Jurnal SAINTIKOM (Jurnal Sains Manajemen Informatika dan Komputer)
Vol.21. No.1, Februari 2022, pp. 1~9
P-ISSN : 1978-6603
E-ISSN : 2615-3475

Implementasi Kriptografi Pengamanan Data Nilai Siswa Menggunakan Algoritma DES

Widiarti Rista Maya[1*], Azanuddin[2], Elfitriani[3]
[1]Teknik Komputer, STMIK Triguna Dharma
[2]Sistem Komputer, STMIK Triguna Dharma
[3]Manajemen Informatika, STMIK Triguna Dharma

Article Info
Article history:
Received Jan 02th, 2022
Revised Jan 20th, 2022
Accepted Februari 24th, 2022

Keyword:
Data Encryption Standard (DES)
Keamanan Data
Kriptografi
Nilai Siswa
Steganografi

ABSTRACT
Perkembangan teknologi pada era digital saat ini, komputer digunakan untuk membantu dan mempercepat kinerja manusia, salah satunya dengan melakukan pengamanan data. Dalam menjaga keamanan data informasi terdapat cabang ilmu dalam pengembangannya seperti kriptografi dan steganografi. Keamanan data nilai siswa sangat penting agar pihak yang tidak berkepentingan tidak akan membaca dan memanipulasi data nilai siswa tersebut. Penelitian ini bertujuan untuk membuat sebuah sistem keamanan data dengan mengimplementasikan kriptografi pada data nilai siswa dengan melakukan perhitungan algoritma *Data Encryption Standard* (DES). Algoritma *Data Encryption Standard* (DES) adalah algoritma *cipher* blok yang digunakan untuk keamanan informasi dengan menggunakan metode simetrik dalam mengenkripsi dan dekripsi data ataupun informasi. Hasil dari penelitian ini diharapkan dapat memberikan manfaat dan solusi kepada SD Negeri 064979 Medan untuk mengamankan data nilai siswa yang diinput oleh guru sehingga meminimalkan kemungkinan untuk dibaca maupun dimanipulasi oleh pihak yang tidak berkepentingan.

Corresponding Author: *
Nama : Widiarti Rista Maya
Program Studi : Teknik Komputer
STMIK Triguna Dharma
Email: widiartirm87@gmail.com

1. PENDAHULUAN

Perkembangan teknologi pada era digital saat ini, komputer digunakan untuk membantu dan mempercepat kinerja manusia, salah satunya dengan melakukan pengamanan data. Berdasarkan literatur tersebut, perlu dilakukan upaya pengamanan informasi dan sistem elektronik. Hal tersebut sesuai dengan Pasal 27 ayat 4 UU ITE yang menyebutkan melarang setiap orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan pemerasan dan/atau pengancaman [1]. Dengan berlakunya Undang-Undang tersebut, beberapa perusahaan, instansi, akademik, sekolah dan lainnya melakukan pengamanan data informasi agar tidak diretas oleh *hacker*. Salah satu sekolah diantaranya adalah SD Negeri 064979 Medan.

SD Negeri 064979 Medan merupakan salah satu sekolah yang memanfaatkan aplikasi *microsoft office* untuk mendukung sistem sekolah terkait nilai pelajaran yang ditempuh siswa. Guru akan menginput nilai siswa dalam bentuk raport atau laporan hasil nilai siswa yang berupa angka, sedangkan siswa akan melihat nilai yang telah di input oleh guru pada raport atau laporan hasil nilai siswa. Akan tetapi, data nilai yang ada pada raport atau laporan hasil nilai siswa tersebut belum mengalami proses enkripsi, atau dengan kata lain masih dalam bentuk *plaintext*. Hal ini tentunya akan mempermudah pihak yang tidak berkepentingan untuk membaca dan memanipulasi data nilai siswa jika data nilai tersebut masih dalam keadaan *plaintext*. Oleh karena itu, beberapa literatur menyatakan bahwa cara untuk menyelesaikan masalah tersebut dengan menerapkan kriptografi.

