

Penerapan Algoritma Vigenere Cipher Dan Aes Untuk Keamanan Biodata Siswa Baru Di SMK Tarbiyah Islamiyah

Implementation of Vigenere Cipher and AES Algorithms for the Security of New Student Biodata at SMK Tarbiyah Islamiyah

Tedy Agustawan^{a,1}, M. Irfan Aldy Nasution^{b,2}

^{a,b}Program Studi Informatika Universitas Potensi Utama

^{a,b}Universitas Potensi Utama, K.L. Yos Sudarso KM 6,5 No. 3A Tj. Mulia - Medan

Email tedyagustawan01@gmail.com¹, aldy.irfan16@gmail.com²

ABSTRAK

Kemajuan teknologi informasi telah mendorong penggunaan yang semakin luas dalam berbagai bidang, termasuk pendidikan. Namun, dampak negatifnya adalah meningkatnya risiko kebocoran data pribadi, terutama dalam konteks pendaftaran siswa baru di lembaga pendidikan. SMK Tarbiyah Islamiyah, sebagai salah satu lembaga pendidikan, juga menghadapi tantangan serupa. Penelitian ini bertujuan untuk mengatasi masalah keamanan data dengan menerapkan teknik kriptografi menggunakan metode Vigenere Cipher dan AES. Dengan mengenkripsi data pribadi siswa baru sebelum penyimpanan, risiko kebocoran dan penyalahgunaan data dapat diminimalkan. Berbagai penelitian terdahulu telah menunjukkan keefektifan metode ini dalam menjaga kerahasiaan data. Melalui implementasi metode ini, penelitian ini memberikan kontribusi dalam meningkatkan keamanan dan kerahasiaan data biodata siswa baru di SMK Tarbiyah Islamiyah. Diharapkan hasil penelitian ini dapat menjadi acuan bagi lembaga pendidikan lain dalam meningkatkan perlindungan data pribadi siswa. Selain itu, penelitian ini juga mengidentifikasi beberapa tantangan yang mungkin dihadapi dalam implementasi teknologi kriptografi di lingkungan pendidikan, serta memberikan rekomendasi untuk mengatasi tantangan tersebut. Dengan demikian, penelitian ini tidak hanya memiliki relevansi praktis dalam konteks keamanan data pendidikan, tetapi juga memberikan kontribusi teoritis terhadap literatur kriptografi dan perlindungan data.

Kata Kunci : Kriptografi, Vigenere Cipher, AES (Advanced Encryption Standard).

ABSTRACT

Advances in information technology have encouraged its increasingly widespread use in various fields, including education. However, the negative impact is the increased risk of personal data leakage, especially in the context of new student enrollment in educational institutions. Tarbiyah Islamiyah Vocational School, as an educational institution, also faces similar challenges. This research aims to overcome data security problems by applying cryptographic techniques using the Vigenere Cipher and AES methods. By encrypting new students' personal data before storage, the risk of data leakage and misuse can be minimized. Various previous studies have shown the effectiveness of this method in maintaining data confidentiality. Through the implementation of this method, this research contributes to increasing the security and confidentiality of new student biodata at Tarbiyah Islamiyah Vocational School. It is hoped that the results of this research can become a reference for other educational institutions in improving the protection of students' personal data. Apart from that, this research also identifies several challenges that may be faced in implementing cryptographic technology in an educational environment, and provides recommendations for overcoming these challenges. Thus, this research not only has practical relevance in the context of educational data security, but also makes a theoretical contribution to the cryptography and data protection literature.

Keywords : Cryptography, Vigenere Cipher, AES (Advanced Encryption Standard).

Info Artikel :

Disubmit : 10 Februari 2025

Direview: 16 Maret 2025

Diterima : 27 April 2025

Copyright © 2025 – Journal UPU. All rights reserved.

1. PENDAHULUAN

Kemajuan ilmu pengetahuan dan teknologi mendorong setiap individu, instansi, atau perusahaan untuk menggunakan teknologi sebagai alat bantu dalam menjalankan tugas dan pemecahan masalah. Namun, ancaman terhadap keamanan pesan dapat terjadi kapan saja, sehingga data rahasia memerlukan perlindungan agar tidak disalahgunakan oleh pihak yang tidak berwenang dan hanya dapat diakses oleh

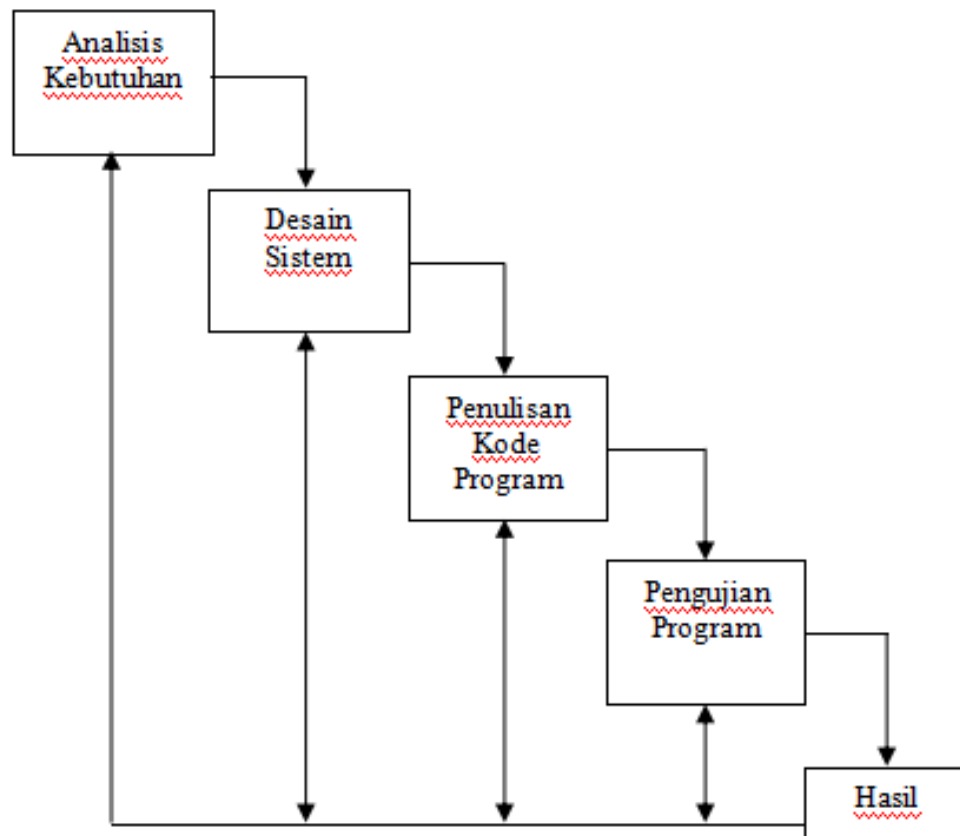
penerima yang sah [1]. SMK Tarbiyah Islamiyah, setiap tahun menerima pendaftaran siswa baru yang melibatkan data pribadi seperti formulir, akta kelahiran, kartu keluarga, dan foto. Sayangnya, sering terjadi kebocoran data pribadi calon siswa, yang berisiko disalahgunakan oleh pihak tidak bertanggung jawab. Data siswa tersebut belum memiliki sistem keamanan yang memadai, padahal keamanan merupakan aspek penting dalam sistem informasi. Namun, masalah keamanan seringkali kurang diperhatikan dan diprioritaskan dibanding tampilan atau aspek lainnya. Keamanan data adalah upaya perlindungan informasi digital dari akses, penggunaan, modifikasi, atau penyebaran yang tidak sah oleh pihak yang tidak berwenang. Tujuannya adalah menjaga kerahasiaan, integritas, dan ketersediaan data agar terhindar dari kebocoran, penyalahgunaan, atau serangan siber [2].

