IMPLEMENTASI KEAMANAN DATA NILAI SISWA MENGGUNAKAN METODE ADVANCED ENCRYPTION STANDARD (AES)

(Studi Kasus : Sekolah Menengah Pertama Negeri (SMPN) 3 Bungku)

[1]Arya Sura Pratama, [2]Sriyanto*

[1]Fakultas Ilmu Komputer, Institut Informatika dan Bisnis Darmajaya, aspkho@gmail.com
[2]Fakultas Ilmu Komputer, Institut Informatika dan Bisnis Darmajaya, sriyanto@darmajaya.ac.id

ABSTRAK

Sekolah Menengah Pertama Negeri (SMPN) 3 Bungku terletak di Jalan Produksi, No.2, Desa Ipi, Kecamatan Bungku Tengah, Kabupaten Morowali, Provinsi Sulawesi Tengah. Kurangnya keamanan database pada sistem informasi akademik Sekolah Menengah Pertama Negeri (SMPN) 3 Bungku. Bertujuan untuk mengamankan, menjaga keutuhan dan mencegah penyalahgunaan data. Maka di implementasikanlah AES pada sistem informasi akademik untuk menjaga kerahasiaan data siswa atau dokumen melalui media website yang akan dibangun. Pada penelitian ini menggunakan metode kualitatif melalui observasi langsung, wawancara dan studi pustaka. Implementasi sistem keamanan data *Advanced Encryption Standard*, diharapkan mampu memberikan sistem yang dapat melakukan enkripsi dan dekripsi serta mengamankan data agar tetap terjaga kerahasiaan dan keaslian data tersebut. Sistem ini dibangun dengan menggunakan web browser dan dibuat menggunakan Bahasa pemograman PHP, Javascript, MySQL dan HTML.

Kata Kunci: Website, *Advanced Encryption Standard*, PHP, MySQL

ABSTRACT

The State Junior High School (SMPN) 3 Bungku is located on Jalan Produk, No.2, Ipi Village, Bungku Tengah District, Morowali Regency, Central Sulawesi Province. Lack of database security in the academic information system of State Junior High School (SMPN) 3 Bungku. Aims to secure, maintain integrity and prevent misuse of data. Then AES is implemented in the academic information system to maintain the confidentiality of student data or documents through the media website that will be built. In this study using qualitative methods through direct observation, interviews and literature study. The implementation of the Advanced *Encryption Standard* data security system is expected to be able to provide a system that can perform encryption and decryption and secure data in order to maintain the confidentiality and authenticity of the data. This system is built using a web browser and is made using the PHP, Javascript, MySQL and HTML programming languages.

Keywords: Website, Advanced *Encryption Standard*, PHP, MySQL

1. Pendahuluan

1.1 Latar Belakang

Sistem informasi pendidikan adalah sistem informasi yang mengelola informasi sekolah, termasuk informasi siswa dan evaluasi siswa, yang dapat diakses oleh siswa, guru, dan kepala sekolah secara online. Sekolah Menengah Negeri (SMP) 3 Bungku. SMPN 3 Bungku terletak di Desa Ipi, No.2, Jalan Produksi, Kecamatan Bungku Tengah, Wilayah Morowali, Provinsi Sulawesi Tengah. Namun pada saat mengoperasikan sistem informasi pendidikan, belum terdapat sistem enkripsi untuk menjamin keamanan data dan mencegah penyalahgunaan.

Sistem enkripsi yang digunakan adalah AES (Advanced Encryption Standard). Pemilihan AES sebagai metode yang digunakan didasarkan pada keamanan dan karakteristiknya. AES

dikenal kuat terhadap analisis kata sandi yang diketahui dan tahan terhadap analisis kata sandi yang tidak diketahui. AES juga dapat digunakan secara gratis.

Salah satu kelemahan AES adalah perbedaan enkripsi dan struktur enkripsi. AES merupakan algoritma block cipher yang menggunakan sistem permutasi dan substitusi (P-Box dan S-Box) sebagai pengganti jaringan Feistel seperti block cipher.Oleh karena itu, penulis melakukan penelitian bertajuk "Implementasi Keamanan Data Menggunakan Teknik Standar Enkripsi Tingkat Lanjut (Studi Kasus: Sekolah Menengah Negeri (SMPN) Negeri 3)" untuk menjaga keamanan dan keandalan data di tanah air. Pendidikan Menengah (SMPN) SIA) 3 kursi.