Penelitian ini akan menjelaskan bagaimana manfaat kriptografi sebagai pengamanan data nilai siswa. Dalam beberapa literatur menjelaskan bahwasannya kriptografi dapat memecahkan permasalahan, diantaranya adalah Pengamanan data pada pesan teks, isi file dokumen, dan file dokumen [2], Pengamanan data rekam medis pasien [3], Keamanan data gaji karyawan [4], Keamanan data simpan pinjam [5].

Keakuratan dalam proses enkripsi dan dekripsi hal yang utama dalam bi-dang kriptografi. Jika terjadi kesalahan dalam proses enkripsi, maka akan menghasilkan pesan yang salah pula. Jika terjadi kesalahan dari hasil enkripsi maka hasil dekripsi juga akan terjadi kesalahan [6].

Penelitian ini diharapkan dapat memberikan manfaat dan solusi kepada SD Negeri 064979 Medan untuk mengamankan data nilai siswa yang diinput oleh guru sehingga meminimalkan kemungkinan untuk dibaca maupun dimanipulasi oleh pihak yang tidak berkepentingan.

2. METODE PENELITIAN

2.1. Teknik Pengumpulan Data

Dalam teknik pengumpulan data terdapat beberapa yang dilakukan di antaranya yaitu observasi. Upaya observasi dalam penelitian ini dilakukan dengan tinjauan langsung ke SD Negeri 064979 Medan.

2.2. Perancangan Sistem

Dalam konsep penulisan metode perancangan sistem merupakan salah satu unsur penting dalam penelitian. Dalam metode perancangan sistem khususnya *software* atau perangkat lunak dapat mengadopsi beberapa metode di antaranya algoritma *waterfall* atau algoritma air terjun. Di dalam penelitian ini, di adopsi sebuah metode perancangan sistem, yaitu *waterfall* algorithm.

2.3. Algoritma Sistem

Algoritma sistem merupakan penjelasan langkah-langkah penyelesaian masalah dalam perancangan aplikasi dalam mengamankan data dengan menggunakan algoritma DES *(Data Encryption Standard)*.

2.4. Nilai Siswa

Nilai siswa merupakan hasil belajar siswa berdasarkan kemampuan, pengetahuan individual yang dimiliki siswa dan digunakan sebagai informasi dalam bentuk raport atau laporan hasil nilai siswa yang berupa angka.

2.5. Kriptografi

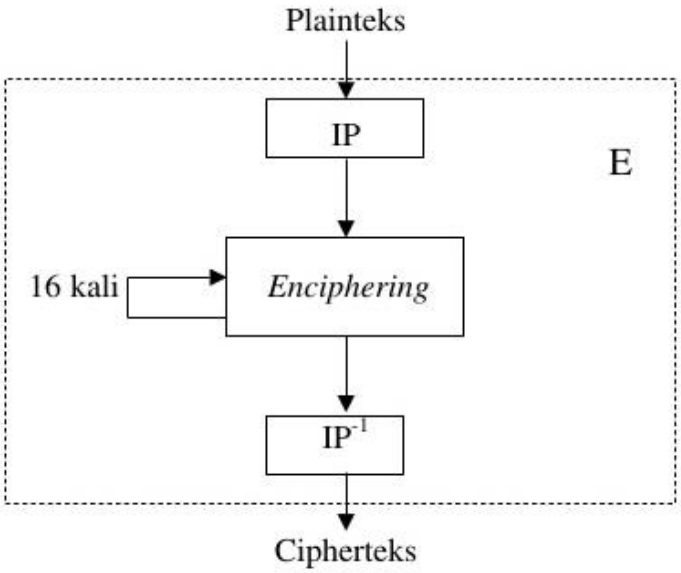
Kriptografi merupakan ilmu dan seni untuk menjaga keamanan informasi seperti kerahasiaan, integritas data, serta otentikasi [7]. Adapun tujuan dari sistem kriptografi adalah sebagai berikut [8] :

