Jurnal Dinamika Informatika
Volume 14, No 1, Maret 2025
ISSN 1978-1660 : 78-93
ISSN *online* 2549-8517

Implementasi Metode Data Encryption Standard (Des) Untuk Enkripsi Dan Dekripsi Data Kependudukan Desa Wonoharjo

Tri Agustina[1], Suhirman[2]
[1]Program Studi Informatika, Universitas Teknologi Yogyakarta
[2]Program Studi Magister Teknologi Informasi, Universitas Teknologi Yogyakarta
e-mail: [1]triagustina@student.uty.ac.id, [2]suhirman@uty.ac.id

Intisari

Desa Wonoharjo adalah salah satu desa yang berada di kecamatan Kemusu, kabupaten Boyolali, provinsi Jawa Tengah dengan jumlah penduduk sebanyak 3.208 jiwa. Data penduduk tersebut saat ini hanya tersimpan didalam folder komputer milik desa yang dapat diakses oleh siapapun dan tanpa adanya pengamanan khusus untuk mengamankan data-data tersebut. Hal ini tentunya sangat beresiko apabila ada orang yang tidak bertanggung jawab mengakses komputer dan menyalahgunakan data penduduk untuk kepentingan pribadi. Untuk mengatasi permasalahan tersebut, maka dibuatlah sebuah sistem yang menggunakan algoritma *Data Encryption Standard* (DES) sebagai metode untuk mengamankan data penduduk. Pengamanan data tersebut dilakukan melalui proses enkripsi menggunakan kunci simetri pada saat data penduduk ditambahkan kedalam sistem. Berdasarkan hasil penelitian yang telah dilakukan data penduduk berhasil terenkripsi dengan baik didalam database dengan bentuk *ciphertext* yang sulit dipahami. Sehingga dapat disimpulkan bahwa sistem yang dibuat dapat mengamankan data penduduk dari kebocoran dan penyalahgunaan data dibandingkan dengan sistem sebelumnya.

Kata kunci— Desa Wonoharjo, Data Penduduk, Keamanan Data, Data Encryption Standard (DES), Enkripsi

Abstract

Wonoharjo Village is one of the villages in Kemusu sub-district, Boyolali district, Central Java province with a population of 3,208 people. The population data is currently only stored in the village computer folder which can be accessed by anyone and without any special security to secure the data. This is certainly very risky if there are irresponsible people accessing the computer and misusing population data for personal gain. To overcome these problems, a system was created that uses the Data Encryption Standard (DES) algorithm as a method to secure resident data. Data security is done through an encryption process using a symmetric key when resident data is added to the system. Based on the results of the research that has been done, the resident data is successfully encrypted properly in the database with a ciphertext form that is difficult to understand. So it can be concluded that the system created can secure resident data from data leakage and misuse compared to the previous system.

Keywords— *Wonoharjo Village, Resident Data, Data Security, Data Encryption Standard (DES),Encryption*

Jurnal Dinamika Informatika
Volume 14, No 1, Maret 2025
ISSN 1978-1660 : 78-93
ISSN *online* 2549-8517

PENDAHULUAN

Desa Wonoharjo adalah salah satu desa di kecamatan Kemusu, kabupaten Boyolali, provinsi Jawa Tengah. Wonoharjo merupakan sebuah desa yang sebenarnya sangat berpotensi untuk daerah wisata karena desa ini langsung berbatasan dengan Waduk Kedung Ombo. Baik dari sektor kehutanan, perkebunan, peternakan dan perikanan. Data jumlah penduduk desa Wonoharjo tahun 2023 yaitu sebanyak 3.208 jiwa. Setiap tahunnya jumlah penduduk selalu meningkat, maka akan bertambah banyak juga data yang harus dikelola oleh perangkat desa, seperti data akta kelahiran, data kartu tanda penduduk, data kartu keluarga, data kematian serta data penting lainnya yang bersifat rahasia. Oleh karena itu perlu pengaman khusus yang berguna untuk mengamankan data-data tersebut.

Pemerintah Desa Wonoharjo bergerak dibidang pengolahan informasi dan pendataan penduduk, di mana kantor tersebut telah menggunakan komputer dalam penerapan kegiatan pelayanannya. Dari hasil pengamatan saya kantor desa tersebut belum menerapkan sistem keamanan untuk data penduduk. Karena komputer yang digunakan dapat diakses oleh seluruh perangkat desa sehingga sangat beresiko apabila ada orang yang tidak bertanggung jawab mengakses komputer tersebut untuk mencuri data, atau kemungkinan lainnya yaitu menyalahgunakan data penduduk untuk kepentingan yang tidak baik misalnya digunakan untuk melakukan pinjaman online, mengolah informasi bantuan sosial pemilik data dan lain sebagainya. Selain itu, apabila data hilang akan menyebabkan kerugian yang sangat besar bagi pemilik data maupun pihak desa.