Untuk mengatasi permasalahan yang dihadapi maka peneliti menggunakan teknik kriptografi dengan digunakannya metode *Vigenere Cipher* Dan AES. Kriptografi adalah ilmu dan teknik mengamankan informasi dengan mengubah data menjadi bentuk tersandi (*ciphertext*) yang hanya dapat dibaca oleh pihak yang memiliki kunci dekripsi yang sah. Tujuannya adalah menjaga kerahasiaan, integritas, dan keaslian data dari ancaman seperti penyadapan atau manipulasi [3]. Enkripsi adalah proses mengubah data asli (*plaintext*) menjadi bentuk tersandi (*ciphertext*) menggunakan algoritma dan kunci tertentu, sehingga hanya pihak yang memiliki kunci dekripsi yang sah dapat mengembalikannya ke bentuk awal. Tujuannya untuk melindungi kerahasiaan data dari akses tidak sah [4]. Sedangkan Deskripsi adalah proses mengubah data yang telah dienkripsi (*ciphertext*) kembali ke bentuk aslinya (*plaintext*) menggunakan kunci dekripsi yang sesuai. Tujuannya adalah memulihkan informasi agar dapat dibaca dan dipahami oleh pihak yang berwenang [5]. *Vigenere Cipher* adalah metode enkripsi klasik yang menggunakan teknik substitusi alfabet berbasis kunci untuk menyamarkan pesan (*plaintext*). Berbeda dengan Caesar Cipher yang hanya menggeser huruf dengan nilai tetap, *Vigenere Cipher* menggeser setiap karakter *plaintext* sesuai urutan huruf kunci yang berulang, sehingga meningkatkan kerumitan pemecahan (*cracking*) [6]. *Vigenere Cipher* adalah metode enkripsi klasik yang menggunakan kunci kata/frase untuk menggeser setiap huruf *plaintext* secara variatif (*polialfabetik*), sehingga menghasilkan *ciphertext* yang lebih aman dibanding *cipher* substitusi sederhana seperti Caesar Cipher [7]. AES (*Advanced Encryption Standard*) adalah algoritma enkripsi simetrik modern yang menggunakan blok 128-bit dengan kunci 128/192/256-bit, dirancang untuk menggantikan DES dengan keamanan dan efisiensi lebih tinggi [8]. AES merupakan sistem kriptografi blok unggulan yang menerapkan proses substitusi (*SubBytes*), permutasi (*ShiftRows*), pencampuran (*MixColumns*), dan penambahan kunci (*AddRoundKey*) dalam *multiple round* untuk mengamankan data sensitive [9]. *Advanced Encryption Standard* adalah skema enkripsi simetris yang tahan terhadap serangan *brute-force*, digunakan secara global untuk proteksi data militer, finansial, dan komunikasi digital karena kecepatan eksekusi dan keandalannya [10].

Beberapa penelitian terdahulu yang mengangkat metode yang sama dapat dijelaskan sebagai berikut. Penelitian yang mengangkat judul “Implementasi Algoritma Kriptografi Aes 128 Dan *Vigenere Cipher* Pada Coffee Shop Ngopi Dengan Aplikasi Berbasis Web”. Hasil penelitiannya menjelaskan kombinasi algoritma *Vigenere Cipher* dan AES-128 dengan autentikasi MD5 berhasil mengamankan data kedai kopi NgoPi [11]. Penelitian yang mengangkat judul “Kriptografi Teks Berbasis Algoritma Substitusi *Vigenere Cipher* 8 Bit”. Penelitian menunjukkan *Vigenere Cipher* efektif mengamankan teks ASCII dengan *Avalanche Effect* >50%, CER/BER 0, dan entropi yang meningkat seiring kompleksitas *plaintext*. Hasil ini membuktikan keandalan algoritma tersebut dalam enkripsi data teks [12]. Penelitian yang mengangkat judul “Implementasi Algoritma *Vigenere Cipher* Dan *Advanced Encryption Standard* (Aes) Untuk Keamanan Data Teks”. Penelitian ini mengembangkan sistem keamanan data dengan mengkombinasikan *Vigenere Cipher* (kriptografi klasik) dan AES (kriptografi modern) untuk mengamankan pesan teks [13]. Penelitian yang mengangkat judul “Enkripsi Database Sistem Informasi Helpdesk Dengan Algoritma Kriptografi AES-128 dan *Vigenere Cipher*”. Penelitian ini mengimplementasikan kombinasi kriptografi simetris AES dan *Vigenere* untuk mengamankan database, guna mencegah penyalahgunaan data oleh pihak tak berwenang [14]. Penelitian yang mengangkat judul “Implementasi Sistem Keamanan Dokumen Kepegawaian Menggunakan Metode Aes-256 Dan *Vigenere Cipher*”. Hasil pengujian membuktikan sistem berhasil mengenkripsi/dekripsi data, memastikan hanya pihak berwenang dengan kunci yang dapat mengakses dokumen, sehingga mencegah penyalahgunaan oleh oknum tak bertanggung jawab [15]. Sedangkan hasil dari penelitian peneliti adalah membantu SMK Tarbiyah Islamiyah dalam menjaga keamanan dan kerahasiaan data Biodata Siswa Baru dengan menerapkan metode *Vigenere Cipher* Dan AES, sehingga dengan demikian data biodata siswa tidak disalahgunakan oleh pihak yang tidak berwenang.

