Jurnal Teknik Mesin, Industri, Elektro Dan Informatika (JTMEI)
Vol.2, No.2 Juni 2023
e-ISSN: 2963-7805; p-ISSN: 2963-8208, Hal 45-56

Keamanan *E-Voting* Di Indonesia Melalui Pemanfaatan Kriptografi Pada Sistem AES *(Advance Encryption Standard)*

Fefiana Diny Hermawati[1)], Muhlis Tahir[2)], Muafa Syaifurrohman[3)], Muzayyanatul Hikmah [4)], Jaya Abadi Amroin[5)], Mochamad Bahruddin[6)] dan Irsyad Irsyad[7)]
[1),2),3),4),5),6),7)] Pendidikan Informatika, Fakultas Ilmu Pendidikan, Universitas Trunojoyo Madura
Korespondensi penulis: fefianadiny@gmail.com

Abstract*. As a democratic country, voting is a mandatory and routine agenda for our country when choosing leaders in an organization to the state level. The paper-based voting system that has been used so far has several weaknesses such as ballot damage, vote counting errors, susceptibility to fraud, and delayed election results. To overcome these issues, a more secure and guaranteed electronic voting system is needed. The shift from conventional media to various media used for opinion polling, such as social media/internet, has occurred in this technological era. The E-Voting system has been confirmed as safe and in line with the latest technological advancements. To enhance its security level, the system can use various types of cryptographic algorithms, including AES. Cryptography can be the solution in maintaining information security such as confidentiality, data integrity, non-repudiation, and authentication.*

Keywords*: AES, encryption, security, e-voting*

Abstrak. Sebagai negara yang demokrasi, pemungutan suara ini merupakan agenda wajib dan rutin bagi negara kita ketika sedang memilih pemimpin dalam suatu organisasi hingga negara. Sistem pemungutan suara kertas yang telah digunakan selama ini memiliki beberapa kelemahan seperti kerusakan surat suara, kesalahan dalam menghitung suara, mudahnya terjadinya kecurangan dan pengumuman hasil pemilu yang memakan waktu lama. Untuk mengatasi hal tersebut, diperlukan sebuah sistem pemungutan suara elektronik yang lebih aman dan terjamin. Pergeseran penggunaan media yang dahulu konvensional dan di era teknologi saat ini sudah banyak beragam media yang digunakan untuk jejak pendapat tersebut di antaranya media sosial/internet. Sistem E-Voting telah dipastikan aman dan sejalan dengan kemajuan teknologi terkini. Untuk menambah tingkat keamanannya, sistem tersebut bisa menggunakan berbagai jenis algoritma kriptografi, termasuk AES. Dalam hal menjaga keamanan informasi seperti kerahasiaan, keutuhan data, ketiadaan penyangkalan, dan otentikasi, kriptografi bisa menjadi solusinya.

Kata kunci: AES, enkripsi, keamanan, e-voting

LATAR BELAKANG

Sistem pemungutan suara elektronik (e-Voting) telah menjadi topik yang semakin populer di seluruh dunia, termasuk di Indonesia. Dalam era digital seperti sekarang, banyak negara telah mengadopsi sistem e-Voting sebagai alternatif untuk pemungutan

Received April 07, 2023; Revised Mei 02, 2023; Juni 01, 2023
* Fefiana Diny Hermawati, fefianadiny@gmail.com

suara manual yang lebih lambat dan rentan terhadap kecurangan. Sistem e-Voting memungkinkan pemilih untuk memberikan suara mereka dengan cepat dan mudah, serta mengurangi kemungkinan kesalahan penghitungan suara.

Namun, sistem e-Voting juga memiliki tantangan tersendiri, terutama dalam hal keamanan informasi dan keandalan. Karena sifatnya yang online, sistem e-Voting dapat rentan terhadap serangan *cyber* dan kebocoran data. Oleh karena itu, penting untuk memastikan bahwa sistem e-Voting yang digunakan aman dan terlindungi dari ancaman siber.

Keamanan dan keandalan merupakan dua aspek penting dalam sistem e-Voting. Untuk memastikan bahwa sistem tersebut aman dari serangan siber dan kecurangan, diperlukan teknologi yang canggih dan terbaru. Salah satu solusi untuk meningkatkan keamanan informasi dalam sistem e-Voting adalah dengan menggunakan kriptografi.