1.2 Batasan Masalah

Batasan masalah dalam penelitian ini yaitu:

a. Data yang diamankan berupa semua data nilai siswa dengan menggunakan metode AES (Advance Encrytipon Standart).
b. Hak akses untuk melakukan enkripsi data hanya diberikan kepada siswa untuk menganmankan data nilai pribadi.
c. Ketika dilakukan enkripsi nama mata pelajaran, nilai dan hal-hal yang bersangkutan akan terenkripsi.
d. Metode yang digunakan hanya AES (Advance Encrytipon Standart).
e. Setelah data dienkripsi maka semua user tidak dapat melihat data dalam bentuk plaintext.

1.3 Tujuan Penelitian

Membangun sistem keamanan AES yang dapat mengingkatkan keamanan pada Sistem Informasi Akademik SMPN 3 Bungku. Sistem AES tersebut akan diimplementasikan pada data nilai siswa dalam Sistem Informasi Akademik. Dengan adanya sistem AES dapat membantu dalam menghindari penyalahgunaan data oleh pihak yang tidak berwenang.

2. Landasan Teori

2.1 Website

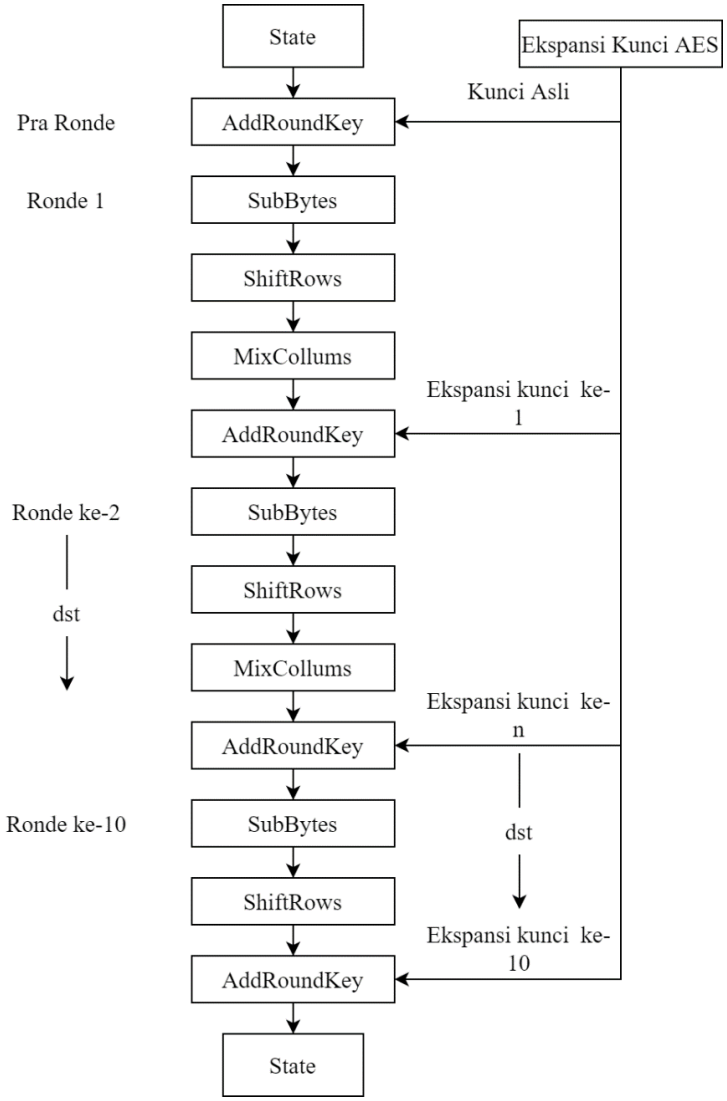
Menurut Simangunsong, A. (2018) Situs web adalah kumpulan halaman web dalam suatu domain yang berisi informasi. Domain adalah nama unik suatu organisasi yang tersedia di Internet (misalnya ephi.id, yahoo.com, google.com, dll). Untuk mendapatkan domain, Anda perlu membayar melalui registry yang ditentukan. Saat ini menurut Nouvel, A. dan Putri, W. (2020), pengertian website adalah jaring laba-laba, dalam dunia internet disebut website atau disebut dengan web. Situs web adalah kumpulan halaman informasi yang dapat diakses oleh dunia melalui Internet. Situs web adalah halaman web suatu domain yang berisi informasi.

