

**IMPLEMENTASI ALGORITMA *ADVANCED ENCRYPTION STANDARD* 256
DAN *SECURE HASH ALGORITHM* 256 PADA APLIKASI PENGAMANAN DATA
*E-VOTING***

SKRIPSI

Diajukan untuk memenuhi sebagian syarat memperoleh gelar Sarjana Matematika



Oleh:

Arya Shidika Listanto

NIM 2104269

**PROGRAM STUDI MATEMATIKA
FAKULTAS PENDIDIKAN MATEMATIKA DAN ILMU PENGETAHUAN ALAM
UNIVERSITAS PENDIDIKAN INDONESIA**

2025

LEMBAR HAK CIPTA
IMPLEMENTASI ALGORITMA *ADVANCED ENCRYPTION STANDARD*
256 DAN *SECURE HASH ALGORITHM* 256 PADA APLIKASI
PENGAMANAN DATA *E-VOTING*

Oleh:

Arya Shidika Listanto

2104269

Diajukan untuk memenuhi sebagian syarat memperoleh gelar Sarjana Matematika
pada Program Studi Matematika Fakultas Pendidikan Matematika dan Ilmu
Pengetahuan Alam

© Arya Shidika Listanto

Universitas Pendidikan Indonesia

Januari 2025

Hak Cipta dilindungi undang-undang

Skripsi ini tidak boleh diperbanyak seluruhnya atau sebagian dengan dicetak
ulang, difotokopi, atau cara lainnya tanpa izin penulis.

LEMBAR PENGESAHAN

ARYA SHIDIKA LISTANTO

IMPLEMENTASI ALGORITMA *ADVANCED ENCRYPTION STANDARD 256*
DAN *SECURE HASH ALGORITHM 256* PADA APLIKASI PENGAMANAN
DATA *E-VOTING*

Disetujui dan disahkan,

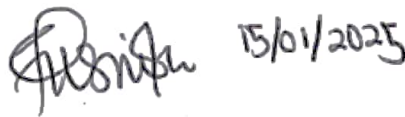
Pembimbing I



Dra. Hj. Rini Marwati, M.S.

NIP.196606251990012001

Pembimbing II



Isniet Yusnitha, M.Ed., Ph.D.

NIP. 198506092012122002

Mengetahui,

Ketua Program Studi Matematika



Dr. Kartika Yulianti, M.Si.

NIP. 198207282005012001

ABSTRAK

Sistem pemilihan berbasis elektronik (*e-voting*) menjadi alternatif yang efektif dan efisien untuk menggantikan metode tradisional. Penelitian ini bertujuan untuk merancang protokol keamanan *e-voting* menggunakan algoritma *Advanced Encryption Standard* (AES-256) dan fungsi hash *Secure Hash Algorithm* (SHA-256). Algoritma AES-256 digunakan untuk menjaga kerahasiaan data pilihan suara, sementara SHA-256 digunakan untuk memverifikasi keaslian dan integritas data pemilih serta suara. Program aplikasi *e-voting* dikembangkan menggunakan bahasa pemrograman *Python* dengan integrasi berbagai *library* untuk mendukung enkripsi, dekripsi, dan antarmuka pengguna. Hasil penelitian menunjukkan bahwa implementasi algoritma kriptografi ini mampu meningkatkan keamanan data *e-voting* dan mempermudah proses verifikasi, menjadikannya solusi yang andal untuk aplikasi pemilu berbasis teknologi.

Kata kunci: *Advanced Encryption Standard 256, e-voting, kriptografi, Secure Hash Algorithm 256*

ABSTRACT

Electronic voting (e-voting) systems offers an effective and efficient alternative to traditional voting methods. This study aims to design a secure e-voting protocol utilizing the Advanced Encryption Standard (AES-256) algorithm and the Secure Hash Algorithm (SHA-256). The AES-256 algorithm is employed to ensure the confidentiality of voting data, while SHA-256 is used to verify the authenticity and integrity of voter and ballot data. An e-voting application program was developed using the Python programming language, integrating various libraries to support encryption, decryption, and user interface functionalities. The research findings indicate that the implementation of these cryptographic algorithms enhances the security of e-voting data and simplifies the verification process, making it a reliable solution for technology-based electoral systems.

