Laporan Praktikum Keamanan Data: Struktur AES (Advanced Encryption Standard)

Laporan ini ini disusun untuk memenuhi tugas mata kuliah Keamanan Data

Dosen Pengampu : Sevi Nurafni, S.T., M.Si., M.Sc.

Disusun oleh :

Indri Nur Sukmawati	(2C2220010)
Catherine Vanya Pangemanan	(2C2220008)
Cahya Rahmawati	(2C2220011)
Ester Salay	(2C2220016)
Sagara Andi Ladzuardi S	(2C2220004)
Ashafa Multazam	(2C2220012)
Muhammad Kamal Shidiq	(2C2220002)

PROGRAM STUDI SAINS DATA
FAKULTAS SAINS DAN TEKNOLOGI
2025

BAB I
PENDAHULUAN

1.1 Definisi AES

AES adalah singkatan dari ***Advanced Encryption Standard*** dan merupakan algoritma enkripsi simetris yang paling banyak digunakan. Algoritma ini digunakan untuk enkripsi dan perlindungan data elektronik. Algoritma ini juga digunakan sebagai pengganti DES (*Data Encryption Standard*) karena jauh lebih cepat dan lebih baik daripada DES. AES terdiri dari tiga blok sandi dan sandi-sandi ini digunakan untuk menyediakan enkripsi data. AES dirancang untuk menjadi cepat, efisien, dan aman. Algoritma ini menggunakan kunci enkripsi yang panjangnya bisa bervariasi, yaitu 128, 192, atau 256 bit. Panjang kunci ini menentukan tingkat keamanan enkripsi-semakin panjang kuncinya, semakin sulit untuk memecahkan enrkipsi tersebut.

1.2 Sejarah Singkat AES

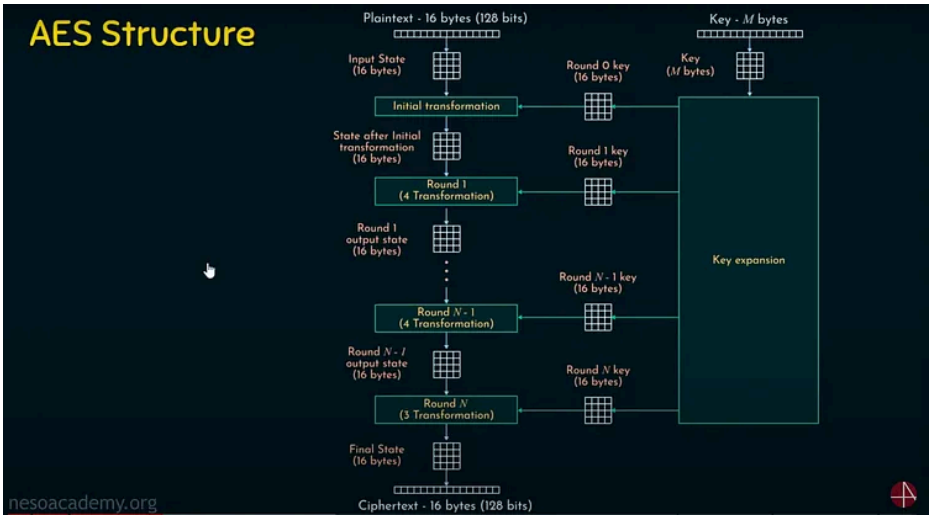
AES dikembangkan oleh NIST (National Institute of Standards and Technology) pada tahun 1997. AES dikembangkan untuk menggantikan DES yang cenderung lebih lambat dan rentan terhadap berbagai serangan. Oleh karena itu, dibuatlah algoritma enkripsi baru untuk mengatasi kekurangan DES. AES kemudian diterbitkan pada tanggal 26 November 2001.Sebenarnya nama original AES adalah algoritma Rijndael, dimana algoritma ini pertama kali dikembangkan oleh Vincent Rijmen dan Joan Daemen.
Pada awalnya algoritma Rijandael merupakan hasil kompetisi yang diadakan oleh NIST setelah sebelumnya algoritma DES berhasil dibobol. Selain Rijndael terdapat dua kandidat terkuat lainnya yaitu Serpent dan juga Twofish. Namun Rijndael berhasil memenangi score dengan nilai pengujian 86 positif dan 10 negatif, sehingga algoritma Rijandael diresmikan sebagai standar enkripsi dengan nama **AES**.