2.2 Advanced *Encryption Standard*

Advanced *Encryption Standard* merupakan algoritma kriptografi simetrik yang beroperasi dalam mode penyandian blok (block cipher) yang memproses blok data 128-bit dengan panjang kunci 128-bit, 192-bit, dan 256-bit. Beberapa mode operasi yang dapat diterapkan pada algoritma kriptografi penyandi blok AES di antaranya adalah Electronic Code Book (ECB), Cipher Block Chaining (CBC), Cipher Feedback (CFB), dan Output Feedback (OFB). Implementasi AES dengan mode operasi ECB, CBC, CFB, dan OFB tentu saja memiliki kelebihan dan kekurangan tertentu dalam aspek tingkat keamanan data. Algoritma kriptografi bernama Rijndael yang didesain oleh oleh Vincent Rijmen dan John Daemen asal Belgia keluar sebagai pemenang kontes Algoritma kriptografi pengganti DES yang diadakan oleh NIST

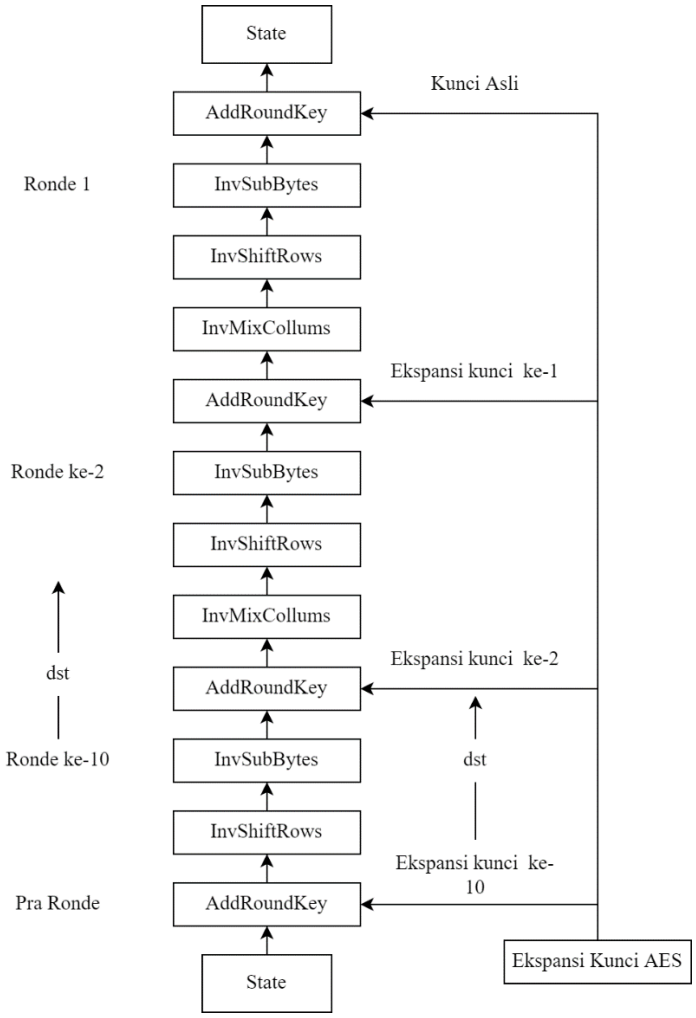
(National Institutes of Standards and Technology) milik pemerintah Amerika Serikat pada 26 November 2001. Algoritma Rijndael inilah yang kemudian dikenal dengan Advanced *Encryption Standard* (AES). Setelah mengalami beberapa proses standardisasi oleh NIST, Rijndael kemudian diadopsi menjadi standard algoritma kriptografi secara resmi pada 22 Mei 2002. Pada 2006, AES merupakan salah satu algoritma terpopuler yang digunakan dalam kriptografi kunci simetrik. (Prayudha, J., dkk., 2019).

Sedangkan menurut Permana, A., dan Nurnaningsih, D., 2018., Advanced *Encryption Standard* (AES) merupakan algoritma cryptographic yang dapat digunkan untuk mengamakan data. Algoritma AES adalah blok chipertext simetrik yang dapat mengenkripsi (encipher) dan dekripsi (decipher) informasi. Enkripsi merubah data yang tidak dapat lagi dibaca disebut ciphertext; sebaliknya dekripsi adalah merubah ciphertext data menjadi bentuk semula yang kita kenal sebagai plaintext. Algoritma AES menggunakan kunci kriptografi 128, 192, dan 256 bits untuk mengenkrip dan dekripsi data. Adapun flowchart dari enkripsi pada algoritma AES-128 dapat dilihat pada gambar 1.



Gambar 1. Flowchart Enkripsi Algoritma AES

Seperti yang dapat dilihat pada gambar 1, proses enkripsi pada algoritma AES memiliki 10 ronde. Pada setiap ronde tersebut terdapat proses SubBytes, ShiftRows, MixCollums, dan AddRoundKey. Pada proses AddRoundKey digunakan kunci yang didapat dari ekspansi kunci dari kunci asli yang kemudian digunakan pada setiap ronde. Kunci tersebut menggunakan key schedule yang digunakan oleh algoritma AES. Sedangkan flowchart dari dekripsi algoritma AES dapat dilihat pada gambar 2.