1. *Confidentiality* : Memberikan kerahasiaan pesan dan menyimpan data dengan menyembunyikan informasi lewat teknik enkripsi.
2. *Message Integrity* : Memberikan jaminan untuk tiap bagian bahwa pesan tidak akan mengalami perubahan dari saat pesan dibuat sampai saat pesan dibuka.
3. *Non-repudiation* : Memberikan cara untuk membuktikan bahwa suatu dokumen datang dari pengirim apabila pengirim tersebut mencoba menyangkal memiliki dokumen tersebut.

2.6. Algoritma DES *(Data Encryption Standard)*

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 [9]. DES menggunakan kunci sebesar 64 bit untuk mengenkripsi blok juga sebesar 64 bit. Akan tetapi, karena 8 bit dari kunci digunakan sebagai *parity*, kunci efektif hanya 65 bit [10]. Adapun skema global dari algoritma DES adalah sebagai berikut [11] :

1. Blok *plaintext* dipermutasi dengan matriks permutasi awal (*initial permutation* atau IP).
2. Hasil permutasi awal kemudian di *enciphering* sebanyak 16 kali (16 putaran). Setiap putaran menggunakan kunci internal yang berbeda.
3. Hasil *enciphering* kemudian dipermutasi dengan matriks permutasi balikan (*invers initial permutation* atau IP-1) menjadi blok *cipher* teks.



Gambar 1. Skema Algoritma DES

3. ANALISA DAN HASIL

3.1. Deskripsi Data Penelitian

Untuk menganalisa algoritma yang digunakan ada beberapa tahapan yang akan dilakukan dengan membuat suatu skenario algoritma DES *(Data Encryption Standard)*. Objek dari penelitian ini yaitu sebuah data nilai siswa SD Negeri 064979 Medan yang dijadikan sebagai *plaintext* dan akan dienkripsikan adalah 77,6000 dan untuk *key* (K) yaitu SDN79MDN, maka langkah pertama yang harus dilakukan untuk mengubah *plaintext* ke dalam bentuk biner.

1. Proses Enkripsi
   a. Mengubah *Plaintext* Dan Kunci Menjadi Bilangan Biner
      Ubahlah *plaintext* ke dalam bentuk biner berdasarkan tabel ASCII.
      Plaintext : 77,6000
      Key (K) : SDN79MDN
      Tabel *plaintext* dan kunci dapat dilihat pada tabel 1 dan 2 berikut ini.

Tabel 1. Plaintext

Hexa		Biner							
		1	2	3	4	5	6	7	8
7	39	0	0	1	1	0	1	1	1
		9	10	11	12	13	14	15	16
7	39	0	0	1	1	0	1	1	1
		17	18	19	20	21	22	23	24
,	2C	0	0	1	0	1	1	0	0
		25	26	27	28	29	30	31	32
6	36	0	0	1	1	0	1	1	0
		33	34	35	36	37	38	39	40
0	30	0	0	1	1	0	0	0	0
		41	42	43	44	45	46	47	48
0	30	0	0	1	1	0	0	0	0
		49	50	51	52	53	54	55	56
0	30	0	0	1	1	0	0	0	0
		57	58	59	60	61	62	63	64
0	30	0	0	1	1	0	0	0	0

Tabel 2. Kunci

Hexa		Biner							
		1	2	3	4	5	6	7	8
S	53	0	1	0	1	0	0	1	1
		9	10	11	12	13	14	15	16
D	44	0	1	0	0	0	1	0	0
		17	18	19	20	21	22	23	24
N	4E	0	1	0	0	1	1	1	0
		25	26	27	28	29	30	31	32
7	37	0	0	1	1	0	1	1	1
		33	34	35	36	37	38	39	40
9	39	0	0	1	1	1	0	0	1
		41	42	43	44	45	46	47	48
M	4D	0	1	0	0	1	1	0	1
		49	50	51	52	53	54	55	56
D	44	0	1	0	0	0	1	0	0
		57	58	59	60	61	62	63	64
N	4E	0	1	0	0	1	1	1	0

b. *Initial Permutation* (IP) pada Plaintext
Lakukan *Initial Permutation* (IP) pada bit *Plaintext* menggunakan tabel IP, sesuai dengan tabel 3 berikut.

