

Tabel 1 Kerangka DES

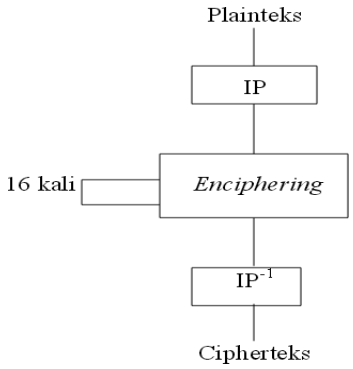
Kerangka	Penjelasan
1	Blok plainteks 64 bit yang akan dienkripsi melakukan proses perubahan dengan perubahan awal, dimana setiap bit nya dipindah ke posisi bit yang baru. Dengan target terjadi pengacakan teks asli sehingga rangkaian bit akan berubah**.**
2	Blok 64 bit yang telah di permutasi terbagi kedalam dua blok panjang setiap blok 32 bit, disebut dengan *left* dan *right*. Nilai awal dari kiri dan kanan blok adalah dilambangkan dengan L0 dan R0. Di *enciphering* sebanyak enam belas iterasi dengan kunci internal berbeda.
3	terdapat 16 iterasi pada blok kiri dan kanan yang dijalankan. Dilakukan permutasi dengan matrik proses kebalikan (IP^{-1}) menjadi blok cipher.
4	Tiap iterasi I, blok R dimana inputan perubahan dinamakan f. di fungsi-f, blok R dikombinasikan bersama *key* internal Ki. luaran fungsi-f di XOR kan dengan blok L dari blok R sebelumnya. Kunci internal sama dengan kunci setiap iterasi.
5	Satu iterasi *Data Encryption Standard* (DES) membentuk jaringan feistel
6	terdapat 16 iterasi pada proses enkripsi, sehingga membutuhkan enam belas *key* internal : K1 sampai K16.

7	*Key* internal difungsikan" sebelum atau bersamaan dengan proses enkripsi".
8	*Key* internal difungsikan dari "kunci eksternal (oleh pengguna) yang panjangnya 64 bit (8 karakter)".

Dan berikut adalah gambar dari skema pembagian dua blok kiri dan kanan serta gambar dari proses *enciphering* DES. digambarkan gambar 3 dan gambar 4, yaitu :



Gambar 3 Skema Pembagian dua blok kiri dan kanan



Gambar 4 Proses *Enciphering Data Encryption Standard* (DES)

2. 4 Rumus Matematis pada 1 iterasi

Simbol matematis untuk satu putaran *Data Encryption Standard* (DES) dapat diterapkan dengan kondisi :

$$L_i = R_{i-1} \quad (1)$$

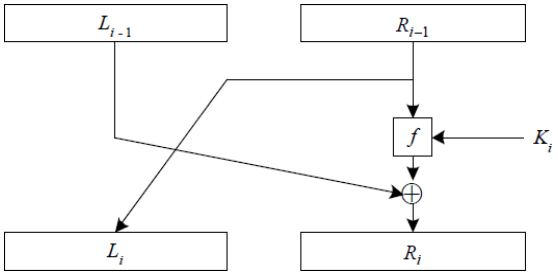
$$R_i = L_{i-1} \oplus f(R_{i-1}, K_i) \quad (2)$$

Sebagai bahan kajian, jika "(***L16, R16)***" adalah bagian keluaran putaran ke-enam belas, jika (***R16, L16***) adalah bagian sebelum cipherteks (*pre-ciphertext)* dari *enciphering*. *Cipherteks* orisinil didapat dengan melakukan perubahan awal balikan, IP^{-1}, terhadap blok pra-cipherteks.