Gambar 2. Flowchart Dekripsi Algoritma AES

Seperti yang dapat dilihat pada gambar 2 proses dekripsi dalam algoritma AES merupakan inverse atau kebalikan dari proses enkripsi. Pada proses dekripsi SubBytes, ShiftRows dan MixCollums yang terdapat pada proses merupakan versi inverse dari langkah-langkah tersebut. Nama dari langkah-langkah tersebut adalah InvSubBytes, InvShiftRows dan InvMixCollums.

3. METODE PENELITIAN

3.1 Bahan /Data

Adapun data yang diperoleh dari Sekolah Menengah Pertama Negeri (SMPN) 3 Bungku berupa profil dan informasi guru dan siswa pada Sekolah Menengah Pertama Negeri (SMPN) 3

Bungku yang diberikan oleh petugas di dalam instansi tersebut. Selain itu, sumber lain sebagai referensi penelitian di dapat dari buku-buku, jurnal, skripsi yang dibuat oleh peneliti sebelumnya.

3.2 Aturan Bisnis

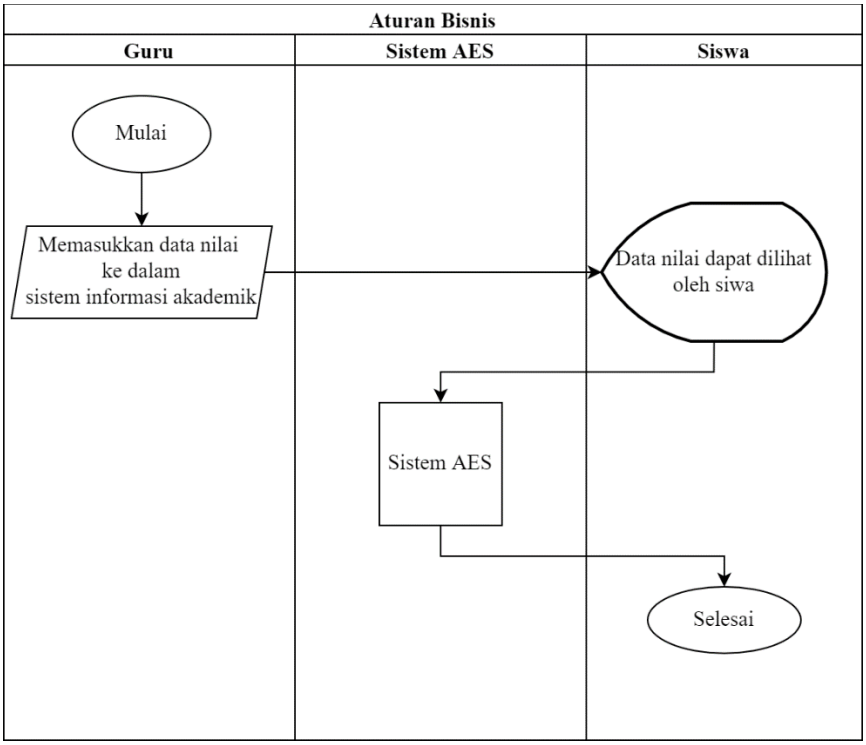
Aturan bisnis (Bussiness rule) adalah sebuah pernyataan yang menjelaskan kebijakan bisnis atau keputusan prosedur.

a. Prosedur

Berikut ini merupakan aturan bisnis sistem informasi akademik untuk nilai siswa :

1. Guru memasukkan data nilai ke dalam sistem informasi akademik.
2. Data nilai dapat dilihat siswa dalam sistem informasi akademik

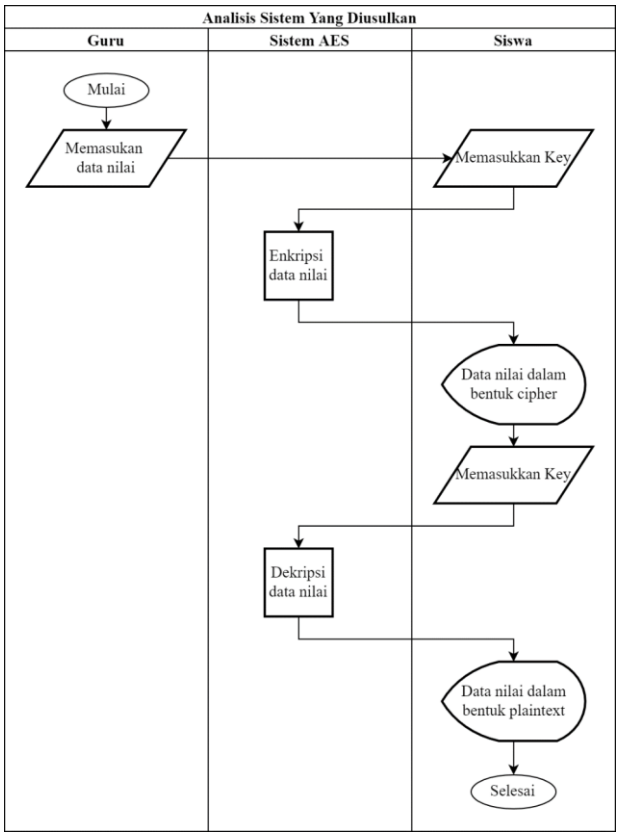
Untuk gambar 3 menunjukkan aturan bisnis dari pengelolaan data nilai sistem informasi akademik SMPN 3 Bungku.