Penelitian Wijaya, P. A., dkk. (2020) [1] menjelaskan bahwa mengimplementasikan sistem untuk pengamanan data menggunakan algoritma Des, Aes Dan Md5 yang digunakan untuk memerkecil tingkat kejahatan yang memanfaatkan data diri penduduk, yang merupakan suatu data yang tidak seharusnya di ketahui oleh banyak orang. Pada penelitian ini berhasil dibuktikan bahwa ukuran file hasil enkripsi dan kebutuhan waktu proses dipengaruhi oleh ukuran file asli, namun tidak dipengaruhi oleh jenis file. Penelitian oleh Fachri, B., & Sembiring, R. M. (2020) [2] menjelaskan bahwa penelitian untuk mengamankan

data teks ini menggunakan algoritma DES *(Data Encryption Standard)* dengan proses enkripsi dan dekripsi, hasil dari pengamanan data teks tersebut dapat mengembalikan pesan yang terenkripsi kembali ke hasil pesan aslinya yaitu dekripsi, pesan dikirim melalui SMS dan *WhatsApp.* Penelitian oleh Dwitri, N., dkk. (2019) [3] membahas tentang bagaimana mengamankan data file dokumen menggunakan kriptografi DES. Hasil dari penelitian tersebut data-data penting dapat diamankan dengan dienkripsi dan dekripsi menggunakan algoritma DES. Penelitian oleh Damanik, A. B. S., dkk. (2020) [4] membahas tentang bagaimana mengamankan data karyawan dalam perusahaan. Hasil dari penelitian ini yaitu menghasilkan enkripsi yang tidak dapat dipahami oleh manusia sehingga data karyawan aman dan tidak mudah diketahui orang. Penelitian oleh Hutapea, M. E. T., dkk. (2020) [5] menjelaskan bahwa penelitian ini menerapkan algoritma DES untuk mengamankan data nasabah koperasi dengan proses enkripsi dan dekripsi, kemudian hasil dari sistem kriptografi yang dibangun menggunakan algoritma DES dengan metode sistem *block cipher* berhasil menajaga kerahasiaan dan keamanan data nasabah pada Koperasi.

Berdasarkan penelitian tersebut banyak manfaat atau dampak positif dan negatif yang di timbulkan oleh perkembangan teknologi, di antaranya adalah keamanan yang semakin mudah di retas oleh setiap orang di karenakan akses untuk masuk ke suatu program atau data seseorang semakin mudah, karena adanya dukungan akses internet dan teknologi lainnya. Oleh sebab itu untuk mengantisipasi masalah tersebut dapat dilakukan dengan cara mengamankan data agar siapapun yang tidak berhak tidak dapat membaca, mengubah atau menghapus data tersebut. Untuk menangani terjadinya masalah tersebut maka, penulis menggunakan algoritma DES untuk proses mengamankan data. DES merupakan algoritma cipher block yang popular untuk penyandian karena algoritma ini dijadikan standar algoritma enkripsi yang menggunakan kunci simetri, yaitu algoritma yang dapat menggunakan kunci enkripsi dan kunci deskripsi yang sama [6]. Dengan menggunakan algoritma *Data encryption Standard* (DES) data penduduk Desa Wonoharjo yang sangat penting dan bersifat rahasia dapat teramankan.

Jurnal Dinamika Informatika
Volume 14, No 1, Maret 2025
ISSN 1978-1660 : 78-93
ISSN *online* 2549-8517

METODE PENELITIAN

Metode Pengamanan Data

Algoritma *Data Encryption Standard* (DES)

Algoritma DES merupakan salah satu algoritma kunci simetris berbentuk cipher blok artinya kunci yang digunakan untuk proses enkripsi sama dengan kunci yang digunakan untuk proses dekripsi [7]. Setiap algoritma DES mengenkripsikan 64 bit plainteks menjadi 64 bit cipherteks menggunakan 56 bit kunci internal atau dengan sub key. Kunci internal yang pada awalnya juga dibangkitkan dari kunci eksternal yang ukuran panjangnya menjadi 64 bit. Cara kerjanya adalah dengan mengubah pesan asli yang dapat dimengerti/dibaca manusia *(plainteks)* ke bentuk lain yang tidak dapat dimengerti/dibaca oleh manusia *(cipherteks)*. Proses transformasi plainteks menjadi cipherteks diistilahkan dengan enkripsi [8].

Metode Pengumpulan Data

1. Observasi

Penulis melakukan observasi secara langsung di kelurahan desa Wonoharjo dengan cara melihat bagaimana proses pengolahan, penyimpanan dan pengamanan data penduduk. Dari pengamatan tersebut, penulis mendapat suatu permasalahan dalam pengelolaan data penduduk salah satunya adalah dalam penyimpanan data-data yang bersifat rahasia masih dismpan pada folder komputer saja tanpa pengaman apapun.

