

Perbandingan Implementasi Algoritma Aes Dalam Pemrograman Jaringan Dan Analisis Algoritma Enkripsi Untuk Pengamanan Komunikasi Jaringan

¹Sri Asri, ²Tigor Peryanto, ³Essy Malays
^{1,2}Tif, Upi Yai, Jakarta Pusat

¹tsriasri@gmail.com ²tigorpervanto@gmail.com, ³essy.malays@gmail.com

Abstrak

Pengamanan komunikasi jaringan merupakan aspek krusial dalam pengembangan aplikasi berbasis jaringan. dua pendekatan utama dalam menghadapi tantangan ini adalah melalui implementasi langsung dari algoritma enkripsi dan analisis komprehensif terhadap berbagai algoritma enkripsi yang tersedia. dalam penelitian ini, kami membandingkan dua pendekatan ini melalui dua jurnal terpisah. jurnal pertama, "implementasi algoritma AES dalam pemrograman jaringan untuk komunikasi aman", mengeksplorasi implementasi praktis dari Advanced Encryption Standard (AES) dalam pengembangan aplikasi jaringan. di sisi lain, jurnal kedua, "analisis algoritma enkripsi untuk pengamanan komunikasi Jaringan", mengadopsi pendekatan analitis untuk mengevaluasi dan membandingkan berbagai algoritma enkripsi yang ada. melalui perbandingan ini, kami menyajikan kontribusi yang unik dalam memahami kelebihan dan kekurangan dari masing-masing pendekatan, serta memberikan wawasan yang berharga bagi para pengembang dalam memilih strategi yang paling sesuai dengan kebutuhan keamanan aplikasi jaringan mereka.

Kata kunci : *Pengamanan, Komunikasi, Jaringan, Aes, Implementasi, Algoritma, Analisis*

Abstrak

Securing network communication is a crucial aspect in the development of network-based applications. Two main approaches in addressing this challenge are through direct implementation of encryption algorithms and comprehensive analysis of various encryption algorithms available. In this research, we compare these two approaches through two separate journals. The first journal, "Implementation of AES Algorithm in Network Programming for Secure Communication," explores the practical implementation of the Advanced Encryption Standard (AES) in network application development. On the other hand, the second journal, "Analysis of Encryption Algorithms for Network Communication Security," adopts an analytical approach to evaluate and compare various existing encryption algorithms. Through this comparison, we present a unique contribution in understanding the strengths and weaknesses of each approach, as well as providing valuable insights for developers in choosing the most suitable strategy for the security needs of their network applications.

Keywords: *Security, Communication, Network, AES, Implementation, Algorithm, Analysis*

1. PENDAHULUAN

Dalam era yang diwarnai oleh pertukaran informasi melalui jaringan komputer yang semakin meluas, keamanan komunikasi jaringan menjadi sangat penting. Pengembangan aplikasi yang mampu melindungi integritas, kerahasiaan, dan otentikasi data yang dikirim dan diterima melalui jaringan menjadi prioritas utama bagi para pengembang perangkat lunak. Dua pendekatan utama yang digunakan untuk mencapai tujuan ini adalah melalui implementasi langsung dari algoritma enkripsi yang kuat dan analisis komprehensif terhadap berbagai algoritma enkripsi yang tersedia.

Dalam konteks ini, penelitian ini bertujuan untuk membandingkan dua pendekatan ini melalui dua jurnal terpisah. Jurnal pertama, berjudul "Implementasi Algoritma AES dalam Pemrograman Jaringan untuk Komunikasi Aman", mengeksplorasi pendekatan implementatif dengan mengevaluasi langkah-langkah praktis dalam mengintegrasikan Advanced Encryption Standard (AES) ke dalam pengembangan aplikasi jaringan. Di sisi lain, jurnal kedua, yang berjudul "Analisis Algoritma Enkripsi untuk Pengamanan Komunikasi Jaringan", mengambil pendekatan analitis dengan melakukan evaluasi menyeluruh terhadap berbagai algoritma enkripsi yang tersedia, termasuk AES, untuk memahami kekuatan, kelemahan, dan kecocokan mereka dalam konteks pengamanan komunikasi jaringan.