Gambar 3. Aturan Bisnis

3.3 Analisis Sistem Yang Diusulkan

Sistem yang diusulkan adalah sebuah sistem keamanan data menggunakan AES untuk sistem informasi akademik. Hal ini diharapkan dapat menjaga keamanan data dari penyalahgunaan. Adapun diagram dari analisis sistem yang diusulkan dapat dilihat pada gambar 4



Gambar 4. Sistem yang diusulkan

3.4 Data Yang Diperoleh

Data yang diperoleh berupa data guru, data siswa dan data mata pelajaran. Data tersebut diperoleh dari petugas pada SMPN 3 Bungku.

No	Nama Mata Pelajaran	Jumlah
1	Data Guru	27
2	Data Siswa	53
3	Data Nama Mata Pelajaran	10

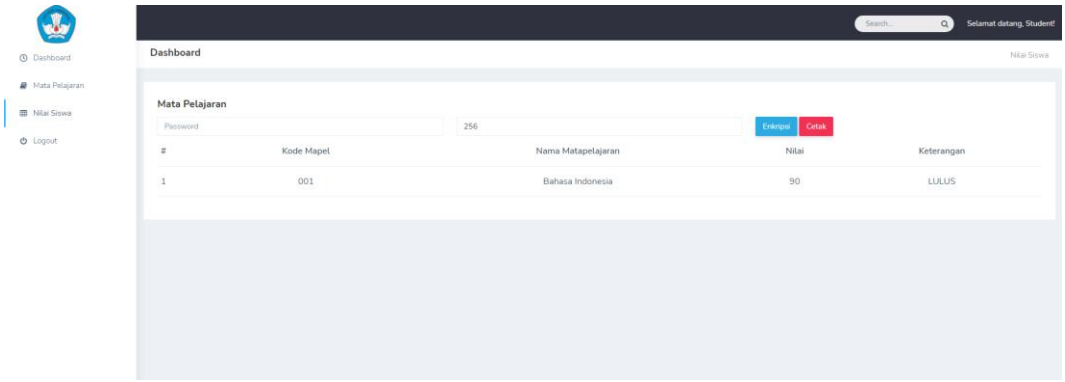
Tabel 1. Data

4 HASIL DAN PEMBAHASAN

4.1 Hasil

a. Implementasi Halaman Nilai Siswa

Halaman nilai siswa adalah halaman dimana siswa dapat melihat nilai dari kelas yang diikuti. Pada halaman ini siswa juga dapat melakukan enkripsi pada data nilai yang dimiliki. halaman nilai siswa yang digunakan untuk menampilkan kode mapel, nama mata pelajaran, nilai dan keterangan pada halaman nilai siswa. Adapun implementasi halaman nilai siswa dapat dilihat pada gambar 5.



Gambar 5. Implementasi Halaman Nilai Siswa

b. Perhitungan Sistem

Hasil merupakan sebuah akhir yang didapatkan dari tahapan-tahapan penelitian yang dilakukan. Dalam perancangan sistem keamanan sistem informasi akademik dengan metode AES. Data nilai yang dimiliki siswa dapat dienkripsi dan kemudian di simpan dalam sistem informasi akademik oleh siswa. Kemudian informasi enkripsi seperti password dan key akan dikirimkan ke email siswa. Siswa dapat melakukan dekripsi dengan menggunakan informasi yang sudah kirimkan melalui email. Adapun hasil dari enkripsi nilai siswa dapat dilihat pada gambar 6.

Gambar 6. Hasil Enkripsi Data Siswa

c. Simulasi Perhitungan

Simulasi perhitungan dalam Advanced *Encryption Standard*-128 dilakukan dengan plain text dan cipher key sebagai berikut:

Plain teks :BAHASAINDONESIA0

Key :1234000000000000

Langkah perhitungan pada algoritma AES dimulai dengan mengubah plainteks dan key yang akan digunakan pada AES ke dalam bentuk tabel 4x4

Tabel 2. Tabel Plain Text

B	S	D	S
A	A	O	I
H	I	N	A
A	N	E	0

Tabel 3. Tabel Cipher Key

1	0	0	0
2	0	0	0
3	0	0	0
4	0	0	0

Langkah ini kemudian dilanjutkan mengubah plainteks dan key dalam tabel 2 dan tabel 3 ke dalam hexadesimal.