2. Wawancara

Tahap ini dilakukan untuk mendapatkan informasi tambahan dari pihak-pihak yang memiliki wewenang dan berinteraksi langsung dengan Ibu Sulistiyah selaku kepala desa wonoharjo dan Ibu Gunanik, S.H selaku sekretaris desa wonoharjo dengan mengajukan beberapa pertanyaan terkait informasi secara detail mengenai permasalahan yang ada sehingga pembuatan sistem dapat berjalan dengan baik.

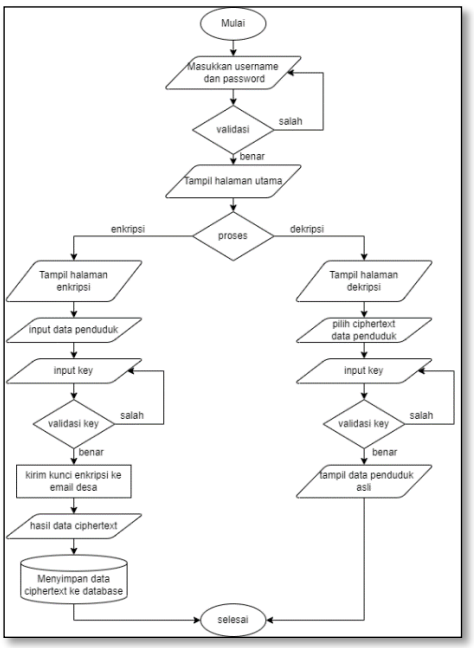
Prosedur pengumpulan data

Metode ini dilakukan dengan cara melakukan peninjauan terhadap buku, referensi, jurnal dan sumber lainnya yang berhubungan dengan permasalahan yang diteliti, dari studi pustaka ini mendapatkan hasil berupa landasan teori dari berbagai sumber

yang kemudian dijadikan sebagai referensi dalam membantu penelitian serta untuk menarik suatu kesimpulan dari berbagai peneliti.

Flowchart Sistem Dari Metode Penyelesaian

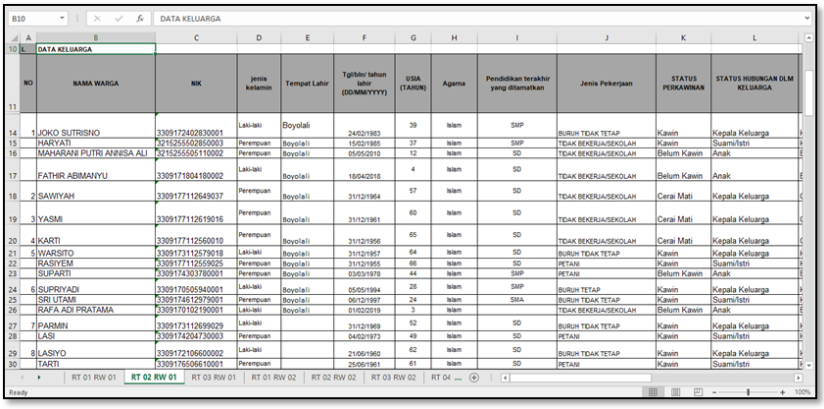
Berikut ini adalah flowchart dari proses enkripsi dan dekripsi dari algoritma DES yaitu sebagai berikut:



Gambar 1. Flowchart proses enkripsi dan dekripsi

Deskripsi Data Penelitian

Berikut merupakan data penduduk yang di dapat dari desa wonoharjo, yang akan diamankan. Dalam pengujiannya, sebagai contoh data yang digunakan sebagai sampel dalam penelitian ini yaitu sebagai berikut:



DATA KELUARGA

NO	NAMA WARGA	NIK	jenis kelamin	Tempat Lahir	Tgl/bln/ tahun lahir (DD/MM/YYYY)	USIA (TAHUN)	Agama	Pendidikan terakhir yang ditamatkan	Jenis Pekerjaan	STATUS PERKAWINAN	STATUS HUBUNGAN DLM KELUARGA
1	JOKO SUTRISNO	3309172402830001	Laki-laki	Boyolali	24/02/1983	39	Islam	SMP	BURUH TDAK TETAP	Kawin	Kepala Keluarga
2	HARYATI	3215255502850003	Perempuan	Boyolali	15/02/1985	37	Islam	SMP	TDAK BEKERJA/SEKOLAH	Kawin	Suami/Istri
3	MAHARANI PUTRI ANNISA ALI	3215255505110002	Perempuan	Boyolali	05/05/2010	12	Islam	SD	TDAK BEKERJA/SEKOLAH	Belum Kawin	Anak
4	FATHIR ABIMANYU	3309171804180002	Laki-laki	Boyolali	18/04/2018	4	Islam	SD	TDAK BEKERJA/SEKOLAH	Belum Kawin	Anak
5	SAWIYAH	3309177112649037	Perempuan	Boyolali	31/12/1964	57	Islam	SD	TDAK BEKERJA/SEKOLAH	Cerai Mati	Kepala Keluarga
6	YASMI	3309177112619016	Perempuan	Boyolali	31/12/1961	60	Islam	SD	TDAK BEKERJA/SEKOLAH	Cerai Mati	Kepala Keluarga
7	KARTI	3309177112560010	Perempuan	Boyolali	31/12/1956	65	Islam	SD	TDAK BEKERJA/SEKOLAH	Cerai Mati	Kepala Keluarga
8	WARSITO	3309173112579018	Laki-laki	Boyolali	31/12/1957	64	Islam	SD	BURUH TDAK TETAP	Kawin	Kepala Keluarga
9	RASIYEM	3309177112559025	Perempuan	Boyolali	31/12/1955	66	Islam	SD	PETANI	Kawin	Suami/Istri
10	SUPARTI	3309174303780001	Perempuan	Boyolali	03/03/1978	44	Islam	SMP	PETANI	Belum Kawin	Anak
11	SUPRIYADI	3309170505940001	Laki-laki	Boyolali	05/05/1994	28	Islam	SMP	BURUH TETAP	Kawin	Kepala Keluarga
12	SRI UTAMI	3309174612979001	Perempuan	Boyolali	06/12/1997	24	Islam	SMA	BURUH TDAK TETAP	Kawin	Suami/Istri
13	RAFA ADI PRATAMA	3309170102190001	Laki-laki	Boyolali	01/02/2019	3	Islam		TDAK BEKERJA/SEKOLAH	Belum Kawin	Anak
14	PARMIN	3309173112699029	Laki-laki		31/12/1969	52	Islam	SD	BURUH TDAK TETAP	Kawin	Kepala Keluarga
15	LASI	3309174204730003	Perempuan		04/02/1973	49	Islam	SD	PETANI	Kawin	Suami/Istri
16	LASIYO	3309172106600002	Laki-laki		21/06/1960	62	Islam	SD	BURUH TDAK TETAP	Kawin	Kepala Keluarga
17	TARTI	3309176506610001	Perempuan		25/06/1961	61	Islam	SD	PETANI	Kawin	Suami/Istri

Gambar 2. Sampel data penduduk desa wonoharjo

Jurnal Dinamika Informatika
Volume 14, No 1, Maret 2025
ISSN 1978-1660 : 78-93
ISSN *online* 2549-8517

Proses Enkripsi

Proses enkripsi adalah proses mengubah data asli (*plaintext*) ke ciphertext. Dalam proses enkripsi terdapat beberapa langkah yaitu, sebagai berikut:

1. Mengubah *Plaintext* dan *key* ke bilangan biner berdasarkan tabel ASCII

Tabel 1. Konversi *plaintext* dan *key* ke biner

PLAINTEXT		
	Dec	**Biner**
B	66	01000010
O	79	01001111
Y	89	01011001
O	79	01001111
L	76	01001100
A	65	01000001
L	76	01001100
I	73	01001001

KEY	
	Biner
12	00010010
28	00101000
7A	01111010
89	10001001
13	00010011
57	01010111
92	10010010
58	01011000

2. *Initial Permutation Plaintext*

Lakukan *initial permutation* (IP) pada bit *plaintext* menggunakan tabel IP:

Tabel 2. *Initial Permutation*

PLAINTEXT (X)								IP1						
0	1	0	0	0	0	1	0	57	49	41	33	25	17	9
0	1	0	0	1	1	1	1	1	58	50	42	34	26	18
0	1	0	1	1	0	0	1	10	2	59	51	43	35	27
0	1	0	0	1	1	1	1	19	11	3	60	52	44	36
0	1	0	0	1	1	0	0	63	55	47	39	31	23	15
0	1	0	0	0	0	0	1	7	62	54	46	38	30	22
0	1	0	0	1	1	0	0	14	6	61	53	45	37	29
0	1	0	0	1	0	0	1	21	13	5	28	20	12	4

Keterangan pada tabel *initial permutation* dan tabel IP(X):

Angka 0 dan 1 merupakan bilangan biner sedangkan angka 1,2,3 dan seterusnya adalah urutan posisi bit. Urutan bit pada plaintext urutan ke 58 ditaruh diposisi 1, urutan bit pada plaintext urutan ke 50 ditauruh di posisi 2 hingga seterusnya. Sehingga hasil outputnya adalah:

IP : 11111111 00000100 01011010 10101110 00000000 00000000 11011110 00001011

Kemudian bit pada IP(X) di pecah menjadi dua bagian yaitu L0 dan R0 masing-masing bernilai 32 bit, maka diperoleh:

L0 = 11111111 00000100 01011010 10101110

R0 = 00000000 00000000 11011110 00001011

3. Melakukan permutasi *key* kompresi PC-1

   Melakukan pembangkitan kunci yang akan digunakan untuk mengenkripsi plaintext dengan menggunakan tabel permutasi kompresi PC-1, dalam langkah ini terjadi kompresi kunci dari 64 bit menjadi 56 bit.