2. LANDASAN TEORI

2.1 Algoritma dan Kriptografi

Menurut Ramadhan (2018), algoritma adalah cara yang dapat ditempuh oleh komputer dalam mencapai suatu tujuan, terdiri atas langkah-langkah yang terdefinisi dengan baik, menerima *input*, melakukan proses dan menghasilkan *output* (Ramadhan et al., 2018).

Kriptografi secara umum adalah ilmu dan seni untuk menjaga kerahasiaan berita. Selain pengertian tersebut terdapat pula pengertian ilmu yang mengajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan data, keabsahan data, integritas data, serta autentikasi data (A. Menezes, P. Van Oorschot and S. Vanstone- Handbook of Applied Cryptography). Sedangkan menurut Kaufman et. al. (2002) menjelaskan bahwa kata

Kriptografi berasal dari bahasa Yunani dan memiliki makna seni dalam menulis pesan rahasia (*The art of secret writing*), dimana kriptografi terdiri dari 2 kata yaitu *cryptós* yang berarti *rahasia* atau *tersembunyi* dan *gráphein* yang berarti *tulisan*. (Apriandala, 2013: 114). Ada empat tujuan mendasar dari ilmu kriptografi ini juga merupakan aspek keamanan informasi yaitu Kerahasiaan adalah layanan yang digunakan untuk menjaga isi dari informasi dari siapapun kecuali yang memiliki otoritas atau kunci rahasia untuk membuka/mengupas informasi yang telah disandi. Integritas data adalah berhubungan dengan penajagaan dari perubahan data secara tidak sah (Anwar, 2017).

Untuk menjaga integritas data, sistem harus memiliki kemampuan untuk mendeteksi manipulasi data oleh pihak-pihak yang tidak berhak, antara lain penyisipan, penghapusan, dan pensubtitusian data lain kedalam data yang sebenarnya. Autentikasi adalah berhubungan dengan identifikasi atau pengenalan, baik secara kesatuan sistem maupun informasi itu sendiri. Dua pihak yang saling berkomunikasi harus saling memperkenalkan diri. Informasi yang dikirimkan melalui kanal harus diautentikasi keaslian isi datanya, waktu pengiriman dan lain-lain. Non-repudiasi atau penyangkalan adalah usaha untuk mencegah terjadinya penyangkalan terhadap pengiriman/terciptanya suatu informasi oleh yang mengirimkan atau membuat (Maulana & Fajrin, 2018).

Kriptografi memiliki 4 komponen utama yaitu:

- 1) *Plaintext*, yaitu pesan yang dapat dibaca.
- 2) *Ciphertext*, yaitu pesan sandi/pesan acak yang tidak bisa dibaca.
- 3) *Key*, yaitu kunci untuk melakukan Teknik kriptografi.
- 4) *Algoritma*, yaitu metode Untuk melakukan enkripsi dan dekripsi.

2.2 Implementasi Algoritma AES dalam Pemrograman Jaringan

AES (Advanced Encryption Standard) : AES adalah sebuah algoritma kriptografi simetris yang digunakan secara luas untuk enkripsi data. Ini adalah standar yang diadopsi oleh pemerintah Amerika Serikat untuk penggunaan di dalam perlindungan informasi

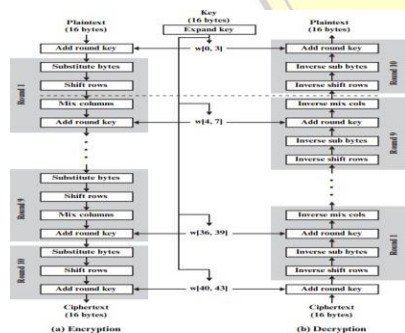
sensitif. AES memiliki tiga variasi kunci dengan panjang 128, 192, dan 256 bit.

Mode Operasi AES : Ada beberapa mode operasi yang dapat digunakan dengan AES, seperti ECB (Electronic Codebook), CBC (Cipher Block Chaining), dan lainnya (Hidayati et al., 2021).

Kriptografi adalah ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan, integritas data, serta otentikasi (Menez 1996). Kriptografi merupakan kaskas (tool) yang sangat penting di dalam keamanan informasi kriptografi memiliki layanan seperti berikut.

- Kerahasiaan Pesan (*Confidentiality/privacy/secretary*)
- Keaslian pesan (*Data Integrity*)
- Keaslian pengirim dan penerima pesan (*Authentication*)
- Anti penyangkalan (*Non-repudiation*).