Tabel 3. *Initial Permutation* (IP)

Plaintext (X)							
1	2	3	4	5	6	7	8
0	0	1	1	0	1	1	1
9	10	11	12	13	14	15	16
0	0	1	1	0	1	1	1
17	18	19	20	21	22	23	24
0	0	1	0	1	1	0	0
25	26	27	28	29	30	31	32
0	0	1	1	0	1	1	0
33	34	35	36	37	38	39	40
0	0	1	1	0	0	0	0
41	42	43	44	45	46	47	48
0	0	1	1	0	0	0	0
49	50	51	52	53	54	55	56
0	0	1	1	0	0	0	0
57	58	59	60	61	62	63	64
0	0	1	1	0	0	0	0

Tabel IP							
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

Hasil *Initial Permutation* (IP), dapat dilihat pada tabel 4 dibawah ini.

Tabel 4. Hasil *Initial Permutation* (IP)

IP (X)							
1	2	3	4	5	6	7	8
0	0	0	0	0	0	0	0
9	10	11	12	13	14	15	16
1	1	1	1	1	0	1	1
17	18	19	20	21	22	23	24
0	0	0	0	1	1	1	1
25	26	27	28	29	30	31	32

L0

0	0	0	0	0	0	1	1
33	34	35	36	37	38	39	40
0	0	0	0	0	0	0	0
41	42	43	44	45	46	47	48
1	1	1	1	1	1	1	1
49	50	51	52	53	54	55	56
0	0	0	0	0	1	0	0
57	58	59	60	61	62	63	64
0	0	0	0	1	0	1	1

R0

Atau bisa dituliskan :

IP (x) : 00000000 11111011 00001111 00000011 00000000 11111111 00000100 00001011

c. Melakukan Permutasi Kompresi PC-1
Permutasi kompresi PC-1 dan hasilnya, sesuai pada tabel 5 dan 6 berikut.

Tabel 5. Permutasi Kompresi PC-1

Kunci							
1	2	3	4	5	6	7	8
0	1	0	1	0	0	1	1
9	10	11	12	13	14	15	16
0	1	0	0	0	1	0	0
17	18	19	20	21	22	23	24
0	1	0	0	1	1	1	0
25	26	27	28	29	30	31	32
0	0	1	1	0	1	1	1
33	34	35	36	37	38	39	40
0	0	1	1	1	0	0	1
41	42	43	44	45	46	47	48
0	1	0	0	1	1	0	1
49	50	51	52	53	54	55	56
0	1	0	0	0	1	0	0
57	58	59	60	61	62	63	64
0	1	0	0	1	1	1	0

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

Tabel 6. Hasil Permutasi Komprensi PC-1

Output						
1	2	3	4	5	6	7
0	0	0	0	0	0	0
8	9	10	11	12	13	14
0	1	1	1	0	0	1
15	16	17	18	19	20	21
1	1	0	0	0	1	1
22	23	24	25	26	27	28
0	0	0	0	0	0	1
29	30	31	32	33	34	35

C0

1	0	0	0	1	1	0
36	37	38	39	40	41	42
1	1	1	1	0	1	1
43	44	45	46	47	48	49
1	0	1	0	1	1	0
50	51	52	53	54	55	56
1	0	0	1	0	0	1

D0

Atau bisa dituliskan :

Output : 0000000 0111001 1100011 0000001 1000110 1111011 1010010 1001001

Iterasi-1

E(r(1)-1) = 100000 000001 011111 111110 100000 001000 000001 010110

K1 = 100000 001001 010001 001110 110111 010010 010100 010101

---------- XOR

A1 = 000000 001000 001110 110000 010111 011010 010101 000011

d. Menggabungkan R16 dengan L16

Langkah terakhir adalah menggabungkan R16 dengan L16 lalu dipermutasikan untuk terakhir kali dengan tabel *inverse initial permutation* (IP-1), sesuai tabel 7 berikut.