Menurut Direktur Pusat Teknologi Informasi dan Komunikasi (BPPT 2013) Pemanfaatan teknologi informasi dan komunikasi (TIK) dalam e-Voting dapat memastikan keberlangsungan dan transparansi pemungutan dan perhitungan suara. Dalam konteks ini, e-Voting dapat dijadikan sebagai solusi yang tepat untuk melaksanakan pemilihan umum yang jujur, akuntabel, dan dapat diaudit di setiap tahapannya.

E-voting memiliki tujuan untuk menjamin kerahasiaan dan keamanan dalam sistemnya menurut (Ridwan, Arifin, and Yulianto 2016). Oleh karena itu, unsur-unsur yang terdapat dalam e-voting mencakup:

1. *Eligibility* memiliki arti bahwa hanya mereka yang terdaftar sebagai pemilih yang memenuhi syarat dapat melakukan pemilihan.
2. *Unreusability* adalah keadaan di mana setiap pemilih hanya dapat memberikan satu suara atau pilihan.
3. *Anonymity* adalah menjaga kerahasiaan identitas pemilih dan menjaga kerahasiaan pilihannya.
4. *Accuracy* berarti suara atau pilihan yang diberikan oleh pemilih harus akurat dan tidak dapat diubah, dihapus, atau ditambah setelah proses pemilihan berakhir.
5. *Fairness* Perhitungan suara sebelum pemilihan ditutup tidak dapat dilakukan.
6. *Vote and Go* berarti pemilih hanya dapat memberikan suaranya dan meninggalkan tempat pemilihan.

7. *Public Verifiability* artinya bahwa proses pemilihan dapat diperiksa oleh siapa saja.

Kriptografi merupakan teknik pengamanan informasi yang mengenkripsi data menjadi bentuk yang tidak dapat dibaca oleh pihak yang tidak berwenang. Dalam sistem e-Voting, kriptografi dapat digunakan untuk mengamankan informasi seperti identitas pemilih, suara yang diberikan, dan hasil pemilihan.

Artikel ini akan membahas lebih lanjut tentang pemanfaatan kriptografi, khususnya algoritma AES, dalam sistem e-Voting untuk meningkatkan keamanan dan keandalan.

KAJIAN TEORITIS

A. Kriptografi

Kriptografi berasal dari kata-kata Yunani, yaitu cryptos yang berarti "secret" atau rahasia, dan graphein yang artinya "writing" atau tulisan. Oleh karena itu, kriptografi dapat diartikan sebagai tulisan rahasia. Menurut Schneier, kriptografi merupakan ilmu dan seni untuk menjaga keamanan pesan, sementara menurut Menezes, kriptografi adalah ilmu yang mempelajari teknik-teknik matematika untuk melindungi aspek keamanan informasi seperti kerahasiaan, integritas data, dan otentikasi. Tujuan dari kriptografi adalah memberikan layanan keamanan informasi, yang meliputi kerahasiaan, integritas data, otentikasi, dan non-repudiation.

B. Algoritma AES

Advanced Encryption Standard (AES) adalah sebuah algoritma kriptografi yang dapat digunakan untuk melindungi data dengan menggunakan gulir ciphertext simetris yang mampu mengenkripsi dan mendekripsi data. Algoritma AES dapat mengubah informasi menjadi ciphertext melalui enkripsi dan mengubah kembali ciphertext menjadi plaintext melalui dekripsi. Algoritma ini menggunakan kunci kriptografi dengan panjang 128, 192, atau 256 bit untuk mengenkripsi dan mendekripsi data pada reel 128-bit.

AES adalah kelanjutan dari algoritma enkripsi standar DES yang masa berlakunya diperkirakan telah berakhir karena masalah keamanan. AES dianggap lebih aman, efisien, dan hemat biaya untuk diterapkan pada berbagai perangkat lunak dan mesin, serta memiliki karakteristik dan aplikasi algoritme yang lebih baik.

Algoritma kriptografi Rijndael Belgia memenangkan Festival Algoritma Kriptopgrafi pengganti DES yang diselenggarakan NIST pada tahun 2001. Pada tahun

2002, setelah NIST mencoba beberapa strategi standardisasi yang berbeda, itu menjadi algoritma kriptografi standar.