3. Hasil Dan Pembahasan

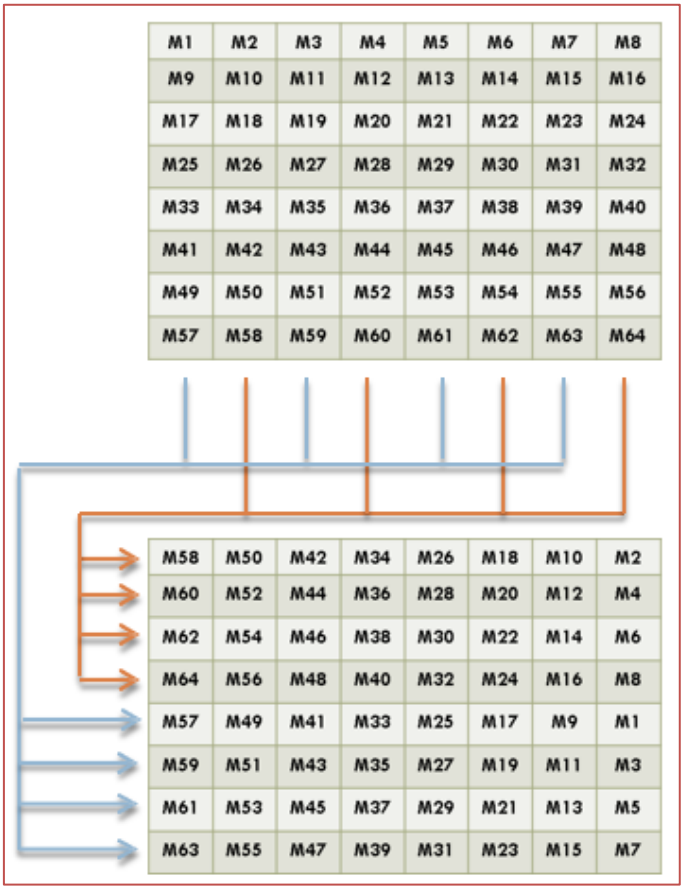
Pada proses hasil untuk implementasi kriptografi algoritma *Data Encryption Standard* (DES) menggunakan bahasa permograman *python*. Objek yang menjadi sebagai plainteks (teks asli) adalah file dokumen PDF (*portable document format*). Berikut adalah mekanisme hasil penerapan *Data Encryption Standard* (DES) tersebut :

A. Membentuk jaringan feistel : dimana pola satu putaran *Data Encryption Standard* (DES) nya pada gambar 5 dibawah ini :



Gambar 5 Satu putaran *Data Encryption Standard* (DES) membentuk jaringan feistel

B. Proses perubahan awal (*initial permutation*) : pengacakan dilakukan dengan menggunakan matrik permutasi awal, "misal M adalah masukan bilangan binary 64 bit. Jika X adalah bilangan binary, permutasi X = IP(M)", maka berikut adalah gambar penjelasannya pada gambar 6 :



Gambar 6 Proses permutasi awal

C. Tabel IP : Berikut adalah tabel IP pada gambar 7dibawah ini :

1	2	3	4	5	6	7	8
58	50	42	34	26	18	10	2
9	10	11	12	13	14	15	16
60	52	44	36	28	20	12	4
17	18	19	20	21	22	23	24
62	54	46	38	30	22	14	6
25	26	27	28	29	30	31	32
64	56	48	40	32	24	16	8
33	34	35	36	37	38	39	40
57	49	41	33	25	17	9	1
41	42	43	44	45	46	47	48
59	51	43	35	27	19	11	3
49	50	51	52	53	54	55	56
61	53	45	37	29	21	13	5
57	58	59	60	61	62	63	64
63	55	47	39	31	23	15	7

Gambar 7 Tabel IP

D. Tabel *invers initial permutation* (IP^{-1}) : Berikut adalah tabel IP pada gambar 8 dibawah ini :

Input	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Output	40	8	48	16	56	24	64	32	39	7	47	15	55	23	63	31
Input	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32
Output	38	6	46	14	54	22	62	30	37	5	45	13	53	21	61	29
Input	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48
Output	36	4	44	12	52	20	60	28	35	3	43	11	51	19	59	27
Input	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63	64
Output	34	2	42	10	50	18	58	26	33	1	41	9	49	17	57	25