Tabel 4. Tabel Plainteks Hexadesimal

42	53	44	53
41	41	4f	49
48	49	4e	41
41	4e	45	30

Tabel 5. Tabel Hexadecimal Cipher Key

31	30	30	30
32	30	30	30
33	30	30	30
34	30	30	30

1. PreRound

Setelah melakukan konversi plain text dan cipher key ke dalam bentuk hexa decimal dilanjutkan dengan merubah menjadi biner dan kemudian kedua tabel tersebut di XOR kan. Hasil XOR tersebut kemudian diubah kembali menjadi hexadesimal. Cara perhitungan XOR dapat dilihat seperti berikut :

42 = 01000010

31 = 00110001

---------- XOR

01110011 = 73

Langkah tersebut kemudian dilakukan pada kedua tabel. Hasil perhitungan XOR tabel Plainteks dan cipher key dapat dilihat seperti berikut :

42 XOR 31 = 01000010 XOR 00110001 = 01110011 = 73

53 XOR 30 = 01010011 XOR 00110000 = 01100011 = 63

44 XOR 30 = 01000100 XOR 00110000 = 01110100 = 74

53 XOR 30 = 01010011 XOR 00110000 = 01100011 = 63

41 XOR 32 = 01000001 XOR 00110010 = 01110011 = 73

41 XOR 30 = 01000001 XOR 00110000 = 01110001 = 71

4f XOR 30 = 01001111 XOR 00110000 = 01111111 = 7f

49 XOR 30 = 01001001 XOR 00110000 = 01111001 = 79

48 XOR 33 = 01001000 XOR 00110011 = 01111011 = 7b

49 XOR 30 = 01001001 XOR 00110000 = 01111001 = 79

4e XOR 30 = 01001110 XOR 00110000 = 01111110 = 7e

41 XOR 30 = 01000001 XOR 00110000 = 01110001 = 71

41 XOR 34 = 01000001 XOR 00110100 = 01110101 = 75

4e XOR 30 = 01001110 XOR 00110000 = 01111110 = 7e

45 XOR 30 = 01000101 XOR 00110000 = 01110101 = 75

30 XOR 30 = 00110000 XOR 00110000 = 00000000 = 00

Hasil AddRoundKey dapat dilihat pada tabel 6

Tabel 6. Tabel Hexadecimal AddRoundKey

73	63	74	63
73	71	7f	79
7b	79	7e	71
75	7e	75	00

2. Round 1

Proses setiap round memiliki beberapa proses yaitu proses SubSytes, ShiftRows, MixCollums dan AddRoundKey. Proses SubBytes merupakan proses dimana hasil dari AddRoundKey pada initial round disubsitusikan dengan tabel Rijndael S-Box. Hasil tersebut dapat dilihat pada tabel 7.

Tabel 7. Tabel Hexadecimal Hasil SubBytes

8f	fb	92	fb
8f	a3	d2	b6
21	b6	f3	a3
9d	f3	9d	63

Setelah melakukan proses SubBytes, proses dilanjutkan dengan melakukan proses ShiftRows. Proses ShiftRows permutasi untuk mengganti nilai pada element state. Permutasi ini hanya mengubah posisi elemen pada state tanpa mengubah nilainya. Transformasi permutasi pada state disebut dengan transformasi ShiftRows. ShiftRows dilakukan dengan cara memutar elemen matriks hasil proses transformasi SubByte pada baris 1, 2, dan 3 ke kiri dengan jumlah perputaran yang berbeda-beda. Baris pertama akan diputar sebanyak 1 kali, baris kedua sebanyak 2 kali, dam baris ke 3 akan diputar sebanyak 3 kali. Sedangkan baris ke 0 tidak diputar. Hasil ShiftRows dapat dilihat pada tabel 8.

Tabel 9. Tabel Hexadecimal Hasil *ShiftRows*

8f	fb	92	fb
a3	d2	b6	8f
f3	a3	21	b6
63	9d	f3	9d

Setelah proses ShiftRows, proses dilanjutkan dengan proses MixCollums. Pada proses MixColumns, tiap kolom dari matriks state dilakukan operasi perkalian. Hal ini bertujuan untuk menyebarkan pengaruh setiap bit plaintext dan cipherkey terhadap ciphertext yang dihasilkan, pada arah kolom matriks state. Setiap kolom matriks state diperlakukan sebagai polinomial empat suku dalam Galois field, kemudian dikalikan dengan modulo $X^8 + X^4 + X^3 + X + 1$. Operasi MixColumns juga dapat dipandang sebagai perkalian matriks, dengan mengalikan empat bilangan di dalam Galois field MixColumns juga disebut sebagai proses mengalikan setiap kolom dengan matriks berikut

$$\begin{bmatrix} 2 & 3 & 1 & 1 \\ 1 & 2 & 3 & 1 \\ 1 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \end{bmatrix}$$

Proses MixCollums kemudian menghasilkan tabel hexadesimal seperti pada tabel 10.