Keywords: *Advanced Encryption Standard 256, e-voting, cryptography, Secure Hash Algorithm 256*

DAFTAR ISI

LEMBAR HAK CIPTA	i
LEMBAR PENGESAHAN	ii
LEMBAR PERNYATAAN.....	iii
KATA PENGANTAR.....	iv
UCAPAN TERIMA KASIH	v
ABSTRAK	vi
ABSTRACT	vii
DAFTAR ISI	viii
DAFTAR GAMBAR	xi
DAFTAR TABEL	xiii
BAB I PENDAHULUAN.....	1
1.1 Latar Belakang	1
1.2 Rumusan Masalah	3
1.3 Tujuan Penelitian	4
1.4 Manfaat Penelitian	4
BAB II KAJIAN PUSTAKA	5
2.1 Teori Dasar Matematika	5
2.1.1 Aritmatika Modulo	5
2.1.2 Grup.....	5
2.1.3 Ring.....	5
2.1.4 Lapangan Galois (<i>Galois Field</i>)	6
2.2 Teori Dasar Kriptografi	9
2.2.1 Istilah Kriptografi (Munir, 2019).....	10
2.2.2 Kriptosistem	10
2.2.3 Block Cipher.....	11
2.2.4 Teori Coding	12
2.2.5 Protokol (Munir, 2019)	14
2.3 Advanced Encryption Standard (AES)	15
2.3.1 AddRoundKey	16

2.3.2	<i>SubBytes</i>	17
2.3.3	<i>ShiftRows</i>	19
2.3.4	<i>MixColumns</i>	19
2.3.5	<i>KeyExpansion</i>	21
2.3.6	<i>InvShiftRows</i>	22
2.3.7	<i>InvSubBytes</i>	22
2.3.8	<i>InvMixColumns</i>	23
2.4	Fungsi <i>Hash</i> (Munir, 2019).....	24
2.5	<i>E-Voting</i>	29
2.6	Bahasa Pemrograman <i>Python</i>	29
BAB III METODE PENELITIAN		31
3.1	Identifikasi Masalah	31
3.2	Model Dasar	32
3.2.1	AES-256.....	32
3.2.2	SHA-256	32
3.3	Pengembangan Model	33
3.4	Konstruksi Program	34
3.4.1	Protokol.....	34
3.4.2	Algoritma Deskriptif	35
3.4.3	Rancangan Tampilan.....	36
3.4.4	<i>Library Python</i>	38
3.5	Proses Validasi.....	39
3.6	Pengambilan Kesimpulan	39
BAB IV PEMBAHASAN		40
4.1	Skema Aplikasi <i>E-Voting</i> Menggunakan AES-256 dan SHA-256....	40
4.2	Konstruksi Aplikasi <i>E-Voting</i> menggunakan AES-256 dan SHA-256	41
4.2.1	<i>Pseudocode</i> Aplikasi <i>E-Voting</i> menggunakan AES-256 dan SHA-256.....	41
4.2.2	Tampilan Utama	44
4.3	Validasi Aplikasi <i>E-Voting</i> menggunakan AES-256 dan SHA-256..	49
4.3.1	Validasi <i>Password</i> Panitia	49
4.3.2	Validasi ID Pemilih	50

4.3.3 Validasi Pilihan Voting Pemilih	51
BAB V KESIMPULAN DAN SARAN	54
5.1 Kesimpulan	54
5.2 Saran	54
DAFTAR PUSTAKA	56
LAMPIRAN	59