2. METODE

Model *Waterfall* adalah metodologi pengembangan perangkat lunak yang bersifat *linier* dan *sekuensial*, di mana setiap *fase* (seperti analisis, desain, implementasi, pengujian, dan pemeliharaan) harus diselesaikan sepenuhnya sebelum melanjutkan ke *fase* berikutnya.



Gambar 1. Kerangka Waterfall

Keterangan :

1. Analisis Kebutuhan

Pada tahapan ini merupakan analisa terhadap kebutuhan yang diperlukan untuk mencapai tujuan penelitian yang akan dilakukan yaitu data biodata siswa baru pada SMK Tarbiyah Islamiyah.

2. Desain Sistem

Desain sistem yang digunakan dalam teori adalah pemodelan UML yaitu *use case diagram*, *class diagram*, *activity diagram* dan *sequence diagram*.

3. Tools

Pada tahapan ini peneliti menggunakan *web browser* dengan menggunakan PHP. Peneliti menggunakan *hardware* komputer/laptop. *Database* yang digunakan adalah MySQL.

4. Pengujian

Pada tahapan ini peneliti menguji sistem yang telah dibuat menggunakan pengujian teori dan praktek. Pengujian teori peneliti menggunakan *blackbox testing* dan pengujian praktek peneliti menggunakan *localhost*.

5. Hasil

Pada tahapan ini penelitian sudah selesai dibuat, hasil dari penelitian ini yaitu Implementasi Penerapan Algoritma Vigenere Cipher Dan AES Untuk Keamanan Biodata Siswa Baru Di SMK Tarbiyah Islamiyah.

3. HASIL DAN PEMBAHASAN

Bagian ini menyajikan temuan utama penelitian beserta analisisnya. Hasil implementasi sistem keamanan data akan dipaparkan secara ringkas, dilanjutkan dengan pembahasan efektivitas metode kriptografi yang digunakan dalam memenuhi tujuan penelitian.

3.1. Pembahasan Algoritma Vigenere Cipher Dan AES

Adapun Langkah-langkah penyelesaian Algoritma Vigenere Cipher Dan AES dapat dijelaskan sebagai berikut :

1. Enkripsi

Contoh perhitungan enkripsi algoritma *Vigenere Cipher* dan AES dapat dilihat pada proses di bawah ini.

Plaintext	A	I	S	Y	A	H	I	N	D	A	H	S	A	R	I
Key	T	E	D	Y	I	T	P	R	O	D	I	T	I	I	F

Langkah pertama yang dilakukan adalah mengubah plaintext dan kunci diatas menjadi bentuk desimal. Hasil konversi plaintext dan kunci diatas adalah sebagai berikut :

Plaintext	65	73	83	89	65	72	73	78	68	65	72	83	65	82	73
Key	84	69	68	89	73	84	80	82	79	68	73	84	73	73	70

Tabel 1 Perhitungan Enkripsi Vigenere Cipher Nama Lengkap

Cipher	Pi	+	Ki	Perhitungan	Hasil
C1	65	+	84	Mod 256	•
C2	73	+	69	Mod 256	Ž
C3	83	+	68	Mod 256	—
C4	89	+	89	Mod 256	²
C5	65	+	73	Mod 256	Š
C6	72	+	84	Mod 256	œ
C7	73	+	80	Mod 256	™
C8	78	+	82	Mod 256	á
C9	68	+	79	Mod 256	“
C10	65	+	68	Mod 256	...
C11	72	+	73	Mod 256	‘
C12	83	+	84	Mod 256	§
C13	65	+	73	Mod 256	Š
C14	82	+	73	Mod 256	›
C15	73	+	70	Mod 256	

Setelah selesai melakukan perhitunagn algoritma *Vigenere Cipher* ,selanjutnya dilakukan perhitungan enkripsi algoritma AES dapat dilihat pada proses di bawah ini.

Plaintext	•	Ž	—	²	Š	œ	™	á	“	...	‘	§	Š	›	
Key	T	E	D	Y	I	T	P	R	O	D	I	T	I	I	F

Langkah selanjutnya yang dilakukan adalah mengubah plaintext dan kunci diatas menjadi bentuk heksadesimal. Hasil konversi plaintext dan kunci diatas adalah sebagai berikut.

Plaintext	95	8E	97	B2	8A	9C	99	E1	93	85	91	A7	8A	9B	8F
Key	54	45	44	59	49	54	50	52	AF	44	49	54	49	49	46

Selanjutnya dilakukan perhitungan xor antara Plaintext dan Key, adapun penjelasannya dapat dijelaskan sebagai berikut.

Tabel 2 Xor Antara Plaintext Dan Key Nama Lengkap

95	8A	93	8A	xor	54	49	4F	49	=	C1	C3	DC	C3
8E	9C	85	9B		45	54	44	49		CB	C8	C1	D2
97	99	91	8F		44	50	49	46		D3	C9	D8	C9
B2	E1	A7	0		59	52	54	0		EB	B3	F3	0

Tahapan enkripsi algoritma kriptografi AES terdiri dari empat proses yaitu SubBytes, ShiftRows, MixColumns dan AddRoundKey. Sebelum melakukan enkripsi perlu dilakukan ekspansi atau

pembangkitan kunci, hal ini bertujuan untuk mendapatkan kunci ronde atau round key yang akan digunakan pada tahap transformasi AddRoundKey.

a. Ekspansi Kunci

Algoritma AES menggunakan *cipher key* dan membuat suatu ekspansi kunci untuk menghasilkan suatu *key schedule*.