Tabel 3. *Initial Permutation*

KEY								PC1						
0	0	0	1	0	0	1	0	57	49	41	33	25	17	9
0	0	1	0	1	0	0	0	1	58	50	42	34	26	18
0	1	1	1	1	0	1	0	10	2	59	51	43	35	27
1	0	0	0	1	0	0	1	19	11	3	60	52	44	36
0	0	0	1	0	0	1	1	63	55	47	39	31	23	15
1	1	0	1	0	1	1	1	7	62	54	46	38	30	22
1	0	0	1	0	0	1	0	14	6	61	53	45	37	29
0	1	0	1	1	0	0	0	21	13	5	28	20	12	4

Hasil Output:

CD= 0110100 0101001 0000000 1101111 0111010 1001000 0010001 1100101

Pecah CD menjadi dua bagian sehingga menjadi:

C0 = 0110100 0101001 0000000 1101111

D0 = 0111010 1001000 0010001 1100101

4. Melakukan pergeseran kiri (*left shift)*

   Lakukan pergeseran kiri (*left shift)* pada C0 dan D0 sebanyak satu atau dua kali berdasarkan putaran yang ada pada tabel pergeseran berikut:

Tabel 4. Left Shift

Putaran *Key*	**Jumlah Pergeseran**
1	1
2	1
3	2
4	2
5	2

Jurnal Dinamika Informatika
Volume 14, No 1, Maret 2025
ISSN 1978-1660 : 78-93
ISSN *online* 2549-8517

6	2
7	2
8	2
9	1
10	2
11	2
12	2
13	2
14	2
15	2
16	1

Pergeseran dimulai dari putaran ke 1, dilakukan pergeseran 1 bit ke kiri, kemudian untuk putaran ke 2, dilakukan pergeseran 1 bit ke kiri, untuk putaran ke 3, dilakukan perputaran bit ke kiri, dan seterusnya hingga ke-16. Berikut hasil dari *left shift*:

Putaran ke-1, digeser 1 bit ke kiri.

C1 = 1101000 1010010 0000001 1011110

D1 = 1110101 0010000 0100011 1001010

Putaran ke-2, digeser 1 bit ke kiri.

C2 = 1010001 0100100 0000011 0111101

D2 = 1101010 0100000 1000111 0010101 dst.

C16 = 0110100 0101001 0000000 1101111

D16 = 0111010 1001000 0010001 1100101

Setiap hasil putaran digabungkan kembali menjadi C_1D_1 dan diinputkan kedalam tabel *Permutation Compression 2* (PC-2) dan terjadi kompresi data C_1D_1 56 bit menjadi C_1D_1 48 bit dan menghasilkan K_1.

Tabel 5. PC-2

14	17	11	24	1	5
3	28	15	6	21	10
23	19	12	4	26	8
16	7	27	20	13	2
41	52	31	37	47	55
30	40	51	45	33	48
44	49	39	56	34	53
46	42	50	36	29	32

Berikut hasil outputnya:

C_1D_1 = 1101000 1010010 0000001 1011110 1110101 0010000 0100011 1001010

K_1 = 000110 000011 000111 001011 001001 100011 110001 001010

C_2D_2 = 1010001 0100100 0000011 0111101 1101010 0100000 1000111 0010101

K_2 = 000110 110010 101010 010100 010110 100001 010110 000011 dst.

$C_{16}D_{16}$= 0110100 0101001 0000000 1101111 0111010 1001000 001000 11100101

K_{16} =101001 110000 100010 001001 001100 011010 000100 101011

5. Melakukan ekspansi data

Pada langkah ini akan dilakukan ekspansi data dari R_{i-1} 32 bit menjadi R_i 48 bit sebanyak 16 kali putaran dengan nilai perputaran 1>=i<= 16 menggunakan tabel ekspansi (E).

Tabel 6. *Ekspansi*

32	1	2	3	4	5
4	5	6	7	8	9
8	9	10	11	12	13
12	13	14	15	16	17
16	17	18	19	20	21
20	21	22	23	24	25
24	25	26	27	28	29
28	29	30	31	32	1

Hasil E(R_{i+1}) kemudian di XOR kan dengan K1 dan akan menghasilkan vektor matriks A1. Berikut hasil *outputnya:*

Iterasi 1

E((R(1)-1) = 100000 000000 000000 000001 011011 111100 000001 010110

K_1 = 000110 110010 101010 010100 010110 100001 010110 000011

---------- XOR

A_1 = 100110 110010 101010 010101 001001 011101 010110 010101

Pada iterasi 1 diatas dari hasil XOR menghasilkan A1, maka proses selanjutnya adalah langsung ke tahap ke-6 terlebih dahulu, A1 akan dimasukkan ke dalam S-box dan menghasilkan PB1 yang akan di XOR kan dengan L0 dan akan menhasilkan nilai R_i. Nilai R_i ini akan digunakan untuk iterasi ke-2.