1.3 Tujuan Laporan

Laporan ini disusun dengan tujuan untuk memahami secara mendalam struktur dari algoritma ***Advanced Encryption Standard*** **(AES)**. Fokus utama dari laporan ini adalah untuk mempelajari bagaimana AES bekerja dalam proses enkripsi dan dekripsi data, termasuk mengenal blok-blok penyusunnya seperti SubBytes, ShiftRows, MixColumns, dan AddRoundKey yang membentuk jaringan substitusi-permutasi (Substitution-Permutation Network). Selain itu, laporan ini juga bertujuan untuk mengidentifikasi perbedaan jumlah putaran (rounds) berdasarkan panjang kunci yang digunakan, serta memberikan contoh enkripsi dan dekripsi sederhana untuk mempermudah pemahaman konsep kerja AES. Dengan adanya laporan ini, diharapkan pembaca dapat memahami keunggulan AES dibandingkan algoritma sebelumnya seperti DES, serta pentingnya penerapan AES dalam menjaga keamanan data digital di berbagai aplikasi.

BAB II
Struktur AES

Structure Enkripsi AES



Gambar 1.0 Dari Neso Academy

1. Dibutuhkan input 16 byte (128 bit) dan mengeluarkan ciphertext (128 bit).
2. Setiap 4 x 4 = 16 byte adalah array status elemen yang dapat menyimpan 16 byte informasi
3. Status masukan: menyimpan teks biasa masukan 16 byte dan memberikan transformasi awal
4. Pada transformasi awal, masukan teks biasa 16 byte beserta fungsi transformasi dan output diberikan ke array elemen transformasi awal yang kemudian diberikan lagi ke Putaran 1
5. Putaran 1 Ambil keluaran langkah 4 dan lakukan 4 transformasi dengannya
6. Demikian pula, Putaran 2 mengambil langkah sebelumnya putaran operasi + 4 transformasi output sampai Putaran N — 1
7. Pada Putaran N terakhir, output dari Putaran N — 1 merupakan input dari Putaran N yang merupakan putaran terakhir dan hanya memiliki 3 Transformasi
8. Output dari langkah 7 sekarang disimpan dalam array elemen. Dan 16 byte adalah cipher sebenarnya yang kita inginkan dari Struktur Enkripsi AES ini.

Block size dan key size

Rijndael mendukung panjang kunci 128 bit sampai 256 bit dengan step 32 bit (yaitu 128 bit, 160, 192, …, 256 bit).

• Panjang kunci dan ukuran blok dapat dipilih secara independen.
• Setiap blok dienkripsi dalam sejumlah putaran tertentu, sebagaimana halnya pada DES.
• Karena AES menetapkan panjang kunci adalah 128, 192, dan 256, maka dikenal AES-128, AES-192, dan AES-256.

AES	Panjang Kunci (*Nk words)*	Ukuran Blok (*Nb words)*	Jumlah Putaran (*Nr*)
128	4	4	10
192	5	4	12
256	6	4	14

Struktur Substitution-Permutation Network (SPN)

AES menggunakan struktur SPN yang terdiri dari beberapa ronde transformasi untuk mencapai tingkat keamanan yang tinggi melalui prinsip confusion dan diffusion. Setiap ronde (kecuali ronde terakhir) terdiri dari empat operasi utama:

1. SubBytes
2. ShiftRows
3. MixColumns
4. AddRoundKey

Setiap putaran enkripsi dalam AES terdiri dari beberapa langkah berikut:

1. **SubBytes**
   Setiap byte dalam blok data digantikan dengan byte lain menggunakan tabel substitusi yang disebut S-box.
2. **ShiftRows**
   Baris-baris dalam matriks data digeser ke kiri dengan jumlah pergeseran yang berbeda-beda untuk setiap baris.
3. **MixColumns**
   Setiap kolom dalam matriks data dikalikan dengan matriks tetap untuk mencampur byte dalam kolom tersebut.
4. **AddRoundKey**
   Blok data dikombinasikan dengan kunci putaran menggunakan operasi XOR.