Tabel 7. IP-1

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

Sehingga inputnya :

R16L16 = **00100101 00010101 10010011 01101000 10100110 00010011 01001111 00101010**

Menghasilkan output :

Cipher (dalam biner) = **01111100 10101110 11011000 00001011 00110000 11000011 00101000 10000100**

3.2. Pengujian Dan Implementasi

Implementasi merupakan tahap yang dalam mengoperasikan sistem yang dibangun. Dalam bab ini akan dijelaskan bagaimana menjalankan sistem yang telah dibangun tersebut. Dibawah ini merupakan tampilan dari implementasi kriptografi menggunakan algoritma DES.

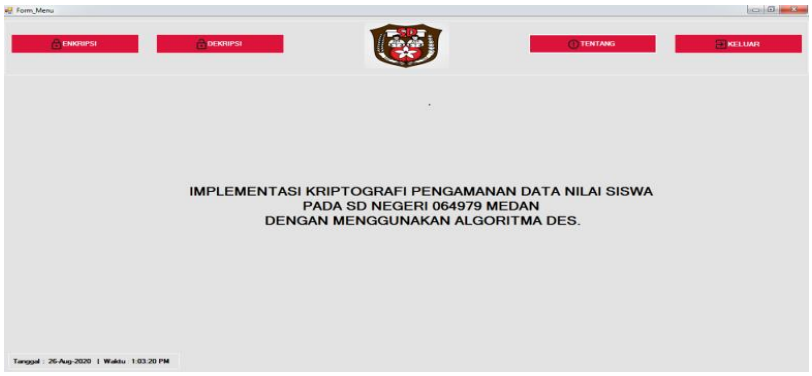
1. Tampilan *Form Login*

Form login merupakan form awal atau *form* untuk masuk yang akan membawa *user* menuju menu utama dalam sistem. Berikut gambar 2 adalah tampilan *form login*, dapat dilihat di bawah ini.

Gambar 2. Tampilan *From Login*

2. Tampilan Menu Utama

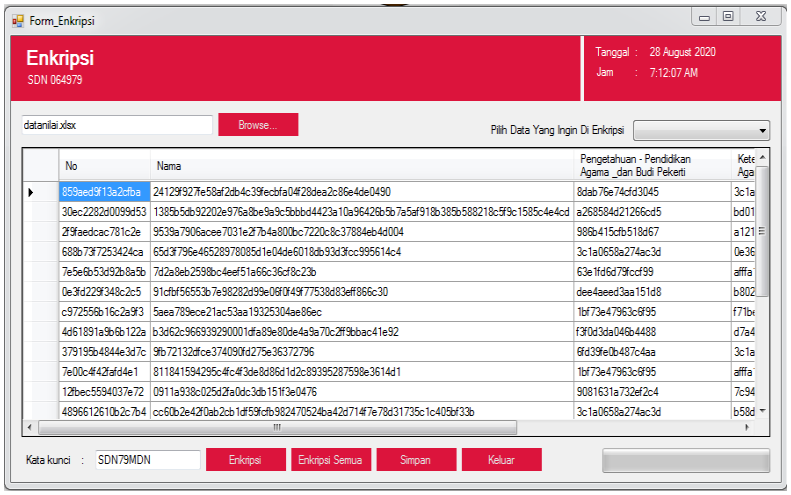
Form menu utama adalah *form* yang dirancang sebagai *form* induk yang menampilkan menu-menu yang akan digunakan *user*. Berikut gambar 3 adalah tampilan *form* menu utama, dapat dilihat di bawah ini.