Tabel 3 Ekspansi Kunci AES Nama Lengkap

54	49	4F	49	6E	27	68	21	34	13	7B	5A	6	15	6E	34
45	54	44	49	1F	4B	F	46	A3	E8	E7	A1	5F	B7	50	F1
44	50	49	46	27	77	3E	78	64	13	2D	55	1D	E	23	76
59	52	54	0	62	30	64	64	9F	AF	CB	AF	21	8E	45	EA
Round 0				Round 1				Round 2				Round 3			
A7	B2	DC	E8	4	B6	6A	82	B6	0	6A	E8	8C	8C	E6	E
67	D0	80	71	1F	CF	4F	3E	1C	D3	9C	A2	6	D5	49	EB
9A	94	B7	C1	37	A3	14	D5	21	82	96	43	44	C6	50	13
39	B7	F2	18	A2	15	E7	FF	B1	A4	43	BC	2A	8E	CD	71
Round 4				Round 5				Round 6				Round 7			
65	E9	F	1	9B	72	7D	7C	B9	CB	B6	CA				
7B	AE	E7	C	D1	7F	98	94	BD	C2	5A	CE				
E7	21	71	62	8A	AB	DA	B8	66	CD	17	AF				
81	F	C2	B3	FD	F2	30	83	ED	1F	2F	AC				
Round 8				Round 9				Round 10							

Proses tahapan SubBytes, ShiftRows, MixColumns dan AddRoundKey enkripsi algoritma AES 256-bit dapat dilihat pada tabel Berikut.

b. Tahapan SubBytes

Tahapan ini menggunakan hasil dari Xor Antara Plaintext Dan Key, selanjutnya akan dicocokkan dengan tabel s-box, adapapun penjelasannya dapat dijelaskan sebagai berikut.

Tabel 4 SubBytes Nama Lengkap

C1	C3	DC	C3
CB	C8	C1	D2
D3	C9	D8	C9
EB	B3	F3	0

=

78	2E	86	2E
1F	E8	78	B5
66	DD	61	DD
E9	89	0D	63

c. Tahapan ShiftRows

Tahapan ini melakukan pergeseran sesuai dengan ketentuan ShiftRows, adapapun penjelasannya dapat dijelaskan sebagai berikut.

Tabel 5 ShiftRows Nama Lengkap

0←	78	2E	86	2E
1←	1F	E8	78	B5
2←	66	DD	61	DD
3←	E9	89	0D	63

=

78	2E	86	2E
E8	78	B5	1F
61	DD	66	DD
63	E9	89	0D

d. Tahapan MixColumns

Tahapan ini melakukan perkalian matriks 4x4, adapapun penjelasannya dapat dijelaskan sebagai berikut.

Tabel 6 MixColumns Nama Lengkap

78	2E	86	2E
E8	78	B5	1F
61	DD	66	DD
63	E9	89	0D

x

2	3	1	1
1	2	3	1
1	1	2	3
3	1	1	2

=

35	36	35	36
38	31	39	39
31	31	31	31
36	39	31	37

e. Tahapan AddRoundKey

Tahapan ini melakukan xor addRoundKey1 dengan hasil MixColumns, adapapun penjelasannya dapat dijelaskan sebagai berikut.

Tabel 7 AddRoundKey Nama Lengkap

35	36	35	36	xor	6E	27	68	21	=	5B	11	5D	17
38	31	39	39		1F	4B	F	46		27	7A	36	7F
31	31	31	31		27	77	3E	78		16	46	F	49
36	39	31	37		62	30	64	64		54	9	55	53

f. Tahapan Enkripsi

Tahapan ini adalah proses akhir untuk algoritma AES, tahapan SubBytes, ShiftRows, MixColumns dan AddRoundKey dilakukan proses perulangan sebanyak 10 kali round, adapun hasil ya dapat dijelaskan sebagai berikut.

Tabel 8 Keseluruhan Proses Enkripsi Algoritma AES 256-bit Nama Lengkap

R	78	2E	86	2E	78	2E	86	2E	35	36	35	36	5B	11	5D	17
O	1F	E8	78	B5	E8	78	B5	1F	38	31	39	39	27	7A	36	7F
U	66	DD	61	DD	61	DD	66	DD	31	31	31	31	16	46	F	49
N	E9	89	0D	63	63	E9	89	0D	36	39	31	37	54	9	55	53
D 1	SubBytes				ShiftRows				MixColumns				AddRoundKey			

R	39	82	4C	F0	39	82	4C	F0	31	37	38	38	5	24	43	62
O	CC	DA	5	D2	DA	5	D2	CC	31	31	38	31	92	D9	DF	90
U	47	5A	76	3B	76	3B	47	5A	36	36	35	35	52	25	18	60
N	20	1	FC	ED	ED	20	77	FC	31	31	38	31	AE	9E	F3	9E
D 2	SubBytes				ShiftRows				MixColumns				AddRoundKey			

R	6B	36	1A	AA	6B	36	1A	AA	38	36	34	35	3E	23	5A	1
O	4F	35	9E	60	35	9E	60	4F	35	36	37	36	6A	81	67	C7
U	0	3F	AD	D0	AD	D0	0	3F	37	39	38	35	2A	37	1B	43
N	E4	B	BB	46	46	E4	B	BB	39	38	39	37	18	B6	7C	DD
D 3	SubBytes				ShiftRows				MixColumns				AddRoundKey			

R	B2	26	BE	7C	B2	26	BE	7C	39	39	37	31	9E	8B	EB	D9
O	2	C	85	C6	C	85	C6	2	33	35	38	37	54	E5	B8	46
U	E5	9A	AF	1A	AF	1A	E5	9A	31	39	38	31	AB	AD	8F	F0
N	AD	4E	10	C1	C1	AD	4E	10	36	31	38	36	F	86	CA	2E
D 4	SubBytes				ShiftRows				MixColumns				AddRoundKey			