Proses enkripsi diawali dengan langkah AddRoundKey, diikuti oleh beberapa putaran transformasi seperti di atas, dan diakhiri dengan putaran terakhir yang tidak mencakup langkah MixColumns.

BAB III
Contoh Enkripsi-Dekripsi Sederhana

3.1 Contoh manual enkripsi dan dekripsi menggunakan AES
Algoritma AES (Advance Encryption Standard)

Langkah Pengerjaan Enkripsi:
<menggunakan bit **128**

1. Masukkan plaintext ke dalam matrix P(4x4)
2. Masukkan kunci kedalam matrix K(4x4)
3. Konversi matrix P & K dalam hexadesimal

4. Round = P xor K (P & K yang sudah dikonversi ke bentuk hexadecimal)
5. Ulangi perintah berikut 9x
    a. R2= SubByte Round dengan S-Box
    b. R3= Lakukan Shift Row dengan R2
    c. R4= Kalikan R3 dengan matrix Mix
    d. Round = R4 xor K
6. Final Round
    a. R2= SubByte Round dengan S-Box
    b. R3= Lakukan Shift Row dengan R2
    c. Round= R4 xor K

Ciphertext= Round

Implementasi Perhitungan:
Plaintext: ariandoharedison
Kunci: kriptografiaesku

<<buat matrix 4x4 untuk plaintext

A	N	A	I
R	D	R	S
I	O	E	O
A	H	D	N

<<matrix plaintext dikonversi ke hexadecimal dalam tabel ASCII

41	4E	41	49
52	44	52	53
49	4F	45	4F
41	48	44	4E

<<buat matrix 4x4 untuk kunci

K	T	A	E
R	O	F	S
I	G	I	K
P	R	A	U

<<matrix kunci dikonversi ke hexadecimal dalam tabel ASCII

4B	54	41	45
52	4F	46	53
49	47	49	4B
50	52	41	55

<<Round = P xor K (P & K yang sudah dikonversi ke bentuk hexadecimal)

Hasil xor:

0A	1A	00	0C
00	0B	14	00
00	08	0C	04
11	1A	05	1B

<<R2= SubByte Round dengan S-Box

Round

0A	1A	00	0C
00	0B	14	00
00	08	0C	04
11	1A	05	1B

menggunakan tabel S-Box:

	x0	x1	x2	x3	x4	x5	x6	x7	x8	x9	xa	xb	xc	xd	xe	xf
0x	63	7c	77	7b	f2	6b	6f	c5	30	01	67	2b	fe	d7	ab	76
1x	ca	82	c9	7d	fa	59	47	f0	ad	d4	a2	af	9c	a4	72	c0
2x	b7	fd	93	26	36	3f	f7	cc	34	a5	e5	f1	71	d8	31	15
3x	04	c7	23	c3	18	96	05	9a	07	12	80	e2	eb	27	b2	75
4x	09	83	2c	1a	1b	6e	5a	a0	52	3b	d6	b3	29	e3	2f	84
5x	53	d1	00	ed	20	fc	b1	5b	6a	cb	be	39	4a	4c	58	cf
6x	d0	ef	aa	fb	43	4d	33	85	45	f9	02	7f	50	3c	9f	a8
7x	51	a3	40	8f	92	9d	38	f5	bc	b6	da	21	10	ff	f3	d2
8x	cd	0c	13	ec	5f	97	44	17	c4	a7	7e	3d	64	5d	19	73
9x	60	81	4f	dc	22	2a	90	88	46	ee	b8	14	de	5e	0b	db
ax	e0	32	3a	0a	49	06	24	5c	c2	d3	ac	62	91	95	e4	79
bx	e7	c8	37	6d	8d	d5	4e	a9	6c	56	f4	ea	65	7a	ae	08
cx	ba	78	25	2e	1c	a6	b4	c6	e8	dd	74	1f	4b	bd	8b	8a
dx	70	3e	b5	66	48	03	f6	0e	61	35	57	b9	86	c1	1d	9e
ex	e1	f8	98	11	69	d9	8e	94	9b	1e	87	e9	ce	55	28	df
fx	8c	a1	89	0d	bf	e6	42	68	41	99	2d	0f	b0	54	bb	16