AES adalah salah satu algoritma kriptografi kunci simetris yang paling banyak digunakan pada tahun 2006 dan menggunakan sistem permutasi dan penggantian (PBox dan S-Box) tanpa menggunakan jaringan Feistel sebagai cipher blok. Karakteristik, keamanan, biaya dan aplikasi algoritme adalah tiga penentu utama untuk menetapkan tolak ukur AES. Ada tiga jenis AES", yaitu:

Tabel 1. Perbandingan Jumlah Putaran dan Kunci

	Jumlah Kunci (Nk)	Jumlah Putaran (Nr)
AES-128 4 10	4	10
AES-192 6 12	6	12
AES-256 8 14	8	14

Sumber: (Prasetyo and Suryana 2016)

Dalam konteks ini, terdapat lima jenis unit data yang digunakan dalam enkripsi AES, yaitu bit sebagai unit data terkecil yang mewakili nilai digit dalam sistem biner, byte dengan ukuran 8 bit, word dengan ukuran 32 bit atau 4 byte, block dengan ukuran 128 bit atau 16 byte, dan state yang merupakan block berukuran 4x4 byte yang disusun dalam bentuk matriks (Prasetyo and Suryana 2016).

C. E-Voting

E-voting atau pemilihan secara elektronik menggunakan teknologi informasi, dan salah satu standar enkripsi yang digunakan dalam proses ini adalah Algoritma AES. AES adalah sebuah algoritma enkripsi kunci-simetris yang diadopsi oleh pemerintah Amerika Serikat. Algoritma ini dipublikasikan oleh Institut Nasional Standar dan Teknologi (NIST) sebagai Standar Pemrosesan Informasi Federal (FIPS) dengan nomor publikasi 197 (FIPS197) pada tanggal 26 November 2001 (Anwar et al. 2018). Proses enkripsi AES terdiri dari empat tahap yaitu SubBytes, ShiftRows, MixColumns, dan AddRoundKey, yang dapat dipantau oleh perangkat elektronik selama proses pemilihan, termasuk dalam proses pendaftaran pemilih, pemungutan suara, dan penghitungan suara secara digital. Keunggulan e-voting mencakup efisiensi logistik karena sebagian besar proses dilakukan secara digital, akselerasi pemungutan dan penghitungan suara, dan mengurangi kemungkinan kesalahan teknis. E-voting juga menjamin keaslian suara pemilih,

kerahasiaan pemilih, serta keakuratan hasil perhitungan suara (Ungkawa, Rosmala, and Fauzi 2021).

Pemungutan suara elektronik mengacu pada penggunaan teknologi informasi dan komunikasi untuk melakukan pemungutan suara. Menggunakan teknik ini seperti pedang bermata dua. Di satu sisi menawarkan banyak kenyamanan dan kecepatan, di sisi lain menciptakan titik lemah. Kelemahan potensial dalam pemungutan suara elektronik terkait dengan keamanan informasi. Menurut (Schneier 1996), berikut adalah beberapa Persyaratan dasar untuk pemungutan suara elektronik:

1) Hanya badan hukum yang berhak memilih.
2) Setiap orang tidak dapat memilih lebih dari satu kali
3) Tidak ada yang bisa mengetahui keputusan orang lain
4) Tidak ada yang bisa meniru suara orang lain
5) Tidak seorang pun dapat mengubah keputusan orang lain tanpa diketahui oleh pihak lain.
6) Setiap orang dapat memastikan pilihannya telah masuk ke pusat tabulasi suara
7) Setiap orang mengetahui siapa yang sudah memilih dan tidak memilih.

D. Keamanan Informasi

Informasi adalah sumber daya yang sangat berharga yang harus dijaga keamanannya di organisasi mana pun. Menurut (Rahmawati Agustina and Kurniati 2009) Aspek keamanan data adalah:

1. Kerahasiaan (confidentiality)

Hal ini merupakan aspek yang menghalangi pengungkapan informasi kepada pihak yang tidak berhak atas informasi tersebut.

2. Integritas Data (integrity)

Ada aspek untuk mencegah data diubah oleh orang yang tidak memiliki kewenangan untuk mengubah data. Untuk memenuhi kebutuhan tersebut diperlukan kemampuan untuk mengenali perubahan data yaitu penyisipan, penghapusan dan penggantian.

3. Ketersediaan (Availability)

Ini adalah aspek di mana informasi harus tersedia saat dibutuhkan.