R	B	3D	E9	35	B	3D	E9	35	34	34	37	38	30	82	5D	BA
O	20	D9	6C	5A	D9	6C	5A	20	37	39	37	36	28	F6	78	8
U	62	95	73	8C	73	8C	62	95	39	38	38	38	E	9B	2C	ED
N	76	44	74	31	31	76	44	74	36	35	36	36	94	20	D1	C9
D 5	SubBytes				ShiftRows				MixColumns				AddRoundKey			

R	4	13	4C	F4	4	13	4C	F4	38	33	34	37	8E	33	5E	DF
O	34	42	BC	30	42	BC	30	34	35	36	37	35	29	E5	AB	97
U	AB	14	71	55	71	55	AB	14	35	37	37	37	14	B5	A1	74
N	22	B7	3E	DD	DD	22	B7	3E	38	39	37	39	89	9D	74	85
D 6	SubBytes				ShiftRows				MixColumns				AddRoundKey			

R	19	C3	58	9E	19	C3	58	9E	38	37	39	38	B4	BB	DF	36
O	A5	D9	62	88	D9	62	88	A5	31	31	39	31	37	E4	70	DA
U	FA	D5	32	92	32	92	FA	D5	31	39	31	31	75	FF	61	22
N	A7	5E	92	97	97	A7	5E	92	31	31	39	38	1B	BF	F4	49
D 7	SubBytes				ShiftRows				MixColumns				AddRoundKey			

R	8D	EA	9E	5	8D	EA	9E	5	36	31	31	38	53	D8	3E	39
O	9A	69	51	57	69	51	57	9A	38	37	36	37	43	99	D1	3B
U	9D	16	EF	93	EF	93	9D	16	38	31	31	39	DF	10	40	5B
N	AF	8	BF	3B	3B	AF	8	BF	38	37	37	36	B9	38	F5	85
D 8	SubBytes				ShiftRows				MixColumns				AddRoundKey			

R	ED	61	B2	12	ED	61	B2	12	38	31	39	39	A3	43	44	45
O	1A	EE	3E	E2	EE	3E	E2	1A	38	31	39	31	E9	4E	A1	A5
U	9E	CA	9	39	9	39	9E	CA	38	35	36	39	B2	9E	EC	81
N	56	7	E6	97	97	56	7	E6	31	38	36	37	CC	CA	6	B4
D 9	SubBytes				ShiftRows				MixColumns				AddRoundKey			

R	A	1A	1B	6E	A	1A	1B	6E	B3	D1	AD	A4
O	1E	2F	32	6	2F	32	6	1E	92	F0	5C	D0
U	37	B	CE	C	CE	C	37	B	A8	C1	20	A4
N	4B	74	6F	8D	8D	4B	74	6F	60	54	5B	C3
D 10	SubBytes				ShiftRows				AddRoundKey			

Tabel III. 9 Output Nama Lengkap

B3	D1	AD	A4	42	44	41	41	*	,	)	)
92	F0	5C	D0	39	46	35	44	'	.	#	,
A8	C1	20	A4	41	43	32	41	)	+		)
60	54	5B	C3	36	35	35	43	\$	#	#	+
AddRoundKey				Desimal				Chipertext			

Sehingga dapat disimpulkan untuk hasil output ya dapat dijelaskan sebagai berikut :

Plaintext A I S Y A H I N D A H S A R I
Chipertext * ') \$, . + #) # #) ,) +

2. Deskripsi

Contoh perhitungan deskripsi algoritma Vigenere Cipher dan AES dapat dilihat pada proses di bawah ini.

Plaintext * ') \$, . + #) # #) ,) +
Key T E D Y I T P R O D I T I I F

Transformasi cipher dapat dibalikkan dan diimplementasikan dalam arah yang berlawanan untuk menghasilkan inverse cipher yang mudah dipahami untuk algoritma AES. Transformasi byte yang digunakan pada invers cipher adalah InvShiftRows, InvSubBytes, InvMixColumns, dan AddRoundKey. Algoritma dekripsi dapat dilihat pada skema berikut ini :

a. InvShiftRows

InvShiftRows adalah transformasi byte yang berkebalikan dengan transformasi ShiftRows. Pada transformasi InvShiftRows, dilakukan pergeseran bit ke kanan sedangkan pada ShiftRows dilakukan pergeseran bit ke kiri. Ilustrasi transformasi InvShiftRows terdapat pada berikut :

Tabel 10 InvShiftRows Nama Lengkap

0→	78	2E	86	2E	=	78	2E	86	2E
1→	E8	78	B5	1F		1F	E8	78	B5
2→	61	DD	66	DD		66	DD	61	DD
3→	63	E9	89	0D		E9	89	0D	63

b. InvSubBytes

InvSubBytes juga merupakan transformasi bytes yang berkebalikan dengan transformasi SubBytes. Pada InvSubBytes, tiap elemen pada state dipetakan dengan menggunakan tabel Inverse S-Box:

Hex	Y															
	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
X	0	52	09	6a	d5	30	36	a5	38	bf	40	a3	9e	81	f3	d7
	1	7c	E3	39	82	9b	2f	ff	87	34	8e	43	44	c4	de	e9
	2	54	7b	94	32	a6	c2	23	3d	ee	4c	95	0b	42	fa	c3
	3	08	2e	a1	66	28	d9	24	b2	76	5b	a2	49	6d	8b	d1
	4	72	f8	f6	64	86	68	98	16	d4	a4	5c	cc	5d	65	b6
	5	6c	70	48	50	fd	ed	b9	da	5e	15	46	57	a7	8d	9d
	6	90	d8	ab	00	8c	bc	d3	0a	17	e4	58	05	b8	b3	45
	7	d0	2c	1e	8f	ca	3f	0f	02	c1	af	bd	03	01	13	8a
	8	3a	91	11	41	4f	67	dc	ea	97	f2	cf	ce	f0	b4	e6
	9	96	ac	74	22	e7	ad	35	85	e2	f9	37	e8	1c	75	df
	a	47	f1	1a	71	1d	29	c5	89	6f	b7	62	0e	aa	18	be
	b	fc	56	3e	4b	c6	d2	79	20	9a	db	e0	fe	78	ed	5a
	c	1f	dd	a8	33	88	07	c7	31	b1	12	10	59	27	80	ec
	d	60	51	7f	a9	19	b5	4a	0d	2d	e5	7a	9f	93	e9	9c
	e	a0	e0	3b	4d	ae	2a	f5	b0	c8	eb	bb	3c	83	53	99
	f	17	2b	04	7e	ba	77	d6	26	e1	69	14	63	55	21	0c