Hasil R2:

67	A2	63	FE
63	2B	FA	63
63	30	FE	F2
82	A2	6B	AF

<<R3= Lakukan Shift Row dengan R2

R2 di shift row

67	A2	63	FE
63	2B	FA	63
63	30	FE	F2
82	A2	6B	AF

Hasil shift row (R3):

67	A2	63	FE
2B	FA	63	63
FE	F2	63	30
AF	82	A2	6B

Pada baris pertama tidak ada pergeseran, pada baris ke-2 terjadi pergeseran 1 ke kiri -> pada baris ke-3 terjadi pergeseran 2 ke kiri -> pada baris ke-4 terjadi pergeseran 3 ke kiri.

<<R4= Kalikan R3 dengan matrix Mix

R3

67	A2	63	FE
2B	FA	63	63
FE	F2	63	30
AF	82	A2	6B

Matrix Mix

02	03	01	01
01	02	03	01
01	01	02	03
03	01	01	02

Hasil R4:

E2	3A	A2	19
87	C2	A2	03
41	3A	3B	40
39	EA	FA	9C

<<Round = R4 xor K

R4

E2	3A	A2	19
87	C2	A2	03
41	3A	3B	40
39	EA	FA	9C

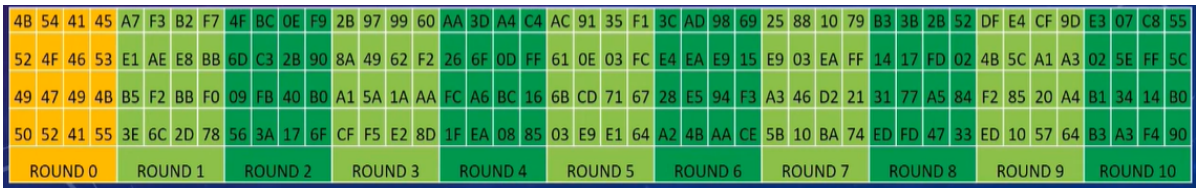
K

A7	F3	B2	F7
E1	AE	E8	BB
B5	F2	BB	F0
3E	6C	2D	78

Hasil : untuk melanjutkan proses enkripsi pada round 2 dan seterusnya sampai diulang 9x

45	C9	10	EE
66	6C	4A	B8
F4	C8	80	B0
07	86	D7	E4

<<Hasil perhitungan Round 2 - Round 9



<<Final Round Pada Round Ke 10

Pada perhitungan enkripsi round ke-10 masih sama seperti langkah perhitungan enkripsi pada round ke-1 samapi ke-9, hanya saja pada enkripsi round ke-10 tidak ada “R4= Kalikan R3 dengan matrix Mix”

<<R2= SubByte Round dengan S-Box

Round 9

6F	0D	7F	DE
0A	86	9C	16
A0	04	FF	16
CC	FB	18	62

Hasil R2

A8	D7	D2	1D
67	44	DE	47
E0	F2	16	47
4B	0F	AD	AA

<<R3= Lakukan Shift Row dengan R2

R2 di Shift Row

A8	D7	D2	1D
67	44	DE	47
E0	F2	16	47
4B	0F	AD	AA

Hasil R3

A8	D7	D2	1D
44	DE	47	67
16	47	E0	F2
AA	4B	0F	AD

<<Hasil Akhir Proses Enkripsi

HEXA	4B	46	A7	19	D0	80	73	E8	1A	B8	F4	FB	48	3B	42	3D
DEC	75	70	167	25	208	128	115	232	26	184	244	251	72	59	66	61
CHIPER TEXT	K	F	º	↓	╨	Ç	s	Φ	→	╕	⌠	√	H	;	B	=

Langkah Pengerjaan Dekripsi:

<menggunakan bit **128**

Berdasarkan hasil Roundkey 1-10 pada tabel berikut, kita bisa melakukan dekripsi dengan cara membalikkan algoritma enkripsi.