Gambar 3. Tampilan Menu Utama

3. Tampilan *From* Enkripsi

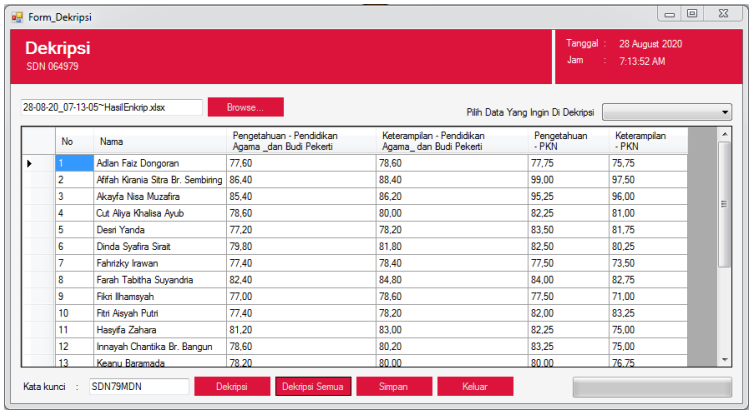
Berikut gambar 4 adalah tampilan *form* enkripsi yang berfungsi untuk melakukan enkripsi dengan menggunakan algoritma DES *(Data Encryption Standard)*.



Gambar 4. Tampilan *From* Enkripsi

4. Tampilan *Form* Dekripsi

Berikut gambar 5 adalah tampilan *form* dekripsi yang berfungsi untuk melakukan dekripsi dengan menggunakan algoritma DES *(Data Encryption Standard).*



Gambar 5. Tampilan *From* Dekripsi

5. Tampilan *Form* Tentang

Form tentang adalah *form* yang dirancang sebagai *form* yang menampilkan tentang asal pembuatan aplikasi ini. Berikut gambar 6 adalah tampilan *form* tentang, dapat dilihat di bawah ini.

Gambar 6. Tampilan *Form* Tentang

4. KESIMPULAN

Dari hasil pembahasan dari Bab 1 sampai Bab 5 mengenai aplikasi kriptografi untuk mengamankan data nilai siswa pada SD Negeri 064979 Medan dengan menggunakan algoritma DES *(Data Encryption Standard)* kesimpulan adalah sebagai berikut:

1. Pengamanan data nilai siswa dengan teknik kriptografi dilakukan dengan cara menggunakan frasa sandi yang kunci keamanan data nilai siswa hanya diketahui oleh pihak yang berkepentingan saja khususnya kepala sekolah atau pengguna aplikasinya.
2. Dalam proses mengamankan isi data nilai dengan algoritma DES *(Data Encryption Standard)*, dimulai dengan melakukan permutasi dengan matriks permutasi awal (*initial permutation* atau IP), kemudian hasil permutasi awal kemudian di *enciphering* sebanyak 16 kali (16 putaran). Setiap putaran menggunakan kunci internal yang berbeda. Hasil *enciphering* kemudian dipermutasi dengan matriks permutasi balikan (*invers initial permutation* atau IP-1) menjadi blok *cipher* teks.

3. Merancang dan mendesain sistem aplikasi kriptografi pengaman data nilai siswa pada SD Negeri 064979 Medan dengan menggunakan algoritma DES *(Data Encryption Standard)* dilakukan dengan mengimplementasikan seluruh rancangan yang ada ke dalam bahasa pemograman *visual basic*.

UCAPAN TERIMA KASIH

Terima kasih kepada STMIK Triguna Dharma dan Team editor serta pihak-pihak yang mendukung penyelesaian artikel ilmiah ini.