6. Substitusi S-Box

A_1 = 100110 110010 101010 010101 001001 011101 010110 010101

Jurnal Dinamika Informatika
Volume 14, No 1, Maret 2025
ISSN 1978-1660 : 78-93
ISSN *online* 2549-8517

Tabel 7. S-Box 1

	0000	0001	0010	0011	0100	0101	0110	0111	1000	1001	1010	1011	1100	1101	1110	1111
00	1110	0100	1101	0001	0010	1111	1011	1000	0011	1010	0110	1100	0101	1001	0000	0111
01	0000	1111	0111	0100	1110	0010	1101	0111	1010	0110	1100	1011	1001	0101	0011	1000
10	0100	0111	1110	1000	1101	0110	0010	1011	1111	1100	1001	0111	0011	1010	0101	0000
11	1111	1100	1000	0010	0100	1001	0111	0111	0101	1011	0011	1110	1010	0000	0110	1101

Kemudian cara untuk mensubtitusi dengan S-Box disini peneliti mengambil contoh blok bit pertama dari vektor A1 yaitu 100110 selanjutnya pisahkan blok menjadi 2 bagian yaitu bit pertama 1 dan terakhir 0 digabungkan menjadi 10. Bit kedua hingga kelima 0011. Kemudian dapat dilihat perpotongan dari bit 10 dan bit 0011 adalah 1000 maka substitusi dari Box 1 adalah **1000**. Dan seterusnya untuk blok ketiga hingga kedelapan dibandingan dengan S3 dan S8. Berikut hasil dari proses diatas:

B1 = 1000 1000 1111 0010 0100 0011 0111 0110

7. Memutasikan Bit Vektor Bi

Setelah menghasilkan Bi, langkah selanjutnya adalah permutasi vektor B menggunakan tabel P-Box, kemudian dikelompokkan menjadi 4 blok dimana setiap blok memiliki 32 bit data.

Tabel 8. *P-Box*

16	7	20	21	29	12	28	17
1	15	23	26	5	18	31	10
2	8	24	14	32	27	3	9
19	13	30	6	22	11	4	25

Sehingga hasil yang didapat adalah sebagai berikut:

P(B1) = 00000110 11111111 01100101 00100100

Hasil P(Bi) di XOR kan dengan Li=1 untuk mendapatkan nilai R_i.

P(B1) = 00000110 11111111 01100101 00100100

L(1)-1 = 11111111 00000100 01011010 10101110

---------- XOR

R1 = 11111001 11111011 00111111 10001010 dst.

P(B16) = 00001110 00101111 10000111 10010010

L(16)-1 = 11100101 01101000 01011011 10101001

---------- XOR

R16 = 11101011 01000111 11011100 00111011

8. Menggabungkan R16 dan L16

   Langkah terakhir adalah menggabungkan R16 dan L16 kemudian dipermutasikan dengan tabel *initial permutation* (IP^{-1}).

Tabel 9. Ip^{-1}

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

R16 = 11101011 01000111 11011100 00111011
L16 = 11100101 01101000 01011011 10101001

R16L16 = 11100111 10100110 01101000 10011111 00001110 11010011 11111100 11001001

Menghasilkan output:

Tabel 10. Hasil proses enkripsi

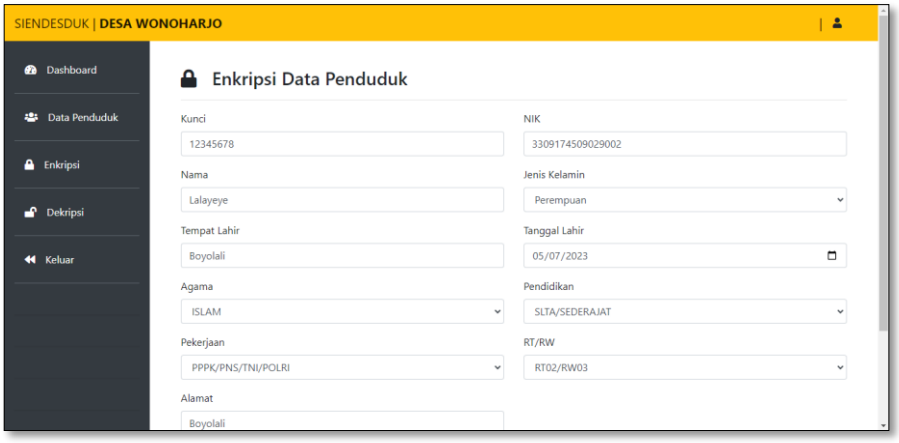
Biner	0001 0010	0010 1000	0111 1010	1000 1001	0001 0011	0101 0111	1001 0010	0101 1000
Hexa	12	28	7A	89	13	57	92	58
Character	=	1/4	Z	Ø	X	i	s	.