4B	54	41	45	A7	F3	B2	F7	4F	BC	0E	F9	2B	97	99	60	AA	3D	A4	C4	AC	91	35	F1	3C	AD	98	69	25	88	10	79	B3	3B	2B	52	DF	E4	CF	9D	E3	07	C8	55
52	4F	46	53	E1	AE	E8	BB	6D	C3	2B	90	8A	49	62	F2	26	6F	0D	FF	61	0E	03	FC	E4	EA	E9	15	E9	03	EA	FF	14	17	FD	02	4B	5C	A1	A3	02	5E	FF	5C
49	47	49	4B	B5	F2	BB	F0	09	FB	40	B0	A1	5A	1A	AA	FC	A6	BC	16	6B	CD	71	67	28	E5	94	F3	A3	46	D2	21	31	77	A5	84	F2	85	20	A4	B1	34	14	B0
50	52	41	55	3E	6C	2D	78	56	3A	17	6F	CF	F5	E2	8D	1F	EA	08	85	03	E9	E1	64	A2	4B	AA	CE	5B	10	BA	74	ED	FD	47	33	ED	10	57	64	B3	A3	F4	90
ROUND 0				ROUND 1				ROUND 2				ROUND 3				ROUND 4				ROUND 5				ROUND 6				ROUND 7				ROUND 8				ROUND 9				ROUND 10			

1. Tahap Roundkey 0: Menggunakan Chipertext yang sudah kita dapatkan sebelumnya, akan dilakukan Invers Addroundkey kemudian hasilnya di-XOR-kan dengan matriks hasil Roundkey Ke-10. (Invers Addroundkey (Chipertext) XOR Roundkey 10 = Block 0).

   << Chipertext yang ada diterapkan Invers Addroundkey

4B	D0	1A	48
46	80	B8	3B
A7	73	F4	42
19	E8	FB	3D

   << XOR hasilnya dengan matriks Roundkey Ke-10 berikut

E3	07	C8	55
02	5E	FF	5C
B1	34	14	B0
B3	A3	F4	90

<<Dihasilkan Block 0

A8	D7	D2	1D
44	DE	47	67
16	47	E0	F2
AA	4B	0F	AD

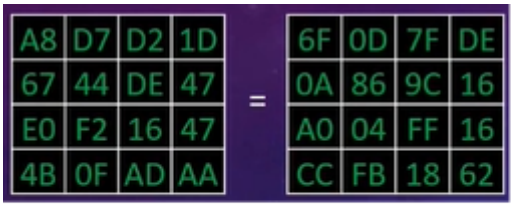
Block 0 ini akan digunakan sebagai Roundkey Ke-1 pada proses Dekripsi.

2. Tahap Round 1: Jika pada proses Enkripsi didahulukan enkripsi Subbytes maka pada tahap Roundkey Ke-1 Dekripsinya yang akan dikerjakan dahulu adalah Invers Shitfrow, kemudian Invers Subbytes, Invers Addroundkey dan Invers Mixcolumn.