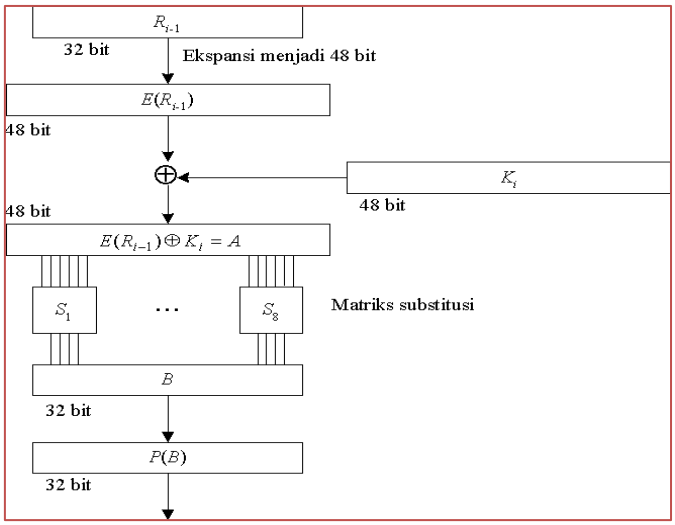
Gambar 8 Tabel invers initial permutation (IP^{-1})

E. Pefungsian kunci internal : Dalam tahap-permutasi ini, “tiap bit kedelapan (*parity bit*) dari delapan byte kunci diabaikan. Hasil permutasinya sepanjang 56 bit, sehingga kunci panjang kunci *Data Encryption Standard* (DES)=56 bit. Yang selanjutnya 56 bit tersebut dibagi menjadi dua bagian kiri dan kanan yang masing-masing memiliki panjang 28 bit disimpan sebagai **C0** dan **D0”**. Berikut adalah gambar tabel yang digunakan sebagai *Data Encryption Standard* (DES) *schedule key* pada gambar 9 sebagai tabel permutasi pilihan 1.(PC-1). PC adalah permutasi *choice*. Berikut adalah gambarnya :

Input	1	2	3	4	5	6	7	8	9	10	11	12	13	14
Output	57	49	41	33	25	17	9	1	58	50	42	34	26	18
Input	15	16	17	18	19	20	21	22	23	24	25	26	27	28
Output	10	2	59	51	43	35	27	19	11	3	60	52	44	36
Input	29	30	31	32	33	34	35	36	37	38	39	40	41	42
Output	63	55	47	35	31	23	15	7	62	54	47	38	30	22
Input	43	44	45	46	47	48	49	50	51	52	53	54	55	56
Output	14	6	61	53	45	3	29	21	15	5	28	20	12	4