AES diperkenalkan untuk menggantikan DES karena DES menggunakan kunci sandi yang sangat kecil dan algoritmenya lebih lambat. Rijndael dikembangkan oleh dua kriptografer Belgia, Joan Daemen dan Vincent Rijmen, dan diajukan oleh mereka untuk proses seleksi AES [10]. Algoritma AES memiliki ukuran blok 128 bit atau 16 byte. Tiga versi AES beserta spesifikasi yang mengikuti tercantum pada Tabel 1. AES terdiri dari tiga penyandian blok, yaitu AES-128, AES-192, dan AES-256. deskripsi AES ditunjukkan oleh Gambar 1.



Gambar 2. 1 Proses Enkripsi dan Dekripsi AES.

Pada tahun 1997, *National Institute of Standard and Technology (NIST) of United States* mengeluarkan *Advanced Encryption Standard(AES)* untuk menggantikan *Data Encryption Standard (DES)*. AES dibangun dengan maksud untuk mengamankan pemerintahan diberbagai bidang. Algoritma AES di design menggunakan blok *chiper* minimal dari blok 128 bit *input* dan mendukung ukuran 3 kunci (*3-key-sizes*), yaitu kunci 128 bit, 192 bit, dan 256 bit. Pada agustus 1998, NIST mengumumkan bahwa ada 15 proposal AES yang telah diterima dan dievaluasi, setelah mengalami proses seleksi terhadap algoritma yang masuk, NIST menumumkan pada tahun 1999 bahwa hanya ada 5 algoritma yang diterima, algoritma tersebut diantara lain adalah MARS, RC6, Rijndael, Serpent, dan Twofish. Algoritma-algoritma tersebut manjalani berbagai macam pengetesan. Pada bulan oktober 2000, NIST mengumumkan bahwa Rijndael sebagai algoritma yang terpilih untuk standar AES yang baru. Baru pada february 2001 NIST mengirimkan *draft* kepada *Federal Information Processing Standards (FIPS)* untuk standar AES. Kemudian pada 26 November 2001, NIST mengumumkan produk akhir dari *Advanced Encryption Standard (Meko, 2018)*.

AES (*Advanced Encryption Standard*) adalah lanjutan dari algoritma enkripsi standar DES (*Data Encryption Standard*) yang masa berlakunya dianggap telah usai karena faktor keamanan. Kecepatan komputer yang sangat pesat dianggap sangat membahayakan DES, sehingga pada tanggal 2 Maret tahun 2001 ditetapkanlah algoritma baru Rijndael sebagai AES. Kriteria pemilihan AES didasarkan pada 3 kriteria utama yaitu: keamanan, harga, dan karakteristik algoritma beserta implementasinya. Keamanan merupakan faktor terpenting dalam evaluasi (minimal seaman triple DES), yang meliputi ketahanan terhadap semua analisis sandi yang telah diketahui dan diharapkan dapat menghadapi analisis sandi yang belum diketahui. Di samping itu, AES juga harus dapat digunakan secara bebas tanpa harus membayar royalti, dan juga murah untuk diimplementasikan pada *smart card* yang memiliki ukuran memori kecil. AES juga harus efisien dan cepat (minimal secepat Triple DES) dijalankan dalam berbagai mesin 8 bit hingga 64 bit, dan berbagai perangkat lunak. DES menggunakan

struktur Feistel yang memiliki kelebihan bahwa struktur enkripsi dan dekripsinya sama, meskipun menggunakan fungsi F yang tidak invertibel. Kelemahan Feistel yang utama adalah bahwa pada setiap ronde, hanya setengah data yang diolah. Sedangkan AES menggunakan struktur SPN (*Substitution Permutation Network*) yang memiliki derajat paralelisme yang lebih besar, sehingga diharapkan lebih cepat dari pada Feistel (Malays et al., n.d.).