4. Otentikasi (Authentication)

Ini adalah bagian dari memastikan keaslian informasi. Juga untuk memastikan legitimasi orang-orang yang berpartisipasi dalam pertukaran informasi.

5. Nir Penyangkalan (Non-repudiation)

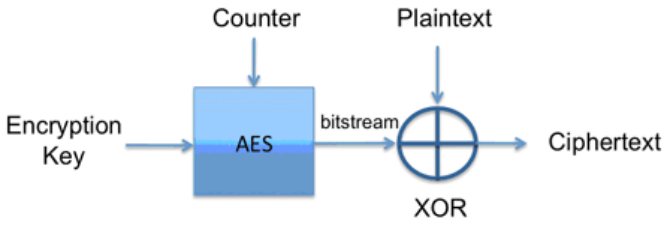
Ini memastikan bahwa para pihak tidak dapat menggugatnya di masa depan.

METODE PENELITIAN

Penelitian ini menggunakan metode deskriptif kualitatif dengan tujuan untuk menjelaskan bagaimana kriptografi dapat meningkatkan keamanan informasi pada sistem e-voting di Indonesia. Dalam penelitian ini, akan dibahas penggunaan algoritma dan protokol kriptografi yang sesuai dengan persyaratan dasar pada sistem e-voting.

HASIL DAN PEMBAHASAN

AES memiliki ukuran kunci sepanjang 128, 192, atau 256 bit dan ukuran blok tetap sepanjang 128 bit. Berbeda dengan Rijndael yang menetapkan ukuran minimum sebesar 128 bit dan maksimum sebesar 256 bit untuk kedua ukuran blok dan kunci, berdasarkan ukuran blok yang tepat, AES bekerja pada kerangka 4x4 di mana setiap sel jaringan terdiri dari 1 byte (8 bit). Sementara itu, Rijndael dapat meningkatkan ukuran matriks dengan menambahkan kolom sesuai kebutuhan. Blok chiper tersebut dalam pembahasan ini diasumsikan sebagai sebuah kotak. Pertama, setiap plainteks akan dikonversi menjadi blok heksadesimal tersebut. Baru kemudian blok tersebut akan diproses dengan metode yang akan dijelaskan.



Gambar 1. Bentuk Metode (Zacky 2016)

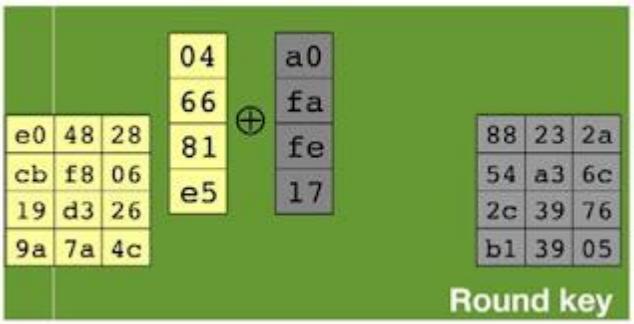
Secara keseluruhan, cara yang digunakan untuk melakukan proses enkripsi dalam algoritma ini dapat ditemukan di dalam Gambar 1.

Jurnal Teknik Mesin, Industri, Elektro Dan Informatika (JTMEI)
Vol.2, No.2 Juni 2023
e-ISSN: 2963-7805; p-ISSN: 2963-8208, Hal 45-56

Gambar2. Diagram AES (Zacky 2016)

Add Round

Adalah proses kunci menggabungkan chiper teks yang ada dengan chiper key menggunakan operasi XOR.



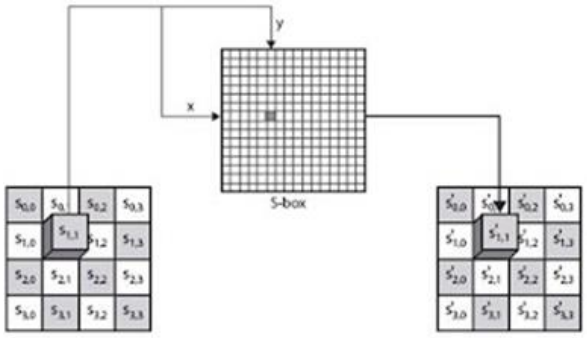
Gambar 3. Round Key (Zacky 2016)

Sub Bytes

Adalah prinsip mengganti nilai pada matriks atau tabel yang sudah ada dengan nilai pada matriks atau tabel lain yang disebut Rijndael 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