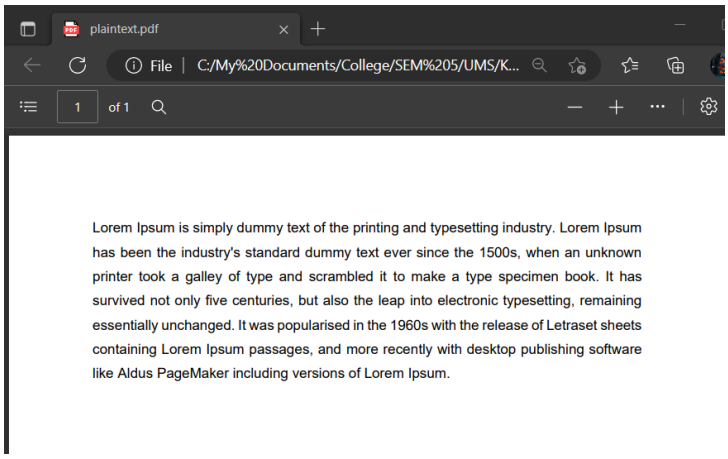
Gambar 9 Tabel permutasi PC-1

F. **"C0** berisi bit-bit dari K pada posisi :
57, 49, 41, 33, 25, 17, 9, 1, 58, 50, 42, 34, 26, 18, 10, 2, 59, 51, 43, 35, 27, 19, 11, 3, 60, 52, 44, 36".
G. **"D0** berisi bit-bit dari K pada posisi :
63, 55, 47, 39, 31, 23, 15, 7, 62, 54, 46, 38, 30, 22, 14, 6, 61, 53, 45, 37, 29, 21, 13, 5, 28, 20, 12, 4".
H. Selanjutnya "kedua bagian digeser ke kiri (*left shift*) sepanjang 1 atau 2 bit tergantung tiap putaran. Operasi pergeseran bersifat *wrapping* atau *round shift"*.
I. *Enciphering* : mengalami 16 kali iterasi *enciphering*.
J. Diagram komputasi fungsi *f* : terdapat pada gambar 10 yaitu :



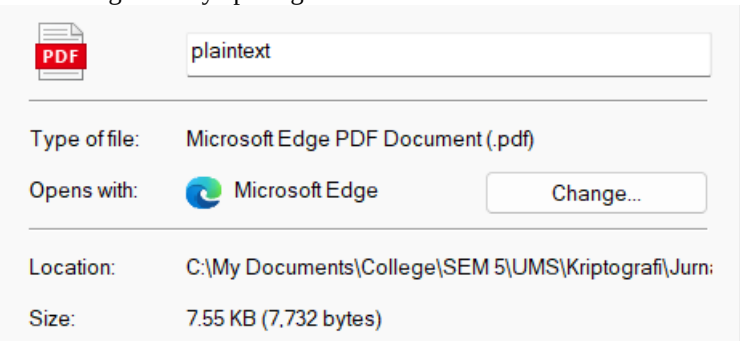
Gambar 10 Komputasi fungsi *f*

K. **"E** adalah fungsi ekspansi yang memperluas blok 32 bit R_{i-1} menjadi 48 bit. Fungsi dari ekspansi direalisasikan dengan matrik permutasi ekspansi".
L. Hasil ekpansi : yaitu $E(R_{i-1})$ di-XOR-kan dengan K_i menghasilkan vektor A 48-bit : $\mathbf{E(R_{i-1})}$ Å $\mathbf{K_i = A}$
M. "Vektor A dikelompokkan menjadi 8 kelompok, masing-masing 6 bit, dan menjadi masukan bagi proses substitusi".
N. "Ada 8 matriks substitusi, masing-masing dinyatakan dengan **Kotak-S"**.
O. **"Kotak–S** menerima masukan 6 bit dan memberikan keluaran 4 bit".
P. "Keluaran proses substitusi adalah vektor B yang panjangnya 48 bit. Vektor B menjadi masukan untuk proses permutasi. Tujuan permutasi adalah untuk mengacak hasil proses substitusi kotak-S".
Q. "Permutasi dilakukan dengan menggunakan matriks permutasi **P** (**P-box**)".
R. Setelah file PDF (portable document format) siap, file tersebut akan diproses oleh program python dan menggunakan library *Data Encryption Standard* (DES) untuk melakukan enkripsi dan dekripsi. Berikut adalah gambar plainteks (teks asli) dari file PDF (*portable document format*) pada gambar 11 :



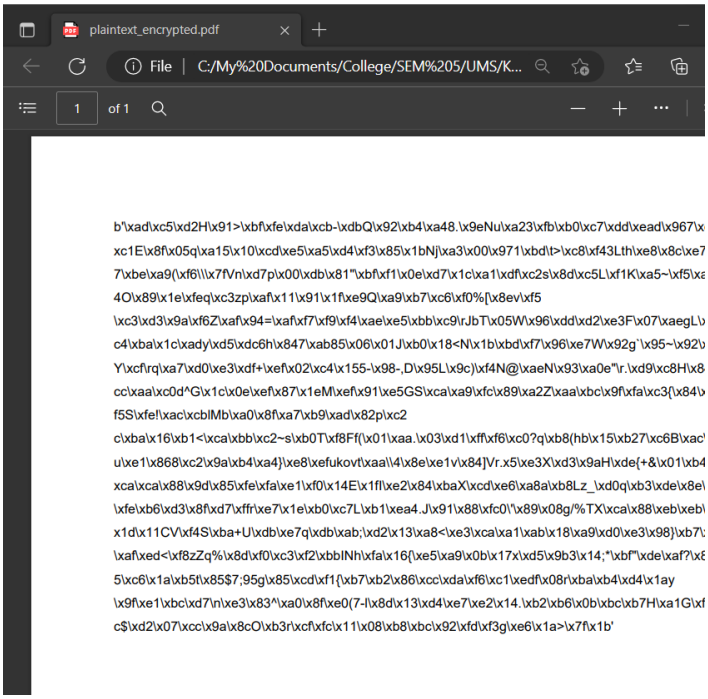
Gambar 11 Plainteks PDF (*portable document format*)