Gambar 2. Tabel Inverse S-Box

Tabel 11 InvSubBytes Nama Lengkap

78	2E	86	2E	=	C1	C3	DC	C3
1F	E8	78	B5		CB	C8	C1	D2
66	DD	61	DD		D3	C9	D8	C9
E9	89	0D	63		EB	B3	F3	0

c. Inverse AddRoundKey

Transformasi Inverse AddRoundKey tidak berbeda dengan transformasi AddRoundkey karena dalam transformasi ini hanya dilakukan operasi penambahan sederhana dengan operasi bitwise XOR.

Tabel 12 InvAddRoundKey Nama Lengkap

C1	C3	DC	C3
CB	C8	C1	D2
D3	C9	D8	C9
EB	B3	F3	0

d. InvMixColumns

Setiap kolom dalam state dikalikan dengan matrik perkalian dalam AES. Perkalian dalam matrik dapat dituliskan :

Tabel 13 InvMixColumns Nama Lengkap

95	8A	93	8A
8E	9C	85	9B
97	99	91	8F
B2	E1	A7	0

54	49	4F	49
45	54	44	49
44	50	49	46
59	52	54	0

bitwise

C1	C3	DC	C3
CB	C8	C1	D2
D3	C9	D8	C9
EB	B3	F3	0

Plaintext	95	8E	97	B2	8A	9C	99	E1	93	85	91	A7	8A	9B	8F
Key	54	45	44	59	49	54	50	52	AF	44	49	54	49	49	46

Langkah pertama yang dilakukan adalah mengubah heksadesimal dan kunci diatas menjadi bentuk plaintext. Hasil konversi plaintext dan kunci diatas adalah sebagai berikut.

Plaintext • Ž — ² Š œ ™ á “ ... ‘ § Š ›
Key T E D Y I T P R O D I T I I F

Setelah selesai melakukan perhitunagn algoritma AES, selanjutnya dilakukan perhitungan deskripsi algoritma *Vigenere Cipher* dapat dilihat pada proses di bawah ini.

Tabel 14 Perhitungan Deskripsi Vigenere Cipher Nama Lengkap

Cipher	Pi	-	Ki
C1	65	-	84
C2	73	-	69
C3	83	-	68
C4	89	-	89
C5	65	-	73
C6	72	-	84
C7	73	-	80
C8	78	-	82
C9	68	-	79
C10	65	-	68
C11	72	-	73
C12	83	-	84
C13	65	-	73
C14	82	-	73
C15	73	-	70

Langkah selanjutnya yang dilakukan adalah mengubah desimal dan kunci diatas menjadi bentuk plaintext. Hasil konversi plaintext dan kunci diatas adalah sebagai berikut :

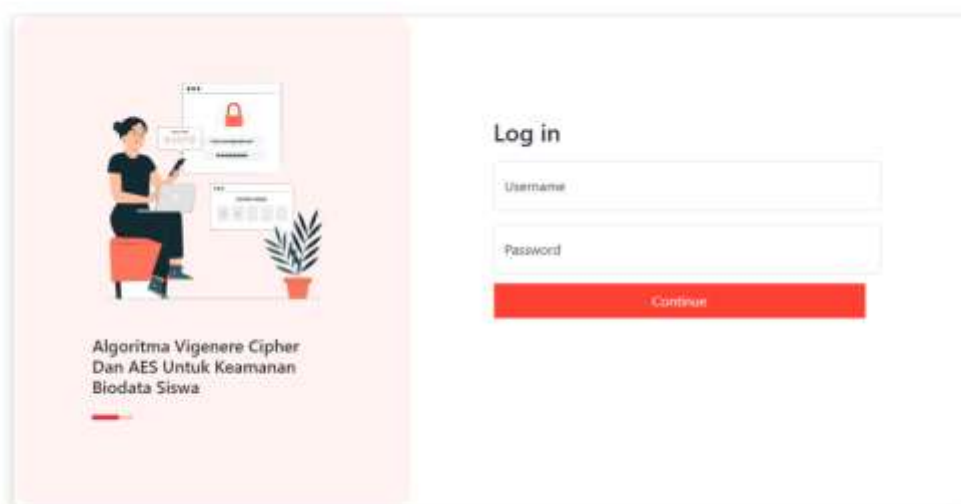
Plaintext A I S Y A H I N D A H S A R I
Key T E D Y I T P R O D I T I I F

3.2. Tampilan Hasil Aplikasi

Berikut ini dijelaskan tentang tampilan hasil dari perancangan sistem yang dibangun dapat dilihat sebagai berikut:

1. Tampilan Menu *Login*

Tampilan menu *login* pada sistem terlihat pada gambar berikut :