Gambar 6. Rijndael S-Box (Zacky 2016)



Gambar 5. Sub Bytes (Zacky 2016)

Shift Rows

Shift Rows adalah sebuah proses yang memindahkan setiap elemen dalam sebuah blok atau tabel pada setiap barisnya. Pada baris pertama tidak terjadi perpindahan, pada baris kedua setiap elemennya dipindahkan satu byte ke kiri, pada baris ketiga setiap elemennya dipindahkan dua byte ke kiri, dan pada baris keempat setiap elemennya dipindahkan tiga byte ke kiri. Pemindahan ini dapat dilihat pada sebuah blok sebagai perpindahan elemen-elemen ke kiri sejauh jumlah byte yang telah ditentukan, di mana perpindahan satu byte menghasilkan perpindahan sejauh satu kali ke kiri, menurut (Aria et al. 2023)

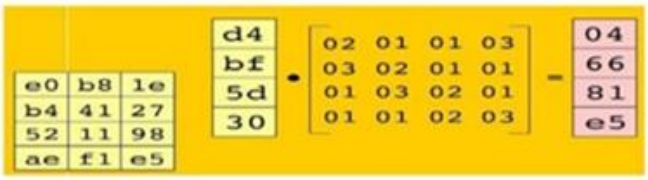
Mix Columns

Proses yang terjadi pada mix column adalah mengalikan setiap elemen blok chiper dengan matriks yang sudah ditentukan seperti yang ditunjukkan pada Gambar 6. Matriks ini sudah disiapkan sebelumnya dan siap digunakan. Perkalian pada mix column dilakukan dengan cara yang sama seperti perkalian matriks biasa, yaitu menggunakan dot product. Hasil perkalian kedua nilai dimasukkan ke dalam blok chiper baru. Cara melakukan perkalian ini dijelaskan pada ilustrasi dalam Gambar 7, (Aria et al. 2023).

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

Gambar 6. Tabel untuk mix column (Zacky 2016)

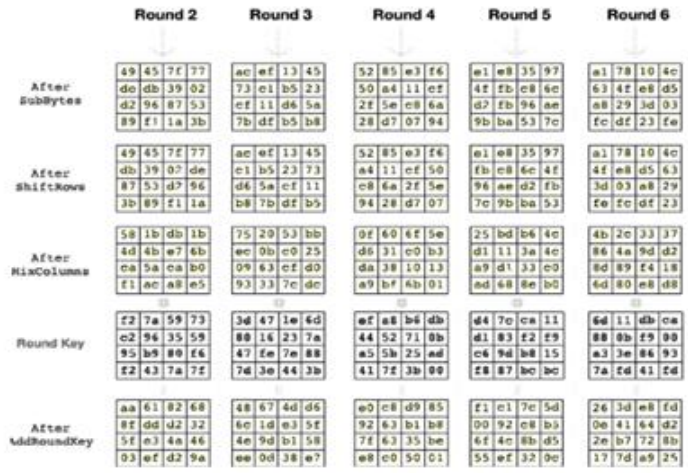
Jurnal Teknik Mesin, Industri, Elektro Dan Informatika (JTMEI)
Vol.2, No.2 Juni 2023
e-ISSN: 2963-7805; p-ISSN: 2963-8208, Hal 45-56



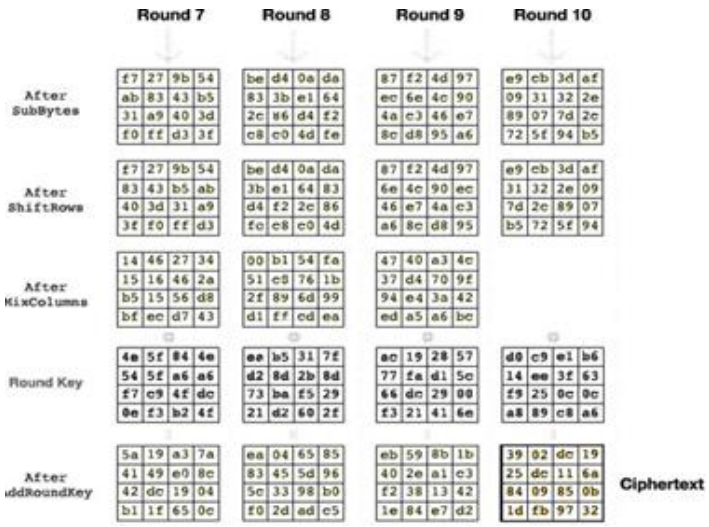
Gambar 7. Ilustrasi mix column (Zacky 2016)