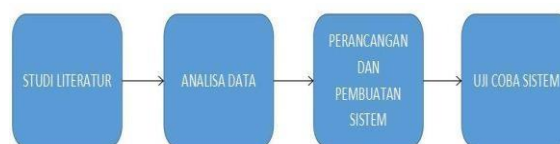
Kelemahan SPN pada umumnya (termasuk pada Rijndael) adalah berbedanya struktur enkripsi dan dekripsi sehingga diperlukan dua algoritma yang berbeda untuk enkripsi dan dekripsi. Dan tentu pula tingkat keamanan enkripsi dan dekripsinya menjadi berbeda. AES memiliki blok masukan dan keluaran serta kunci 128 bit. Untuk tingkat keamanan yang lebih tinggi, AES dapat menggunakan kunci 192 dan 256 bit. Setiap masukan 128 bit plaintext dimasukkan ke dalam state yang berbentuk bujursangkar berukuran 4×4 byte. State ini di-XOR dengan key dan selanjutnya diolah 10 kali dengan substitusi- transformasi *linear-Addkey*. Dan di akhir diperoleh ciphertext (Enkripsi Algoritma AES (Advanced Encryption Standard), n.d.).

Berikut ini adalah operasi Rijndael (AES) yang menggunakan 128 bit kunci:

1. Ekspansi kunci utama (dari 128 bit menjadi 1408 bit);
2. Pencampuran *subkey*;
3. Ulang dari $i=1$ sampai $i=10$
Transformasi : ByteSub (substitusi per byte) ShiftRow (Pergeseran byte perbaris) MixColumn (Operasi perkalian $GF(2)$ per kolom);
4. Pencampuran *subkey* (dengan XOR);
5. Transformasi : ByteSub dan ShiftRow;
6. Pencampuran *subkey*.

3. METODE PENELITIAN

Langkah yang dilakukan dalam penelitian diawali dengan studi literatur tentang kriptografi, khususnya algoritma AES. Langkah selanjutnya adalah menganalisis data dan mempelajari apa yang dilakukan untuk keamanan data. Selanjutnya membuat rancangan aplikasi berdasarkan literature review dan analisis data untuk



membuat aplikasi keamanan data berbasis web. Setelah aplikasi dibuat, sistem akan diuji.

Gambar 3. 1 Metode Penelitian

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 standarisasi 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. AES ini merupakan algoritma *block cipher* dengan menggunakan sistem permutasi dan substitusi (*P-Box* dan *S-Box*) bukan dengan jaringan Feistel sebagaimana *block cipher* pada umumnya. Jenis AES terbagi 3, yaitu AES-128, AES-192, dan AES-256. Pengelompokan jenis AES ini adalah berdasarkan panjang kunci yang digunakan. Angka-angka di belakang kata AES menggambarkan panjang kunci yang digunakan pada tiap-tiap AES. Selain itu, hal yang membedakan dari masing-masing AES ini adalah banyaknya *round* yang dipakai. AES-128 menggunakan 10 round, AES-192 sebanyak 12 round, dan AES-256 sebanyak 14 round.

AES memiliki ukuran *block* yang tetap sepanjang 128 bit dan ukuran kunci sepanjang 128, 192, atau 256 bit. Tidak seperti Rijndael yang *block* dan kuncinya dapat berukuran kelipatan 32 bit dengan ukuran minimum 128 bit dan maksimum 256 bit. Berdasarkan ukuran *block* yang tetap, AES bekerja pada matriks berukuran 4×4 di mana tiap-tiap sel matriks terdiri atas 1 byte (8 bit). Sedangkan Rijndael sendiri dapat mempunyai ukuran matriks yang lebih dari itu dengan menambahkan kolom sebanyak yang diperlukan. Blok chipper tersebut dalam pembahasan ini akan diasumsikan sebagai sebuah kotak. Setiap plaintext akan dikonversikan terlebih dahulu ke

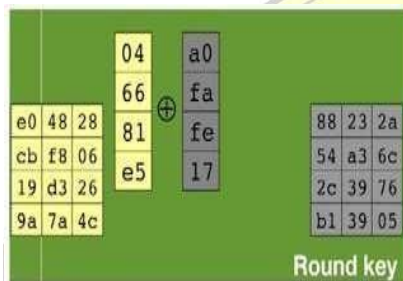
dalam blok-blok tersebut dalam bentuk heksadesimal. Barulah kemudian blok itu akan diproses dengan metode yang akan dijelaskan.

4. HASIL DAN PEMBAHASAN

4.1 Proses Enkripsi AES-128

Berikut adalah ringkasan dari algoritma AES yang bekerja di blok 128bit menggunakan kunci 128bit (selain proses pembuatan round kunci).