S. Spesifikasi file PDF (*portable document format*) sebelum dilakukan enkripsi adalah 7.55 KB (7.732 *bytes*). Dan berikut adalah gambarnya pada gambar 12 :



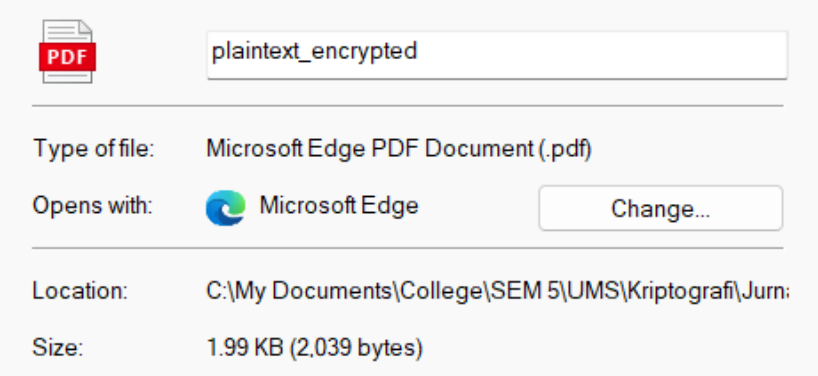
Gambar 12 Spesifikasi sebelum dilakukan enkripsi

T. Hasil *cipherteks*. Terlihat pada gambar 13 :



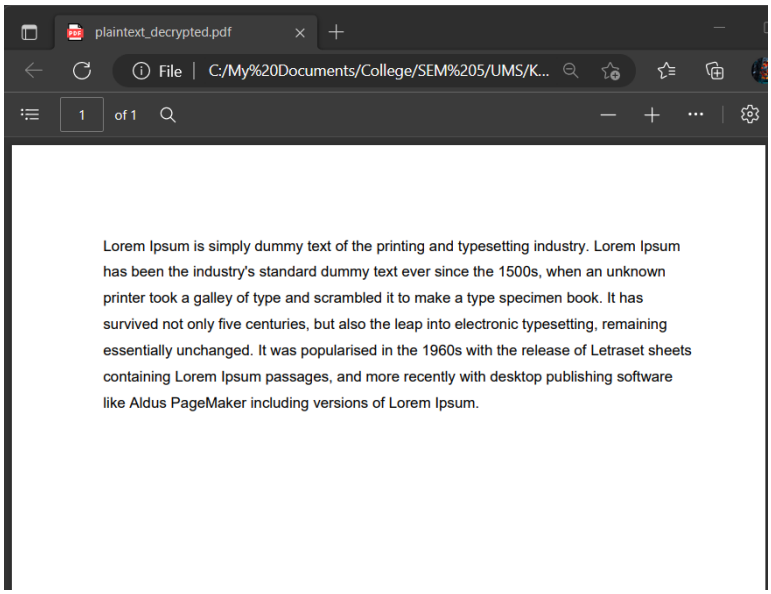
Gambar 13 Hasil cipherteks file PDF (*portable document format*)

U. Spesifikasi file PDF (*portable document format*) sesudah dilakukan enkripsi menjadi 1.99 KB (2.039 *bytes*). Dan berikut adalah gambarnya pada gambar 14 :