Diagram Alir AES

Pada Gambar 2 terdapat seluruh proses algoritma AES yang telah dijelaskan sebelumnya. Proses dimulai dari ronde kedua dan diulangi secara berurutan dengan rangkaian Sub Bytes, Shift Rows, Mix Columns, dan Add Round Key. Hasil dari setiap ronde akan digunakan pada ronde berikutnya dengan metode yang sama. Pada ronde ke-10, tidak ada proses Mix Columns. Urutan proses pada ronde ke-10 adalah Sub Bytes, Shift Rows, dan Add Round Key, dan hasil dari proses Add Round Key ini menjadi chiperteks dari AES. Dengan memahami seluruh proses yang ada pada AES, maka algoritma tersebut dapat digunakan pada berbagai kasus yang terjadi dalam kehidupan sehari-hari. Untuk lebih detail, bisa dilihat pada Gambar 9 dan 10 yang menjelaskan kasus tersebut (Aria et al. 2023).



Gambar 9. Ilustrasi ronde 2 sampai (Zacky 2016)



Gambar 10. Ilustrasi ronde 7 sampai 10 (Zacky 2016)

Dibawah ini merupakan pembahasan keamanan informasi dengan memanfaatkan kriptografi:

1. Kerahasiaan (*confidentiality*)

Algoritma kriptografi sangat mendukung didalam aspek kerahasiaan ini yaitu dengan memanfaatkan algoritma enskripsi/deskripsi mulai dari simetri ataupun asimetri. Pada spek ini sangatlah berkaitan dengan adanya kunci yang mana jangan sampai kunci tersebut diketahui oleh pihak yang tidak berkepentingan. Algoritma simetri diantaranya DES, AES, Tripple DES, dll. Adapun algoritma asimetrik misalnya RSA, Knapsack, Rabin, Elgamal, dll (Rahmawati Agustina and Kurniati 2009).

2. Integritas Data (*integrity*)

Aspek integritas dapat memanfaatkan algoritma yang bersifat searah atau disebut "algoritma hash" dengan tujuan agar nilai yang keluar dari hash bisa dikembalikan lagi. Prakteknya yaitu pengirim akan menghitung nilai hash yang keluar dengan memasukkan pesan ke algoritma hash. Lalu setelah dihitung, nilai hash yang di daptkan digabungkan dengan pesan. Kemudian gabungan tersebut baru dikirimkan kepada pihak penerima. setelah itu penerima memisahkan kembali nilai hash dan pesan yang telah dia terima agar dapat mendapat nilai hash dari pesan yang diterimanya dengan cara memasukkan pesan kedalam algoritma hash. Kemudian nilai hash yang dihasilkan oleh perhitungan penerima dibandingkan dengan nilai hash yang dikirimkan oleh pengirim untuk memastikan bahwa pesan yang diterimanya tidak mengalami perubahan selama proses pengiriman dengan

memastikan nilai hash yang dihasilkan penerima itu sama dengan nilai hash yang pengirim kirim (Aria et al. 2023).

3. Otentikasi (*authentication*)

Untuk menjamin keamanan informasi, aspek pembuktian keaslian atau otentikasi dapat dilakukan melalui penggunaan sistem *digital signature*. Sistem *digital signature* memanfaatkan algoritma kriptografi untuk menghasilkan tanda tangan digital, menurut (Adminlp2m 2022).

4. Ketersediaan (*availability*)

Dalam sebuah keamanan informasi, aspek ketersediaan ini emiliki artian tersedianya semua informasi yang dicari ketika sedang dibutuhkan. Dalam hal ini tidak bisa di dukung dengan kriptografi dikarenakan keterbatasan kriptografi yang tidak mampu mencegah adanya sabotase dan pengeboman informasi ataupun ancaman-ancaman lainnya. Aspek ketersediaan ini dapat diwujudkan dengan Business Continuity Plan (BCP) serta Disaster Recovery Plan (DRP) yang bisa menyediakan informasi-informasi yang dicari (Rahmawati Agustina and Kurniati 2009).