REFERENSI

[1] Rahmad Toni Ryan. Pembahasan Tentang IT. Rabu, 04 April 2018. [Online].Available:http://rahmadryantoni.blogspot.com/ [Akses : 14 Desember 2019].
[2] Fresly Nandar Pabokory, Indah Fitri Astuti, and Awang Harsa Kridalaksana, "Implementasi Kriptografi Pengamanan Data Pada Pesan Teks, Isi File Dokumen, Dan File Dokumen Menggunakan Algoritma Advanced Encryption Standard", 2015.
[3] Erwin Gunadhi and Agung Sudrajat, "Pengamanan Data Rekam Medis Pasien Menggunakan Kriptografi Vigènere Cipher",2016.
[4] J. Prayudha, _ S., and _ I., "Implementasi Keamanan Data Gaji Karyawan Pada PT. Capella Medan Menggunakan Metode Advanced Encryption Standard (AES)," *J. SAINTIKOM (Jurnal Sains Manaj. Inform. dan Komputer)*, vol. 18, no. 2, p. 119, 2019, doi: 10.53513/jis.v18i2.150.
[5] B. Anwar, N. B. Nugroho, J. Prayudha, and A. Azanuddin, "Implementasi Algoritma RSA Terhadap Keamanan Data Simpan Pinjam," *J. SAINTIKOM (Jurnal Sains Manaj. Inform. dan Komputer)*, vol. 18, no. 1, p. 30, 2019, doi: 10.53513/jis.v18i1.100.
[6] M. Syaifuddin, J. Hutagalung, and G. Ganefri, "E-Learning Dalam Pengembangan Pembelajaran Kriptografi," JURTEKSI (Jurnal Teknol. dan Sist. Informasi), vol. 7, no. 2, pp. 117–126, 2021, doi: 10.33330/jurteksi.v7i2.914.
[7] Desi Nurnaningsih and Angga Aditya Permana, "Rancangan Aplikasi Pengamanan Data Dengan Algoritma Advanced Encyption Standard (AES)," *Jurnal Teknik Informatika*, vol. 11, no. 2, pp. 177-186, Nov. 2018.
[8] Nur Muhammad Dwi Oktafiansyah et al., "14. Sakti Nur Muhammad Dwi_Penerapan Kriptografi Dengan Algoritma Data Encryption Standart Pada Text Hasil Konversi Dari Citra", 2016
[9] Husna Ismatul, Siswanto Apri, Syukur Abdul, "Perbandingan Metode Data Encryption Standard (DES) Dan Advanced Encryption Standard (AES) Pada Steganografi File Citra", 2018
[10] Widiarti Rista Maya,"Analisis Kinerja Algoritma Rabin dan Rivest Shamir Adleman (RSA) pada Kriptografi",2013
[11] Azanuddin,"Sistem Pengamanan Data Customer dengan Metode Data Encryption Standart (DES)",2019

BIBLIOGRAFI PENULIS

	Nama : Widiarti Rista Maya, ST., M.Kom NIDN : 0102128603 Program Studi : Teknik komputer Deskripsi :dosen tetap STMIK yang aktif mengajar dan fokus di bidang ilmu komputer dengan bidang keilmuan yaitu simulasi,kriptografi, pemrograman berbasis visual dan pemrograman berbasis web. Prestasi : Dosen Terbaik tahun 2019
	Nama : Azanuddin, S.Kom., M.Kom NIP : 0126068901 Jabatan : Ka. Prodi MI Divisi : Akademik
	Nama : Elfitriani, SPd., Msi NIDN : 0124097301 Program Studi : Manajemen Informatika Deskripsi : Dosen Tetap STMIK Triguna Dharma yang aktif mengajar dan fokus pada bidang keilmuan Bahasa Inggris yaitu English Quantum Club (EQC) Prestasi : berprestasi di Bidang Bahasa Inggris dengan Aktif menjadi Pembimbing Club' Keahlian Bahasa Inggris yaitu English Quantum Club (EQC) sejak tahun 2014 sampai sekarang.