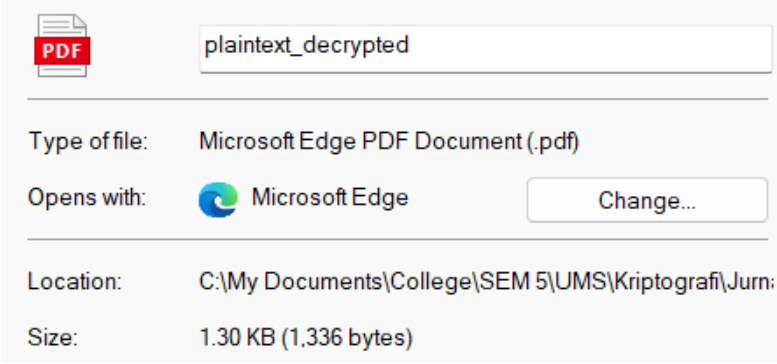
Gambar 15 Spesifikasi file PDF (*portable document format*) yang sudah di enkripsi

V. Proses dekripsi : program akan menulis kembali isi dari plainteks yang sebelumnya di enkripsi dengan membuat file PDF (*portable document format*) yang baru. Dari hasil dekripsi file yang telah terenkripsi tersebut dihasilkan file plainteks yang dapat dibaca kembali. Hasil dari dekripsi dapat dilihat pada gambar 16 :



Gambar 16 Plainteks hasil dekripsi

W. Spesifikasi file PDF (*portable document format*) dari proses dekripsi adalah 1.30 KB (1.336 *bytes*). Dan berikut adalah gambarnya pada gambar 17 :



Gambar 17 Spesifikasi file PDF (*portable document format*) yang sudah di dekripsi

X. Penjelasan hasil dari proses file PDF (*portable document format*) menggunakan *Data Encryption Standard* (DES) dengan program *phyton* dapat dilihat pada tabel 2 dibawah ini :

Tabel 2. Hasil Proses File PDF

Nama File	Ukuran
Plaintext.pdf	7.55KB
Plaintext_encrypted.pdf	1.99KB
Plaintext_decrypted.pdf	1.3 KB

4. Kesimpulan

Dari hasil percobaan melakukan enkripsi file text menggunakan metode algoritma *Data Encryption Standard* (DES) dapat disimpulkan bahwa:

- Dari hasil ujicoba enkripsi yang dilakukan dengan menggunakan bahasa pemrograman *phyton* terhadap file pdf terlihat cukup aman, karena seluruh isi text menjadi tidak bisa terbaca, dan memerlukan kunci dekripsi agar dapat melakukan dekripsi dan file text tersebut dapat digunakan kembali.
- Bahasa pemrograman *python* yang dijalankan dapat melakukan enkripsi sekaligus melakukan kompresi ukuran PDF (*portable document format*) menjadi lebih kecil.
- Dalam penelitian ini belum dilakukan ujicoba ketika didalam file PDF (*portable document format*) terdapat gambar, grafik, data. Dalam hal ini hanya berupa tulisan teks saja.

5. Saran

Saran-saran untuk untuk penelitian lebih lanjut adalah :

- Penerapan kriptografi algoritma *Data Encryption Standard* (DES) dapat dikombinasikan dengan kriptografi algoritma lainnya, khususnya dalam proses enkripsi atau ciphering.
- Menggunakan bahasa phyton yang juga dapat mengenkripsi data dokumen berbasis citra.

Daftar Pustaka

[1] N. Fahriani and I. Kurniawati, "Keamanan Data Pasien dengan Algoritma Blowfish pada HOTSPODT," *J-COSINE*, vol. 5, no. 2, pp. 140-148, 2021.

[2] N. Fahriani and H. Rosyid, "IMPLEMENTASI TEKNIK ENKRIPSI DAN DEKRIPSI DI FILE VIDEO MENGGUNAKAN ALGORITMA BLOWFISH," *Jurnal Teknologi Informasi dan Ilmu Komputer (JTIIK)*, vol. 6, no. 6, pp. 697-702, Desember 2019.