KESIMPULAN DAN SARAN

Dalam upaya meningkatkan keamanan dan mengatasi beberapa kelemahan dalam sistem pemungutan suara kertas, diperlukan sebuah sistem pemungutan suara elektronik yang lebih aman dan terjamin. Pemanfaatan AES (Advanced Encryption Standard) dapat menjadi salah satu solusi untuk meningkatkan keamanan dalam sistem E-Voting. AES adalah algoritma kriptografi simetris yang dapat melakukan enkripsi dan dekripsi data menggunakan kunci kriptografi dengan panjang 128, 192, dan 256 bit. Ada tiga kriteria utama yang digunakan untuk menilai AES, yaitu keamanan, biaya, dan karakteristik serta aplikasi algoritma. Kriptografi dapat memberikan solusi untuk beberapa masalah yang timbul dalam sistem E-Voting, seperti kerahasiaan, keutuhan data, ketiadaan penyangkalan, dan otentikasi, dalam rangka menjaga keamanan informasi.

DAFTAR REFERENSI

Adminlp2m. 2022. "Mengenal Kriptografi : Definisi, Tujuan Dan Jenis-Jenisnya." *Lp2m.Uma*. Retrieved April 27, 2022 (https://lp2m.uma.ac.id/2022/04/26/mengenal-kriptografi-definisi-tujuan-dan-jenis-jenisnya/).

Anwar, Nizirwan, Munawwar, Muhammad Abduh, and Nugroho Budhi Santosa. 2018. "Komparatif Performance Model Keamanan Menggunakan Metode Algoritma AES 256 Bit Dan RSA." *Jurnal RESTI (Rekayasa Sistem Dan Teknologi Informasi)* 2(3):783–91. doi: 10.29207/resti.v2i3.606.

Aria, Mhd, Agung Widodo, Myra Thasandra, Septia Ona Sutra, Adnan Buyung Nasution, Ali Ikhwan, Universitas Islam Negeri, Sumatera Utara, Jl William, Iskandar V Ps, Medan Estate, Kec Percut, Sei Tuan, and Deli Serdang. 2023. "Pemanfaatan Kriptografi Dalam Mewujudkan Keamanan Informasi Pada E-Voting Di Kota Medan Dengan Menggunakan Algoritma AES." *Journal on Education* 05(03):6780–87.

BPPT. 2013. "E Voting Pilkades Jembrana, Sebuah Miniatur Pemilukada." *Bppt.Go.Id*. Retrieved (https://www.bppt.go.id/berita-bppt/e-voting-pilkades-jembrana-sebuah-miniatur-pemilukada).

Prasetyo, Ratno, and Asep Suryana. 2016. "Aplikasi Pengamanan Data Dengan Teknik Algoritma Kriptografi AES Dan Fungsi Hash SHA-1 Berbasis Desktop." *Jurnal Sisfokom (Sistem Informasi Dan Komputer)* 5(2):61–65. doi: 10.32736/sisfokom.v5i2.40.

Rahmawati Agustina, Esti, and Agus Kurniati. 2009. "Pemanfaatan Kriptografi Dalam Mewujudkan Keamanan Informasi Pada E-Voting Di Indonesia." *Seminar Nasional Informatika* 2009(semnasIF):23–2009.

Ridwan, Muhammad, Zainal Arifin, and Yulianto. 2016. "Rancang Bangun E-Voting Dengan Menggunakan Keamanan Algoritma Rivest Shamir Adleman (RSA) Berbasis Web (Studi Kasus : Pemilihan Ketua Bem Fmipa)." *Informatika Mulawarman : Jurnal Ilmiah Ilmu Komputer* 11(2):22. doi: 10.30872/jim.v11i2.210.

Schneier, Bruce. 1996. *Applied Cryptography, Second Edition: Protocols, Algorthms, and Source Code in C (Cloth)*. John Wiley & Sons, Inc.

Ungkawa, Uung, Dewi Rosmala, and Helmy Fauzi. 2021. "Penerapan Advance Encryption Standart Dalam Pengamanan Elektronik Voting." *Journal of Information Technology* 3(1):17–23. doi: 10.47292/joint.v3i1.51.

Zacky. 2016. "Enkripsi Algoritma AES (Advanced Encryption Standard)." *Kriptografi & Jaringan Komputer*. Retrieved April 25, 2022 (http://kriptografijaringan.blogspot.com/2016/03/enkripsi-algoritma-aes-advanced.html).