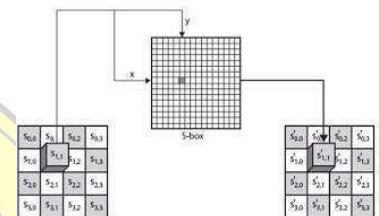
1. *AddRoundKey* : XOR state awal (*plainteks*) dengan *cipherkey*. Langkah ini disebut *initial round*.



Gambar 4.1 Add Round Key

2. Blok : Blok yang didapat dari proses XOR antara state awal (*plainteks*) dengan cipher key akan masuk ke tahap selanjutnya dan mengalami putaran sebanyak $Nr - 1$ kali (Teguh Utomo & Pradana, 2022). Langkah yang dilakukan dalam setiap putaran adalah :
 - a. *SubBytes* : Substitusi byte dengan S- box (tabel substitusi).
 - b. *ShiftRows* : Memindahkan baris array state dengan wrapping. Prinsip dari *Sub Bytes* adalah menukar isi matriks/tabel yang ada dengan matriks/tabel lain yang disebut dengan Rijndael S- Box. Di bawah ini adalah contoh *Sub Bytes* dan Rijndael S-Box. Baris pertama tidak dilakukan pergeseran, baris kedua dilakukan pergeseran 1 *byte*,

baris ketiga dilakukan pergeseran 2 *byte*, dan baris keempat dilakukan pergeseran 3 *byte*. Pergeseran tersebut terlihat dalam sebuah blok adalah sebuah pergeseran tiap elemen ke kiri tergantung berapa *byte* tergesernya, tiap pergeseran 1 *byte* berarti bergeser ke kiri sebanyak satu kali.

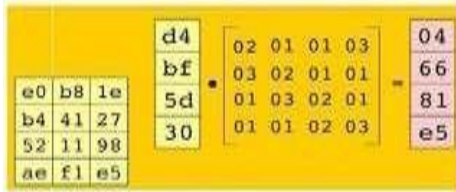


Gambar 4.2 Ilustrasi Sub Bytes

- c. *MixColumns* : Acak data pada setiap kolom *state array*. Yang terjadi saat *Mix Column* adalah mengalikan tiap elemen dari blok chipper dengan matriks yang ditunjukkan oleh Gambar 6. Tabel sudah ditentukan dan siap pakai. Pengalihan dilakukan seperti perkalian matriks biasa yaitu menggunakan *dot product* lalu perkalian keduanya dimasukkan ke dalam sebuah blok chipper baru. Ilustrasi dalam gambar 7 akan menjelaskan mengenai bagaimana perkalian ini seharusnya dilakukan. Dengan begitu seluruh rangkaian proses yang terjadi pada AES telah dijelaskan dan selanjutnya adalah menerangkan mengenai penggunaan tiap-tiap proses tersebut.

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

Gambar 4. 3 Tabel untuk Mix Coloumn

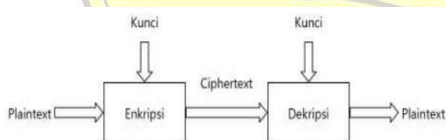


Gambar 4. 4 Ilustrasi Mix Column

- d. *AddRoundKey* : Melakukan XOR antara state saat ini dengan *round key*.

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

Gambar 4. 5 Rijndael S-Box



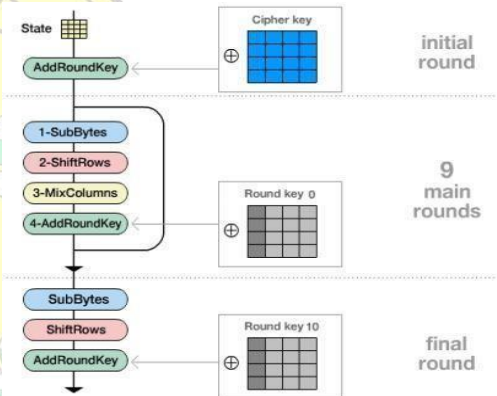
Gambar 4. 6 Proses Enkripsi AES-128

4.2 Proses Dekripsi AES

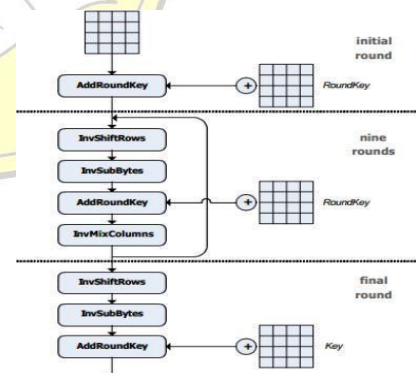
Langkah dekripsi AES, juga dikenal sebagai *Invers Cipher* dari algoritma Rijndael, yang beroperasi blok 128bit dengan kunci 128bit, adalah :