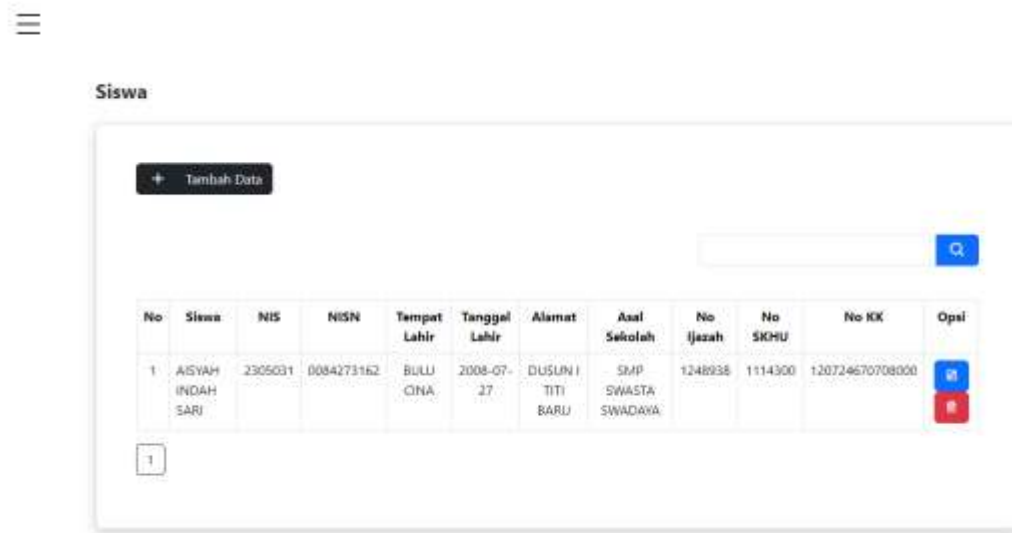
Gambar 3 Tampilan Menu *Login*

Keterangan pada menu *login* digunakan untuk masuk kesistem, menu *login* ini menggunakan tabel akun. Menu *login* ini digunakan oleh admin. Jika *username* dan *password* valid dengan *database* maka user

akan berhasil login, jika sebalik ya *username* dan *password* invalid dengan *database* maka sistem akan memberikan notif pesan gagal *login*.

2. Tampilan Data Siswa

Tampilan data siswa pada sistem terlihat pada gambar berikut :

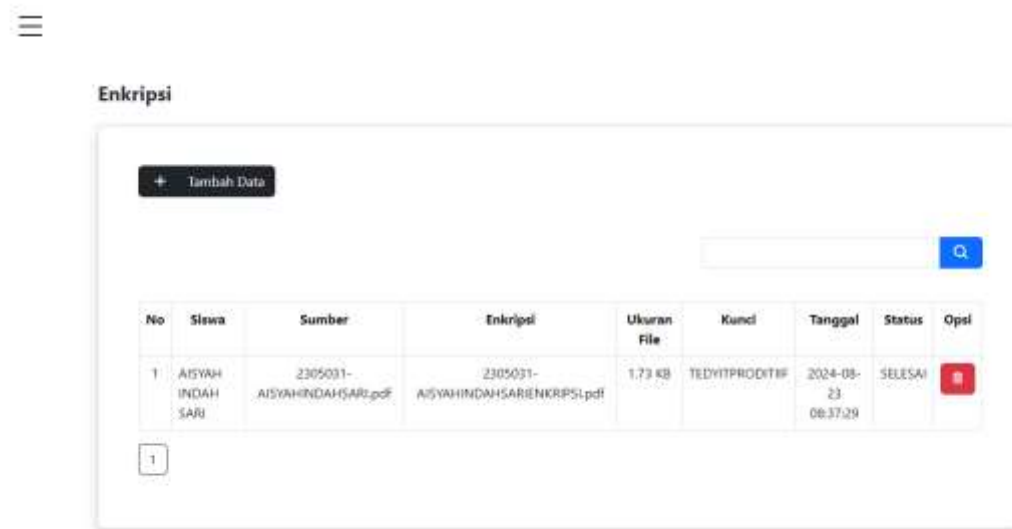


Gambar 4 Tampilan Data Siswa

Keterangan pada menu data bonus, menu yang digunakan untuk menampung data siswa, didalam menu ini memiliki 3 opsi yaitu tambah data untuk melakukan tambah data siswa, ubah data untuk melakukan perubahan data pada data siswa, dan data hapus data digunakan untuk menghapus data siswa. Menu ini hanya dapat diakses oleh admin.

3. Tampilan Data Enkripsi

Tampilan data enkripsi pada sistem terlihat pada gambar berikut :

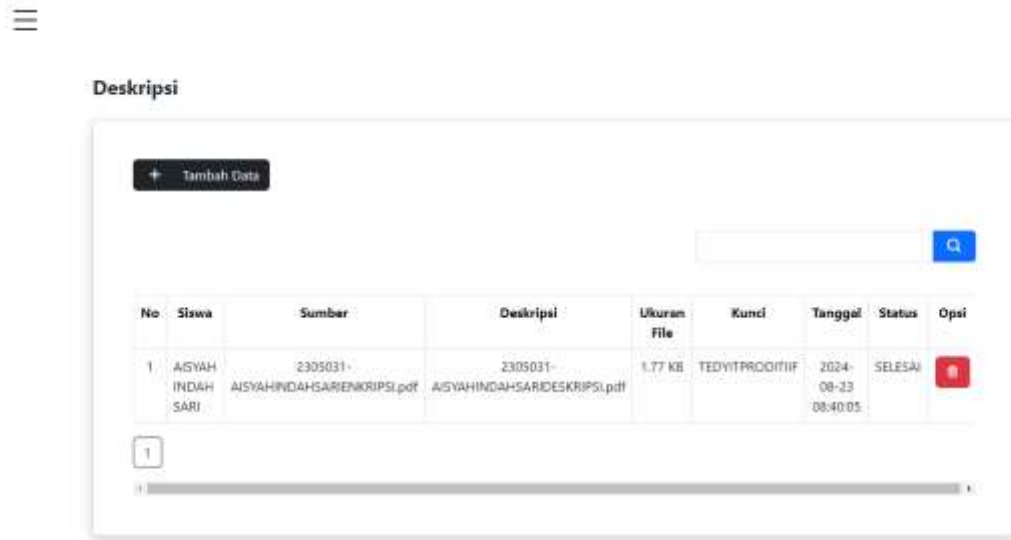


Gambar 5 Tampilan Data Enkripsi

Keterangan pada menu data enkripsi, menu yang digunakan untuk menampung data enkripsi, didalam menu ini memiliki 2 opsi yaitu tambah data untuk melakukan tambah data enkripsi, dan data hapus data digunakan untuk menghapus data enkripsi. Menu ini hanya dapat diakses oleh admin.