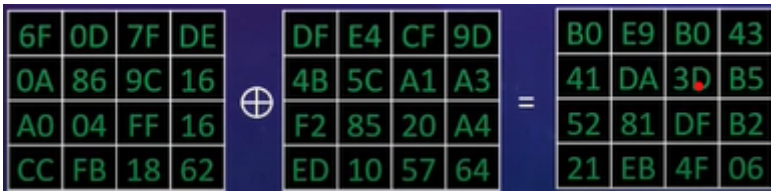
   Menggunakan Chipertext yang sudah kita dapatkan sebelumnya, yaitu Block 0 atau Roundkey Ke-1 untuk dekripsi, akan dilakukan:

   << Block 0 atau Roundkey Ke-1 Dekripsi diterapkan Invers Shiftrow

   <<Hasilnya diterapkan Invers Subbytes



   <<Hasilnya diterapkan Invers Addroundkey XOR dengan Addroundkey Ke-9



   <<Hasilnya diterapkan Invers Mixcolumn

3. Tahap Roundkey 2-10: Ulangi terus proses Inverse Shiftrow sampai Mixcolumn. Terkecuali untuk Roundkey Ke-10 dia tidak melalui perhitungan Invers Mixcolumn lagi.

41	4E	41	49
52	44	52	53
49	4F	45	4F
41	48	44	4E

Matriks tersebut merupakan hasil Dekripsi Roundkey Ke-10.

4. Sesuaikan Hexadesimal terhadap Tabel ASCII maka dihasilkan Plain Text

HEXA	41	52	49	41	4E	44	4F	48	41	52	45	44	49	53	4F	4E
DEC	65	82	73	65	78	68	79	72	65	82	69	68	73	83	79	78
PLAIN TEXT	A	R	I	A	N	D	O	H	A	R	E	D	I	S	O	N

BAB IV
Performa AES

4.1 Kelebihan AES

a) AES mendukung panjang kunci **128**, **192**, dan **256 BIT**, sementara DES hanya menggunakan kunci 56 bit. Ukuran kunci yang lebih panjang membuat AES jauh lebih tahan terhadap serangan brute force.

b) AES menggunakan prinsip substitusi dan permutasi, berbeda dengan struktur Feistel pada DES. Pendekatan ini memberikan keamanan yang lebih tinggi dan efisiensi yang lebih baik dalam proses enkripsi dan dekripsi.

c) AES umumnya lebih cepat dan efisien dibandingkan DES, terutama dalam implementasi perangkat lunak, menjadikannya pilihan yang lebih baik untuk aplikasi modern.

4.2 Kekurangan AES

a) Sebagai algoritma simetris, keamanan AES sangat bergantung pada kerahasiaan kunci enkripsi. Jika kunci tersebut bocor atau disimpan dengan tidak aman, maka seluruh sistem enkripsi dapat dengan mudah ditembus, terlepas dari kekuatan algoritma itu sendiri.

b) Penggunaan AES dalam mode operasi Electronic Codebook (ECB) memiliki kelemahan karena setiap blok plaintext yang identik akan dienkripsi menjadi ciphertext yang identik pula. Hal ini dapat menyebabkan pola dalam data asli tetap terlihat dalam data terenkripsi, membuatnya rentan terhadap serangan tertentu seperti chosen plaintext attack.

c) Meskipun AES-256 memiliki panjang kunci yang lebih besar, penelitian menunjukkan bahwa terdapat kelemahan dalam fungsi ekspansi kuncinya. Serangan teoretis telah

berhasil mengurangi kompleksitas serangan terhadap AES-256 menjadi lebih rendah dibandingkan AES-128, meskipun serangan ini masih belum praktis dengan teknologi saat ini.

d) Kemajuan dalam komputasi kuantum dapat mengancam keamanan algoritma enkripsi saat ini, termasuk AES. Algoritma kuantum seperti Grover's algorithm dapat secara teoritis mengurangi efektivitas panjang kunci AES, sehingga AES-128 dapat setara dengan keamanan AES-64 dalam konteks kuantum.

e) Implementasi AES dalam perangkat lunak dapat menjadi kompleks, terutama dalam mode operasi seperti Counter (CTR) yang memerlukan perhatian khusus terhadap aspek keamanan dan kinerja. Kesalahan dalam implementasi dapat membuka celah keamanan yang serius.

f) pada perangkat dengan sumber daya terbatas seperti perangkat IoT, implementasi AES-256 dapat menjadi beban karena membutuhkan lebih banyak daya dan memori. Hal ini mendorong pengembangan algoritma kriptografi ringan yang lebih sesuai untuk perangkat semacam itu.