1. *InitialRound* : Tahap *AddRoundKey* yang melakukan XOR antara state awal (*ciphertext*) dan kunci enkripsi. Langkah ini juga disebut *InitialRound*.
2. Putaran sebanyak $Nr - 1$ kali. Proses yang terjadi pada setiap putaran yaitu :

- a. *InvShiftRow* : Memindahkan baris *state array* dengan wrapping.
 - b. *InvByteSub* : Substitusi byte dengan tabel substitusi kebalikan (*inverse S-box*).
 - c. *AddRoundKey* : Yaitu XOR antara state saat ini dengan *round key*.
 - d. *InvMixColumn*: Acak data di setiap kolom *state array*.
3. *Final Round* : Langkah untuk putaran terakhir :
- a. *InvShiftRow*,
 - b. *InvByteSub*,
 - c. *AddRoundKey*



Gambar 4. 7 Proses Dekripsi AES



Gambar 4. 8 Skema Enkripsi dan Dekripsi AES

4.3 Diagram Alir AES

Kembali melihat diagram yang ditunjukkan oleh Gambar 1. Seperti yang terlihat semua proses yang telah dijelaskan sebelumnya

terdapat pada diagram tersebut. Yang artinya adalah mulai dari ronde kedua, dilakukan pengulangan terus menerus dengan rangkaian proses *Sub Bytes*, *Shift Rows*, *Mix Columns*, dan *Add Round Key*, setelah itu hasil dari ronde tersebut akan digunakan pada ronde berikutnya dengan metode yang sama. Namun pada ronde kesepuluh, Proses *Mix Columns* tidak dilakukan, dengan kata lain urutan proses yang dilakukan adalah *Sub Bytes*, *Shift Rows*, dan *Add Round Key*, hasil dari *Add Round Key* inilah yang dijadikan sebagai *chiperteks* dari AES.

	Round 2	Round 3	Round 4	Round 5	Round 6
After SubBytes	49 45 7f 7f 4e 0b 3f 02 c2 96 07 51 38 71 1a 8b	ee 47 13 45 71 e3 16 23 e7 71 46 5a 7b e7 55 2a	32 83 e3 28 50 ea 11 e7 2f 5a e8 6a 28 07 01 94	a1 08 25 97 4f 1b e6 6e 42 7b 96 ea 6b ba 53 2e	a1 78 10 0c 43 47 08 05 4a 7b 5d 03 0a d1 23 6e
After ShiftRows	49 45 7f 7f ab 10 03 da e7 53 d3 94 36 89 11 1a	ee 47 13 45 31 52 23 72 e8 5a e8 11 58 7b e8 05	32 83 e3 28 e4 11 e7 33 e8 6a 2f 3a 94 28 d7 27	a1 08 25 97 3b e8 6e 4f 34 ea e2 6b 1e 9b ba 53	a1 78 10 0c 41 e8 25 43 3a 03 ea 19 6e 7c d1 23
After MixColumns	18 1b 0a 13 48 3a e7 94 c8 5a e8 11 15 e8 e8 01	11 10 53 3a e8 5a e8 11 39 83 e7 03 23 33 5c 0d	04 03 e2 5a 48 11 e7 33 e8 6a 2f 3a 48 71 2a 05	23 0a 96 4e 43 11 3a 6e a3 d1 53 e7 e8 6a 2f 3a	4b 2b 53 97 41 e8 25 43 3a 03 ea 19 4a 83 ea 08
Round Key	03 1a 59 32 39 39 03 e5 e8 6a 2f 3a e8 71 2a 05	47 2a 6a 47 2a 6a 47 2a 6a 47 2a 6a	04 03 e2 5a 43 11 3a 6e 43 11 3a 6e 43 11 3a 6e	04 7b 96 ea 08 7b 96 ea 08 7b 96 ea 08 7b 96 ea	01 13 0b 0e 01 13 0b 0e 01 13 0b 0e 01 13 0b 0e
After AddRoundKey	0a 11 02 01 4f e8 d7 82 48 3a e7 94 11 e7 d8 5a	ee 00 38 01 ee 00 38 01 ee 00 38 01 ee 00 38 01	e7 e8 03 51 47 e3 16 23 e8 6a 2f 3a 48 71 2a 05	f1 e3 16 23 f1 e3 16 23 f1 e3 16 23 f1 e3 16 23	24 3a 03 02 0e 41 ea e2 4a 7b 5d 03 17 1b 08 05