HASIL DAN PEMBAHASAN

Hasil dari penelitian ini berupa sistem kependudukan desa dalam bentuk website dengan mengimplementasikan algoritma Data Encryption Standard (DES) sebagai metode pengamanannya. Pada pembahasan ini akan menguji coba sistem yang bertujuan untuk membuktikan bahwa *input, proses* dan *output* yang dihasilkan oleh sistem telah sesuai. Berikut merupakan tahapan untuk pengujian sistem yaitu:

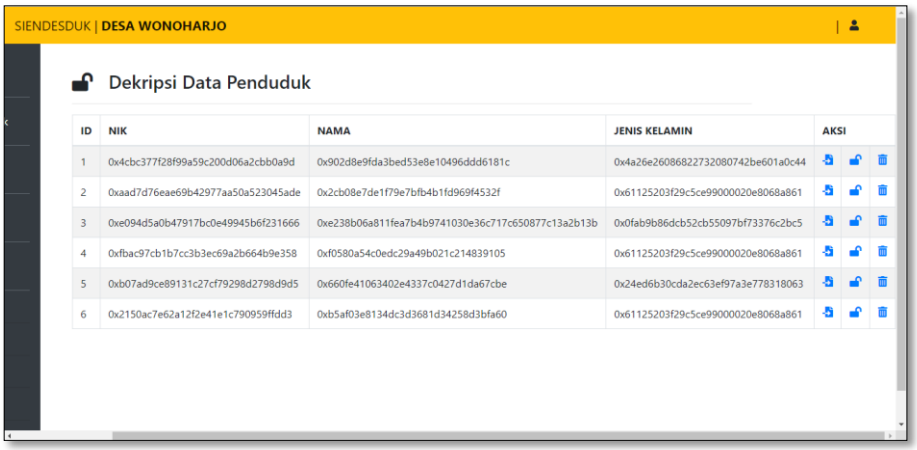
1. Melakukan *input* data penduduk yang kemudian sistem akan menampilkan data penduduk yang tersimpan kedalam database dalam bentuk *ciphertext.*

Jurnal Dinamika Informatika
Volume 14, No 1, Maret 2025
ISSN 1978-1660 : 78-93
ISSN *online* 2549-8517



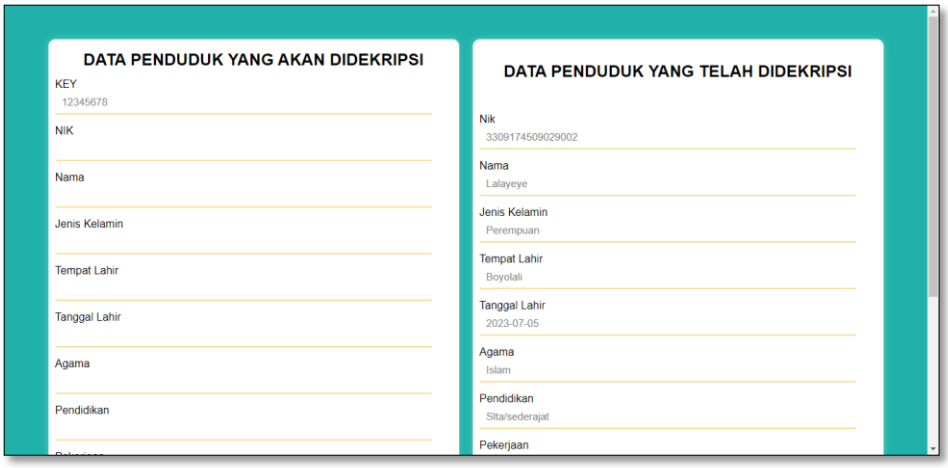
Gambar 3. Pengujian enkripsi data penduduk

2. Setelah selesai menambahkan data penduduk, maka data akan ditampilkan di sistem yaitu dibagian dekripsi, admin bisa memilih tiga aksi yaitu detail, dekripsi dan hapus data penduduk. Hasil enkripsi dapat dilihat pada gambar 4 dibawah ini.



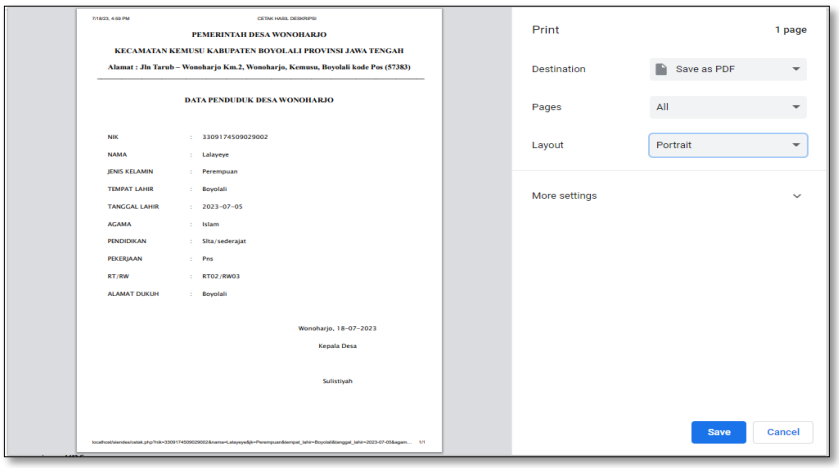
Gambar 4. Menampilkan hasil enkripsi data penduduk

3. Selanjutnya untuk melihat kembali data asli penduduk admin dapat mendekripsi dengan cara memilih icon kunci terbuka setelah itu admin bisa memasukkan kunci yang digunakan untuk proses enkripsi sebelumnya. Tahap dekripsi data dapat dilihat pada gambar 5.