Tabel 10. Tabel Hexadecimal Hasil MixCollumns

6b	be	2c	4c
bf	27	75	a2

74	c8	68	bf
1c	46	c7	0e

Setelah proses transformasi MixColumns, maka terdapat proses AddRoundKey dengan cara yang sama seperti sebelumnya, namun proses XOR nya dengan sub-key yang bersesuaian tiap iterasi yang terdapat pada key-expansion dengan melakukan ekspansi kunci. Sub-key yang digunakan pada proses round 1 dapat dilihat pada tabel 11.

Tabel 11. Tabel Hexadecimal Sub-Keys Round 1

34	04	34	04
36	06	36	06
37	07	37	07
30	00	30	00

Sub-keys kemudian di XOR kan dengan hasil dari MixCollums. Perhitungan XOR dapat dilihat seperti berkut :

6b XOR 34 = 01101011 XOR 00110100 = 01011111 = 5f

be XOR 04 = 10111110 XOR 00000100 = 10111010 = ba

2c XOR 34 = 00101100 XOR 00110100 = 00011000 = 18

4c XOR 04 = 01001100 XOR 00000100 = 01001000 = 48

bf XOR 36 = 10111111 XOR 00110110 = 10001001 = 89

27 XOR 06 = 00100111 XOR 00000110 = 00100001 = 21

75 XOR 36 = 01110101 XOR 00110110 = 01000011 = 43

a2 XOR 06 = 10100010 XOR 00000110 = 10100100 = a4

74 XOR 37 = 01110100 XOR 00110111 = 01000011 = 43

c8 XOR 07 = 11001000 XOR 00000111 = 11001111 = cf

68 XOR 37 = 01101000 XOR 00110111 = 01011111 = 5f

bf XOR 07 = 10111111 XOR 00000111 = 10111000 = b8

1c XOR 30 = 00011100 XOR 00110000 = 00101100 = 2c

46 XOR 00 = 01000110 XOR 00000000 = 01000110 = 46

c7 XOR 30 = 11000111 XOR 00110000 = 11110111 = f7

0e XOR 00 = 00001110 XOR 00000000 = 00001110 = 0e

Hasil AddRoundKey seperti pada tabel 12

Tabel 13. Tabel Hexadecimal hasil AddRoundKey Round 1

5f	ba	18	48
89	21	43	a4
43	cf	5f	b8

Tabel 14. Tabel Hexadecimal hasil AddRoundKey Round 1 (lanjutan)

2c	46	f7	0e

3. Round 2 Sampai Dengan Round 9

Pada proses round 2 sampai dengan round 9, proses yang dilakukan sama dengan round 1 pada AES-128 bit. Setiap round tersebut dimulai dengan SubBytes, kemudian dilanjutkan dengan proses ShiftRows, proses MixCollums dan proses AddRoundKey.

4. Round 10

Round 10 merupakan proses terakhir pada AES 128 bit. Berbeda dengan round 1 sampai dengan round 9, round 10 hanya memilki proses SubBytes, ShiftRows dan AddRoundKey tanpa adanya proses MixCollums. Proses ini kemudian menghasilkan ciphertext yang telah melalui algoritma AES. Hasil pada round 10 dapat dilihat pada tabel 5.10

Tabel 15. Tabel Hexadecimal Hasil Round 10

90	9e	27	f3
da	0d	44	3d
0b	e8	aa	60
bf	95	f6	fd

5. SIMPULAN

5.1 Kesimpulan

Berdasarkan hasil membuat sistem keamanan menggunakan metode AES pada sistem informasi akademik dapat ditarik kesimpulan sebagai berikut:

1. Dengan adanya sistem keamanan pada sistem informasi akademik SMPN 3 Bungku dapat membantu mengamankan data yang terdapat pada sistem informasi. Data tersebut kemudian dapat terhindarkan dari penyalahgunaan oleh pihak yang tidak berwenang

2. Pemakaian metode Advanced *Encryption Standard* (AES) ini dapat mengamankan data dengan tingkat keamanan yang tinggi.

5.2 Saran

Dari beberapa kesimpulan yang sudah dijelaskan, maka ada beberapa saran yang penulis sampaikan diantaranya:

1. Sistem keamanan dapat diimplementasikan juga untuk data pribadi siswa dan guru bukan hanya data nilai siswa.
2. Opsi pemilihan jenis AES dapat dihilangkan dan hanya menggunakan satu dari beberapa pilihan algoritma AES

DAFTAR PUSTAKA

Andrianto, P., & Nursikuwagus, A. (2017). *SistemInformasiPelayanan Kesehatan Berbasis Webdi Puskesmas.* Prosiding Seminar Nasional Komputer Dan Informatika , 978–602.