Gambar 4. 9 Ilustrasi Ronde 2 hingga Ronde 6

	Round 7	Round 8	Round 9	Round 10
After SubBytes	e7 27 9b 54 ab 93 43 55 31 93 40 2a e9 4f d7 22	3a 03 da 0a da 43 3a 55 ab 2c 99 da e2 c9 c0 04 e8	01 72 4c 97 e8 6a e8 90 7a 52 4e e7 8c d8 93 e5	09 0b 2d a2 08 11 32 2e 49 01 7a 2c 72 24 94 b5
After ShiftRows	e7 27 9b 54 83 43 55 ab 49 3a 31 49 9c 0c 07 c3	3a 03 da 0a da 3b e3 64 83 da e2 2c 8a 7e c8 c0 4c	01 72 4c 97 6e e8 90 e8 4e e7 8a e3 e8 8c d8 95	e8 0b 2d a2 11 22 2a 05 7a 52 4e e7 05 12 5f 84
After MixColumns	1a 44 37 34 15 18 4e 2a 05 15 5a 2b 8f e8 47 e2	0a 03 04 f4 51 e8 76 13 2f 09 ad 93 d1 e2 ea ea	41 40 a3 4e 37 da 7d 9e 54 ea 3a 42 e8 45 ak 0a	41 40 a3 4e 37 da 7d 9e 54 ea 3a 42 e8 45 ak 0a
Round Key	0a 1c 61 0a 54 5f 06 08 07 e9 4f e8 0a 71 02 22	0a 03 04 f4 02 08 2b 9d 73 ea 85 21 23 d2 1a 72	0a 19 28 07 77 fa 01 5e 8a d8 2f 00 01 21 41 6e	0b e8 fa 1a 18 ea 2f 63 09 21 0e 5e 08 18 e8 1a
After AddRoundKey	0a 19 28 07 41 49 e0 0c 42 0a 19 04 b1 1f 83 0e	0a 03 04 f4 03 45 5d 94 3a 19 9b 0a 00 2a 0e 05	4b 59 0b 1b 40 2a e3 e3 82 3a 1f 62 3e 84 e7 42	0b e8 fa 1a 22 d5 11 6a 8a 09 08 3b 1e e8 97 32

Gambar 4. 10 Ilustrasi Ronde 7 hingga Ronde 10

4.4 Implementasi AES

AES atau algoritma Rijndael sebagai salah satu algoritma yang penting tentu memiliki berbagai kegunaan yang sudah diaplikasikan atau diimplementasikan di kehidupan sehari-hari

yang tentu saja membutuhkan suatu perlindungan atau penyembunyian informasi di dalam prosesnya. Salah satu contoh penggunaan AES adalah pada kompresi 7-Zip. Salah satu proses di dalam 7-Zip adalah mengenkripsi isi dari data dengan menggunakan metode AES-256. Yang kuncinya dihasilkan melalui fungsi *Hash*. Perpaduan ini membuat suatu informasi yang terlindungi dan tidak mudah rusak terutama oleh virus yang merupakan salah satu musuh besar dalam dunia komputer dan informasi karena sifatnya adalah merusak sebuah data.

Hal yang serupa digunakan pada WinZip sebagai salah satu perangkat lunak yang digunakan untuk melakukan kompresi. Tapi prinsip kompresi pun tidak sama dengan prinsip enkripsi. Karena kompresi adalah mengecilkan ukuran suatu data, biasanya digunakan kode Huffman dalam melakukan hal tersebut. Contoh penggunaan lain adalah pada perangkat lunak *DiskCryptor* yang kegunaannya adalah mengenkripsi keseluruhan isi disk/partisi pada sebuah komputer. Metode enkripsi yang ditawarkan adalah menggunakan AES-256, Twofish, atau Serpent.