Gambar 5. Pengujian dekripsi data penduduk

4. Button cetak dibawah form dekripsi digunakan untuk melihat detail data penduduk yang telah kembali ke bentuk semula. Tampilan hasil dekripsi penduduk dapat dilihat pafa gambar 6.



Gambar 7. Tampilan data penduduk asli

KESIMPULAN

Berdasarkan uraian dari pembahasan yang telah dibahas sebelumnya mengenai implementasi metode Data Encryption Standard (DES) peneliti dapat menarik kesimpulan yaitu dengan adanya implementasi pengamanan data penduduk menggunakan metode DES ini berhasil mengenkripsi data penduduk dengan baik didalam database dengan bentuk ciphertext yang sulit untuk dipahami.

Jurnal Dinamika Informatika
Volume 14, No 1, Maret 2025
ISSN 1978-1660 : 78-93
ISSN *online* 2549-8517

Sehingga dapat disimpulkan bahwa sistem yang dibuat dapat mengamankan data penduduk dari kebocoran dan penyalahgunaan data dibandingkan dengan sistem sebelumnya yang hanya disimpan ke dalam folder saja.

SARAN

Dari kesimpulan penelitian yang sudah dijelaskan, penulis memiliki beberapa saran yang disampaikan yaitu :

1. Dalam penelitian selanjutnya sistem dapat dikembangkan dengan menggabungkan atau menambah beberapa metode untuk mengamankan data.
2. Penerapan pengamanan data dalam proses enkripsi dengan menggunakan metode *Data Encryption Standar* (DES) dapat menggunakan ekstensi file.

UCAPAN TERIMA KASIH

Penulis mengucapkan terima kasih kepada Program Studi Informatika yang mendukung penelitian ini di Universitas Teknologi Yogyakarta sebagai tempat menggali data dan melengkapi penyusunan laporan penelitian. Selain itu, penulis juga mengucapkan terima kasih kepada Kantor Desa Wonoharjo yang telah berkenan menjadi obyek dalam penelitian ini.

DAFTAR PUSTAKA

[1] Wijaya, P. A., Damanik, M., Hartati, P., & Gunawan, I. (2020). Implementasi Enkripsi Dan Deskripsi Data Siak (Sistem Informasi Administrasi Kependudukan) Menggunakan Algoritma Des, Aes Dan Md5. *Techsi- Jurnal Teknik Informatika*, *12*(1), 43-51.

[2] Fachri, B., & Sembiring, R. M. (2020). Pengamanan Data Teks Menggunakan Algoritma DES Berbasis Android. *Jurnal Media Informatika Budidarma*, *4*(1), 110-116.

[3] Dwitri, N., Sindi, S., & Sihombing, I. A. (2020). Pengamanan Data File Document Mengunakan Kriptografi Encryption System (Des). *Journal Of Information System, Informatics And Computing*, *4*(1), 40-45.

[4] Damanik, A. B. S., Gunawan, I., Damanik, B. E., Sumarno, S., & Hartama, D. (2020). Implementasi Algoritma Data Encryption Standart (DES) Dalam Pengamanan Data Karyawan Ramayana Department Store. *Journal of Computer System and Informatics (JoSYC)*, *2*(1), 70-76.

[5] Hutapea, M. E. T., Taufik, F., & Al Hafiz, A. (2022). Implementasi Kriptografi Untuk Pengamanan Data Nasabah Dengan Metode DES (Data Encription Standard). *Jurnal Cyber Tech*, *3*(1), 1-12.

[6] Budi, A., & Chicali, A. (2019). Analisis Perbandingan Algoritma Kriptografi Metode Data Encryption Standard Dengan Metode Advanced Encryption System: Studi Kasus Pada Pt. One Standard Group Pte Ltd. *Jurnal Informatika Dan Bisnis, 8*(2).

[7] Ibrahim, R. N. (2019). Perangkat Lunak Keamanan Data Menggunakan Algoritma Kriptografi Simetri Tiny Encription Algorithm (Tea). *Jurnal Computech & Bisnis*, *13*(1), 01-10.

[8] Buulolo, N., & Sindar, A. (2020). Analisis dan Perancangan Keamanan Data Teks Menggunakan Algoritma Kriptografi DES (Data Encryption Standard). Respati, 15(3), 61-65.