Budianto, W., Amini, S., & Ariyani, P. F. (2017). *Aplikasi Pengamanan Dokumen Digital Menggunakan Algoritma Kriptografi Advanced Encryptionstandard (Aes-128), Kompresi Huffmandan Steganografi End of File (EOF) Berbasis Desktop Pada Cv. Karya Perdana*. Prosiding Snatif Ke-4 Tahun 2017.

Budihartanti, C., Wijoyo, E. B., Nusa, S., & Jakarta, M. (2017). *Perancangan Aplikasi Enkripsi Data Menggunakan Metode Advanced Encryption Standard*. Konferensi Nasional Ilmu Sosial & Teknologi (KNiST), 165–171.

Lutfi, A. (2017). *Sistem Informasi Akademik Madrasah Aliyah Salafiyah Syafi'iyah Menggunakan PHP dan Mysql*. AiTech, 3(2), 104–112.

Nirmala, E. (2020). *Penerapan Steganografi File Gambar Menggunakan Metode Least Significant Bit (LSB) dan Algoritma Kriptografi Advanced Encryption Standard (AES) Berbasis Android.* Jurnal Informatika Universitas Pamulang, 5(1).

Nouvel, A., Purnama, W., & Putri, S. (2020). *Rancangan Sistim Informasi Reservasi Hotel Berbasis Web Pada Hotel Pandawa Syariah Purwokerto.* Journal Speed-Sentra Penelitian Engineering Dan Edukasi, 12(2).

Nuari, R., & Ratama, N. (2020). *Implementasi Algoritma Kriptografi AES (Advanced Encryption Standard) 128 Bit Untuk Pengamanan Dokumen* Shipping. Journal Of Artificial Intelligence and Innovative Applications, 1(2), 2716–1501.

Novianto, D., & Setiawan, Y. (2018). *Aplikasi Pengamanan Informasi Menggunakan Metode Least Significant Bit (LSB) dan Algoritma Kriptografi Advanced Encryption Standard (AES)*. Jurnal Ilmiah Informatika Global, 9(2).

Parinduri, I., & Hutagalung, S. N. (2018). Perangkaian Gerbang Logika Dengan Menggunakan Matlab (Simulink). JURTEKSI (Jurnal Teknologi dan Sistem Informasi), 5(1), 63-70.

Permana, A., & Nurnaningsih, D. (2018). *Rancangan Aplikasi Pengamanan Data Dengan Algoritma Advanced Encyption Standard (AES).* JURNAL TEKNIK INFORMATIKA, 11(2), 177–186.

Pradinata, P., & Syafrullah, M. (2018). *Keamanan Algoritma Kriptografi Database Menggunakan Metode Advanced Encryption Standard (AES-128) Berbasis Desktop.* Jurnal SKANIKA, *1*(2).

Prayudha, J., & dkk. (2019). *Implementasi Keamanan Data Gaji Karyawan Pada PT. Capella Medan Menggunakan Metode Advanced Encryption Standard (AES)*. Jurnal Sains Dan Komputer (SAINTIKOM), 18(2), 119–129.

Purnomo, D. (2017). Model Prototyping Pada Pengembangan Sistem Informasi. *JIMP-Jurnal Informatika Merdeka Pasuruan*, *2*(2), 54–61.

Simangunsong, A. (2018). *Sistem Informasi Pengarsipan Dokumen Berbasis Web*. Jurnal Mantik Penusa, 2(1), 11–19.

Soufitri, F. (2019). *Perancangan Data Flow Diagram Untuk Sistem Informasi Sekolah (Studi Kasus Pada SMP Plus Terpadu)*. Jurnal Ready Star 2, 2(1), 240–246.

Sitohang, H. T. (2018). *Sistem Informasi Pengagendaan Surat Berbasis Web Pada Pengadilan Tinggi Medan*. Journal Of Informatic Pelita Nusantara, 3(1).

Suranto, I., Suhery, C., & Brianorman, Y. (2017). *Pengembangan Aplikasi Chat Messenger Dengan Metode Advanced Encryption Standard (AES) Pada Smartphone*. Jurnal Coding Sistem Komputer Untan, 5(2).

Togatorop, P. R., dkk. (2021). *Pembangkit Entity Relationship Diagram Dari Spesifikasi Kebutuhan Menggunakan Natural Language Processing Untuk Bahasa Indonesia*. Jurnal Komputer Dan Informatika J-ICON, 9(2), 196–206.