4.3 Keamanan AES

a) Dengan panjang kunci hingga **256 BIT**, jumlah kemungkinan kombinasi kunci sangat besar, membuat serangan brute force secara praktis tidak mungkin dilakukan dengan teknologi saat ini.

b) AES dirancang untuk tahan terhadap berbagai jenis serangan kriptografi, termasuk analisis diferensial dan linier, berkat struktur algoritmanya yang kompleks.

c) Meskipun AES sangat aman terhadap serangan klasik, kemajuan dalam komputasi kuantum dapat mengancam keamanannya di masa depan, karena komputer kuantum memiliki potensi untuk memecahkan enkripsi AES lebih efisien dibandingkan komputer klasik.

4.4 Penggunaan AES dalam Aplikasi Nyata

a) AES digunakan dalam protokol keamanan seperti HTTPS untuk melindungi data yang dikirimkan melalui internet.

b) Banyak perangkat lunak keamanan dan sistem operasi modern menggunakan AES untuk mengenkripsi data di hard drive atau perangkat penyimpanan lainnya.

c) Beberapa aplikasi chatting mengimplementasikan AES untuk memastikan keamanan pesan yang dikirim antar pengguna.

d) Program seperti 7-Zip menggunakan AES-256 untuk mengenkripsi arsip, memberikan perlindungan tambahan terhadap akses tidak sah.

BAB V
Kesimpulan

Advanced Encryption Standard (AES) merupakan algoritma **kriptografi simetris**, yaitu jenis kriptografi yang menggunakan **kunci enkripsi dan dekripsi yang sama**, sehingga sangat efisien dalam proses pertukaran data dalam sistem yang sudah terautentikasi. AES telah ditetapkan sebagai **standar enkripsi** oleh **National Institute of Standards and Technology (NIST)** pada tahun 2001 untuk menggantikan algoritma **Data Encryption Standard (DES)** yang telah dianggap tidak lagi memberikan tingkat perlindungan yang memadai akibat kemajuan **kriptanalisis** (ilmu untuk memecahkan sandi) dan pertumbuhan **kekuatan komputasi** yang pesat.

AES mendukung **panjang kunci** sebesar 128, 192, dan 256 bit. Panjang kunci ini mengacu pada jumlah bit dalam kunci kriptografi yang digunakan untuk proses enkripsi dan dekripsi, di mana semakin panjang kunci, semakin tinggi tingkat keamanan yang diberikan. AES memiliki struktur internal berbasis **jaringan substitusi-permutasi (Substitution-Permutation Network/SPN)**, yakni arsitektur enkripsi yang menggabungkan operasi substitusi (penggantian simbol) dan permutasi (pengacakan posisi) dalam beberapa putaran untuk menyembunyikan pola data asli. Desain ini menghasilkan proses yang **aman, efisien, dan fleksibel**, serta dapat diimplementasikan baik dalam **perangkat lunak (software)** seperti aplikasi komputer, maupun **perangkat keras (hardware)** seperti chip enkripsi.

Keunggulan utama AES terletak pada penerapan prinsip **confusion** dan **diffusion**. *Confusion* adalah upaya menyulitkan keterkaitan langsung antara kunci dan ciphertext (hasil enkripsi), sedangkan *diffusion* berupaya menyebarkan informasi plaintext (teks asli) ke seluruh ciphertext agar satu perubahan kecil pada input menghasilkan perubahan besar pada output. Kedua prinsip ini diimplementasikan melalui **transformasi non-linier** (seperti substitusi menggunakan S-Box) dan **operasi linier** (seperti pergantian posisi dan perkalian matriks) dalam setiap **putaran enkripsi**. AES memiliki jumlah putaran yang berbeda tergantung panjang kunci—misalnya, 10 putaran untuk kunci 128-bit dan 14 putaran untuk kunci 256-bit.