5. KESIMPULAN

Melindungi data dari serangan merupakan hal yang sulit. Salah satu cara untuk mengamankan data dari serangan adalah dengan menggunakan enkripsi. Salah satunya menggunakan metode enkripsi AES yang sudah dijabarkan dalam makalah ini. Dirancang untuk menggantikan DES (*launching* akhir 2001), menggunakan *variable length block chipper*, *key length*: 128-bit, 192-bit, 256-bit, dapat diterapkan untuk smart card. Algoritma Rijndael yang ditetapkan sebagai AES memiliki karakteristik yang istimewa yang menjadikannya mendapat status tersebut. Dalam hal ini pula maka algoritma ini perlu lah untuk dipelajari karena penggunaannya di kehidupan sehari-hari sudah sangatlah banyak dan hal ini akan berguna dalam pengembangan dari teknologi kriptografi agar dapat menemukan terobosan-terobosan baru.

6. UCAPAN TERIMAKASIH

Kami mengucapkan terima kasih yang sebesar-besarnya kepada semua pihak yang telah

memberikan dukungan dan pendanaan bagi penelitian ini. Terutama, kami berterima kasih kepada Semua pihak atas bantuan yang telah memungkinkan penelitian ini terlaksana. Kami juga berterima kasih kepada rekan-rekan satu tim di kelas Informatika Universitas Persada Indonesia Y. A. I. yang telah memberikan kontribusi berharga selama proses penelitian. Dukungan dan kerja sama dari berbagai pihak sangat berarti dalam keberhasilan penelitian ini.

Dengan kalimat ucapan terima kasih ini, kami berharap dapat mengakui dan menghargai kontribusi serta dukungan dari pihak-pihak yang telah membantu dalam pelaksanaan penelitian ini.

DAFTAR PUSTAKA

- Anwar, S. (2017). *IMPLEMENTASI PENGAMANAN DATA DAN INFORMASI DENGAN METODE STEGANOGRAFI LSB DAN ALGORITMA KRIPTOGRAFI AES*.
Enkripsi Algoritma AES (Advanced Encryption Standard). (n.d.).
- Hidayati, L. N., Fitriana, G. F., & Adam, I. F. (2021). Perbandingan Keacakan Citra Enkripsi Algoritma AES dan Camelia Uji NPCR dan UACI. *JURIKOM (Jurnal Riset Komputer)*, 8(6), 274. <https://doi.org/10.30865/jurikom.v8i6.3624>
- Malays, E., Sakti, S., & Basry, A. (n.d.). *Petunjuk Pemanfaatan Load Balancing dan Failover Dalam Perencanaan Pengembangan Jaringan Komputer untuk Menghindari Down Time*.
- Maulana, A., & Fajrin, A. A. (2018). Penerapan Data Mining Untuk Analisis Pola Pembelian Konsumen Dengan Algoritma Fp-Growth Pada Data Transaksi Penjualan Spare Part Motor. *Klik - Kumpulan Jurnal Ilmu Komputer*, 5(1), 27. <https://doi.org/10.20527/klik.v5i1.100>
- Meko, D. A. (2018). Perbandingan Algoritma DES, AES, IDEA Dan Blowfish dalam Enkripsi dan Dekripsi Data. *Jurnal Teknologi Terpadu*, 4(1).
- Ramadhan, Z., Zarlis, M., Efendi, S., Putera, A., & Siahaan, U. (2018). Perbandingan Algoritma Prim Dengan Algoritma Floyd-Warshall Dalam Menentukan Rute Terpendek (Shortest Path Problem). In *JURIKOM* (Vol. 5, Issue 2). <http://ejournal.stmik-budidarma.ac.id/index.php/jurikom|Page|130>
- Teguh Utomo, A., & Pradana, R. (2022). IMPLEMENTASI ALGORITMA ADVANCED ENCRYPTION STANDARD (AES-128) UNTUK ENKRIPSI DAN DEKRIPSI FILE. In *Seminar Nasional Mahasiswa Fakultas Teknologi Informasi (SENAFTI) Jakarta-Indonesia*.