[3] N. D. P. Siregar, Azanuddin and W. R. Maya, "IMPLEMENTASI KRIPTOGRAFI PENGAMANAN DATA NILAI SISWA PADA SD NEGERI 064979 MEDAN DENGAN MENGGUNAKAN ALGORITMA DES," *Jurnal CyberTech*, vol. 4, no. 6, 2021.

[4] G. Putrodjojo, J. H. Purba and J. Candra, "Aplikasi Algoritma Des (Data Encryption Standard) untuk Pengaman Data," *Creative Communication and Innovative Technology Journal*, vol. 10, pp. 62-74, 2017.

[5] A. Vuppala, R. S. Roshan, S. Nawaz and J. Ravindra, "An Efficient Optimization and Secured Triple Data Encryption Standard Using Enhanced Key Scheduling Algorithm," *Procedia Computer Science* , pp. 1054-1063, 2020.

[6] Ariska and Wahyuddin, "PENERAPAN KRIPTOGRAFI MENGGUNAKAN ALGORITMA DES (DATA ENCRYPTION STANDARD)," *JURNAL SINTAKS LOGIKA (JSilog)*, vol. 2, no. 2, pp. 9-19, Mei 2022.

[7] A. Siswanto, A. Syukur and I. Husna, "PERBANDINGAN METODE DATA ENCRYPTION STANDARD (DES) DAN ADVANCED ENCRYPTION STANDARD (AES) PADA STEGANOGRAFI FILE CITRA," in *Seminar Nasional Teknologi Informasi Dan Komunikasi (SEMNASTIK) X*, Palembang-Indonesia, Oktober 2018.

[8] S. Hanadwiputra, "IMPLEMENTASI ENKRIPSI DALAM PENGAMANAN FILE DATA KARYAWANDENGAN METODE ALGORITMA DES (DATA ENCRYPTION STANDARD) PADA CV. SINERGI INFORMASI GLOBAL," *Jurnal "Gema Kampus"*, vol. 13, no. 2, pp. 61-69, 2018.

[9] D. Adhar, "IMPLEMENTASI ALGORITMA DES (DATA ENCRYPTION STANDARD) PADA ENKRIPSI DAN DESKRIPSI SMS BERBASIS ANDROID," *Jurnal Teknik Informatika Kaputama (JTIK)*, vol. 3, no. 2, pp. 53-60, 2019.

[10] C. Irawan and A. Winarno, "KOMBINASI ALGORITMA KRIPTOGARAFI AES DAN DES UNTUK ENKRIPSI FILE DOKUMEN PROPOSAL," in *Semnas Multi Disiplin Ilmu (SENDI_U)*, Semarang, 2020.

[11] T. hagras, D. Salama and H. Youness, "Anti-attacks encryption algorithm based on DNA computing and data encryption standard," *Alexandria Engineering Journal*, pp. 11651-11662, May 2022.

[12] G. Sharma, Implementation and analysis of DES algorithm, LAP LAMBERT Academic Publishing, 2014.

[13] T. Hagras, D. Salama and H. Youness, "Anti-attacks encryption algorithm based on DNA computing and data encryption standard," *Alexandria Engineering Journal*, pp. 11651-11662, 2022.

[14] N. Kaur and S. Sodhi, "Data Encryption Standard Algorithm (DES) for Secure Data Transmission," *IJCA Proceedings on International Conference on Advances in Emerging Technology*, vol. ICAET 2016, pp. 31-37, 2016.

[15] A. Vuppala, R. S. Roshan, S. Nawaz and J. Ravindra, "An Efficient Optimization and Secured Triple Data Encryption Standard Using Enhanced Key Scheduling Algorithm," in *Third International Conference on Computing and Network Communications (CoCoNet'19)*, 2020.

[16] C.-h. Liu, J.-s. Ji and Z.-l. Liu, "Implementation of DES Encryption Arithmetic based on FPGA," in *AASRI Conference on Parallel and Distributed Computing Systems*, 2013.