Struktur ini membuat AES sangat tangguh terhadap serangan **kriptografi klasik** seperti **differential cryptanalysis** (serangan berdasarkan analisis perbedaan input dan output) dan **linear cryptanalysis** (serangan berbasis pendekatan linier terhadap hubungan antar bit plaintext dan ciphertext).

Dalam praktiknya, AES telah banyak digunakan dalam **protokol komunikasi aman** seperti **Transport Layer Security (TLS)** dan **Secure Sockets Layer (SSL)**, yang melindungi transmisi data di internet. Selain itu, AES juga digunakan untuk **enkripsi data pada perangkat penyimpanan digital**, **aplikasi perpesanan**, serta sistem berbasis **Internet of Things (IoT)**, yang membutuhkan pengamanan data pada perangkat kecil dengan sumber daya terbatas.

Walaupun hingga saat ini AES tetap dianggap sangat aman, munculnya **komputasi kuantum** membuka kemungkinan terhadap **serangan kuantum** di masa depan. Misalnya, **Grover's Algorithm** berpotensi mengurangi efektivitas panjang kunci AES secara signifikan, sehingga mengharuskan pengembangan teknik mitigasi atau algoritma kriptografi post-kuantum sebagai alternatif.

Dengan demikian, AES tidak hanya merupakan tulang punggung dalam pengamanan informasi digital modern, tetapi juga menjadi simbol dari kemajuan teknologi kriptografi yang mengedepankan **keamanan, efisiensi, dan kemampuan adaptasi** terhadap tantangan era digital yang terus berkembang.

BAB VI
Referensi

Agastyra, H., n.d. *Pengkajian Metode dan Implementasi AES.* [Online]
Available at:
https://informatika.stei.itb.ac.id/~rinaldi.munir/Matdis/2010-2011/Makalah2010/MakalahStrukdis2010-023.pdf

Cyber, K., 2023. *Apa kekuatan utama Advanced Encryption Standard (AES) dalam hal ketahanannya terhadap serangan dan keamanan?.* [Online]
Available at:
https://id.eitca.org/keamanan-cyber/eitc-adalah-dasar-dasar-kriptografi-klasik-ccf/aes-blok-cipher-cryptosystem/standar-enkripsi-canggih-aes/pemeriksaan-ulasan-standar-enkripsi-canggih-aes/apa-kekuatan-utama-dari-standar-enkripsi-lanjutan-aes-dalam-hal-ke

geeksforgeeks, 2025. *Advanced Encryption Standard (AES).* [Online]
Available at: https://www.geeksforgeeks.org/advanced-encryption-standard-aes/

Insights, C., 2024. *Advanced Encryption Standard (AES) Structure: An In-Depth Analysis.* [Online]
Available at:
https://codedinsights.com/modern-cryptography/advanced-encryption-standard-aes-structure/

Kantinit, 2023. *Algoritma AES? Pengertian, Cara Kerja dan Implementasi.* [Online]
Available at:
https://kantinit.com/programming/algoritma-aes-pengertian-cara-kerja-dan-implementasi/

M, N. D., 2014. *Universitas Aki Semarang.* [Online]
Available at:
https://www.academia.edu/7426961/Algoritma_Advanced_Encryption_Standard_AES_?utm_

Syafrayani, P. R., 2024. *Mengenal Kriptografi AES: Standar Enkripsi Teraman Saat Ini.* [Online]
Available at:
https://uptjurnal.umsu.ac.id/mengenal-kriptografi-aes-standar-enkripsi-teraman-saat-ini/

tekkom.upi, 2024. *Keamanan dan Enkripsi Data Menggunakan Advanced Encryption Standard (AES).* [Online]
Available at:
https://tekkom.upi.edu/2024/03/keamanan-dan-enkripsi-data-menggunakan-advanced-encryption-standard-aes/

ascii-code. (n.d.). Retrieved from ASCII Table: https://www.ascii-code.com/