4. Tampilan Data Deskripsi

Tampilan data deskripsi pada sistem terlihat pada gambar berikut :



Gambar 6 Tampilan Data Deskripsi

Keterangan pada menu deskripsi digunakan untuk menampung data deskripsi, menu ini memiliki 2 opsi, yaitu tambah data digunakan untuk menambah data, dan hapus data digunakan untuk menghapus data. Menu ini dapat diakses oleh admin.

4. KESIMPULAN

Berdasarkan penelitian yang telah dilakukan peneliti menarik beberapa kesimpulan:

1. Implementasi algoritma Vigenere Cipher dan AES berhasil meningkatkan keamanan data pribadi siswa baru di SMK Tarbiyah Islamiyah.
2. Kombinasi dua algoritma enkripsi, Vigenere Cipher dan AES, memberikan lapisan keamanan tambahan, sehingga informasi sensitif seperti biodata siswa dapat terlindungi dengan lebih baik, meskipun memerlukan waktu proses yang sedikit lebih lama.
3. Dengan enkripsi pada data yang diinput, SMK Tarbiyah Islamiyah dapat menjaga privasi siswa baru secara optimal, memberikan rasa aman bagi pihak yang terlibat dalam proses pendaftaran..

UCAPAN TERIMA KASIH

Penulis mengucapkan terima kasih yang tulus kepada Universitas Potensi Utama atas segala bantuan yang telah diberikan dalam penyelesaian karya tulis ilmiah ini.

REFERENSI

- [1] Setiawan, A., Nasution, M. I. A., Rustam, M. T., & Dewi, R. (2024). Keamanan Siber Untuk Melindungi Umkm Mikro Dari Ancaman Keamanan Digital. *CORAL (Community Service Journal)*, 3(2), 82-91.

- [2] Latiep, A., & Syahputri, N. (2024). Rancang Bangun Aplikasi Keamanan Data Penjualan Berbasis Web Menggunakan Metode Caesar Cipher Dan Base64 Pada Pabrik Tahu SS. *Jurnal Info Digit (JID)*, 2(3), 952-964.
- [3] Azhar, A. H., Destari, R. A., Negoro, W. S., & Ardansyah, A. (2024). Pelatihan Teknik Caesar Cipher Terhadap Keamanan Informasi. *Jurnal TUNAS*, 5(2), 88-92.
- [4] Harris, F., & Sari, R. E. (2024). Meningkatkan Keamanan Source Code Web Melalui Teknik Enkripsi dan Dekripsi Dengan Metode Reverse Cipher dan Caesar Cipher. *Jurnal Info Digit (JID)*, 2(1), 405-417.
- [5] Parhusip, S. L., & Sari, R. E. (2024). Pesan yang Dirahasiakan Menggunakan Algoritma Feal dan Caesar Cipher Disisipkan ke Dalam Gambar Menggunakan Metode Least Signifigan Bit (LSB). *Jurnal Info Digit (JID)*, 2(2), 694-708.
- [6] Asih, M. S., Rismayanti, R., Fadhlurahman, M. I., & Hasibuan, A. Z. (2025). Pengembangan Algoritma Vigenere Cipher Berbasis Kunci Dinamis Dalam Pengamanan Pesan Teks. *Jurnal Ilmu Komputer dan Sistem Informasi*, 4(1), 92-99.
- [7] Hidayah, V. M., Mulyana, D. I., & Bachtiar, Y. (2023). Algoritma Caesar cipher atau Vigenere cipher pada pengenkripsian pesan teks. *Journal on Education*, 5(3), 8563-8573.
- [8] Cristy, N., & Riandari, F. (2021). Implementasi Metode Advanced Encryption Standard (AES 128 Bit) Untuk Mengamankan Data Keuangan. *Jurnal Ilmu Komputer dan Sistem Informasi (JIKOMSI)*, 4(2), 75-85.
- [9] Sianipar, J. S., Nugroho, N. B., & Mariami, I. (2024). Pengamanan Data Gaji Karyawan Dengan Menggunakan Metode Advanced Encryption Standard (AES). *Jurnal Sistem Informasi Triguna Dharma (JURSI TGD)*, 3(1), 35-45.
- [10] Ananda, S. P., & Lukman, S. (2022). Analisa Metode Kriptografi Modern Advance Encryption Standard (AES) 128 Bit dalam Mengenkripsi dan Mendekripsi File Dokumen Digital: Array. *Jurnal Ilmiah Komputasi*, 21(3), 333-344.
- [11] Syahrani, F. N., & Pramusinto, W. (2024, September). IMPLEMENTASI ALGORITMA KRIPTOGRAFI AES 128 DAN VIGENERE CIPHER PADA COFFEE SHOP NGOPI DENGAN APLIKASI BERBASIS WEB. In *Prosiding Seminar Nasional Mahasiswa Fakultas Teknologi Informasi (SENAFTI)* (Vol. 3, No. 2, pp. 74-81).
- [12] Karima, N. A., Aisyah, A. N., Silla, H. V., Handoko, L. B., & Sani, R. R. (2024). Kriptografi Teks Berbasis Algoritma Substitusi Vigenere Cipher 8 Bit. *Jurnal Masyarakat Informatika*, 15(1), 1-13.
- [13] Devi, L. P. (2023). Implementasi Algoritma Algoritma Vigenere Cipher Dan Advanced Encryption Standart (Aes) Untuk Keamanan Data Teks. *Bulletin Information Systems*, 1(1), 25-29.
- [14] Ruswandi, M. A., & Windarto, W. (2022). Enkripsi Database Sistem Informasi Helpdesk Dengan Algoritme Kriptografi AES-128 dan Vigenere Cipher. *SKANIKA: Sistem Komputer dan Teknik Informatika*, 5(2), 240-254.
- [15] Adam, P., & Romli, M. A. (2024). IMPLEMENTASI SISTEM KEAMANAN DOKUMEN KEPEGAWAIAN MENGGUNAKAN METODE AES-256 DAN VIGENERE CHIPER. *Jurnal Komputer dan Teknologi*, 3(1), 20-26.