DAFTAR GAMBAR

Gambar 2.1 Diagram Enkripsi dan Dekripsi	11
Gambar 2.2 Skema Enkripsi dan Dekripsi pada Cipher Block	12
Gambar 2.3 ASCII.....	13
Gambar 2.4 AES (Ariyus, 2008).....	16
Gambar 2.5 Proses AddRoundKey.....	17
Gambar 2.6 Contoh AddRoundKey	17
Gambar 2.7 Proses SubBytes	18
Gambar 2.8 Contoh SubBytes.....	19
Gambar 2.9 Proses ShiftRows.....	19
Gambar 2.10 Contoh ShiftRows	19
Gambar 2.11 Proses MixColumns.....	20
Gambar 2.12 Proses InvShiftRows.....	22
Gambar 2.13 Inverse S-Box.....	23
Gambar 2.14 Proses InvSubBytes	23
Gambar 2.15 Proses InvMixColumns.....	23
Gambar 2.16 $k[0] \dots k[63]$	28
Gambar 3.1 Skema AES-256	32
Gambar 3.2 Skema SHA-256.....	33
Gambar 3.3 Skema Fungsi Hash	33
Gambar 3.4 Pengembangan Model	34
Gambar 3.5 Rancangan Program Input Kunci oleh Panitia	36
Gambar 3.6 Rancangan Program Input ID Pemilih oleh Panitia.....	36
Gambar 3.7 Rancangan Program Registrasi ID oleh Pemilih	36
Gambar 3.8 Rancangan Program Generate Token oleh Pemilih.....	37
Gambar 3.9 Rancangan Program Voting oleh Pemilih.....	37
Gambar 3.10 Rancangan Program Verifikasi Suara oleh Pemilih	37
Gambar 3.11 Rancangan Program Cek Hasil Suara	38
Gambar 4.1 Skema <i>E-Voting</i> menggunakan AES-256 dan SHA-256.....	40
Gambar 4.2 Tampilan Halaman Menu Utama	45
Gambar 4.3 Tampilan Halaman Input Password Panitia	45
Gambar 4.4 Tampilan Halaman Input Kunci Panitia	46
Gambar 4.5 Halaman Voting Selesai atau Input ID	46
Gambar 4.6 Tampilan Halaman Input ID Panitia.....	46
Gambar 4.7 Tampilan Input ID Pemilih	47
Gambar 4.8 Tampilan Halaman Generate Token.....	47
Gambar 4.9 Tampilan Halaman Voting.....	48
Gambar 4.10 Tampilan Halaman Verifikasi dengan Token.....	48
Gambar 4.11 Halaman Hasil Voting	49
Gambar 4.12 Validasi Password Panitia yang Berhasil.....	49
Gambar 4.13 Validasi Password Panitia yang Gagal	50
Gambar 4.14 Validasi ID Pemilih Terdaftar	50
Gambar 4.15 Validasi ID Pemilih Tidak Terdaftar	51
Gambar 4.16 Validasi ID Pemilih Sudah Voting	51

Gambar 4.17 Token untuk "kriptografi"	52
Gambar 4.18 Token untuk "Kriptografi"	52
Gambar 4.19 Verifikasi Token yang Berhasil.....	53
Gambar 4.20 Verifikasi Token yang Tidak Berhasil.....	53

DAFTAR TABEL

Tabel 2.1 Desimal ke Heksadesimal.....	14
Tabel 2.2 Parameter AES.....	15
Tabel 2.3 S-Box	18
Tabel 2.4 Rcon	21
Tabel 2.5 Hasil Padding dan Append Pesan	25
Tabel 2.6 Hasil Perluasan Pesan	27

DAFTAR PUSTAKA

- Afrin, T., & Satao, K. J. (2013). E-Voting System for on Duty Person Using RSA Algorithm with Kerberos Concept. *International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)*, Vol.2, N0.7, 2258-2261.
<https://ijircce.com/admin/main/storage/app/pdf/nhSXIW2Ua56DUUDS3NibBma4xXTet4lW67iVSd83.pdf>
- Ariyus, D. (2006). *Kriptografi: Keamanan Data dan Komunikasi*. Yogyakarta: Graha Ilmu.
- Ariyus, D. (2008). *Pengantar Ilmu kriptografi: Teori, Analisis, dan Implementasi*. Yogyakarta: Andi.
- Az-Zahra, F., Marwati, R., & Sispiyati, R. (2024). Implementasi QR Code dengan Algoritma Secure Hash Algorithm (SHA)-256 dan Rivest Shamir Adleman (RSA) yang Ditingkatkan untuk Autetikasi Dokumen Digital. *EurekaMatika* 12(1), 11-22.
<https://ejournal.upi.edu/index.php/JEM/article/view/67161>
- Burton, D. M. (2011). *elementary Number Theory*. New York: McGraw-Hill.
- Easttom, W. (2021). *Modern Cryptography*. Washington DC: Springer Cham.
- Fikriansyah, I. (2021). Program Aplikasi E-Voting Menggunakan Algoritma El Gamal dan SHA-256. *Skripsi. Universitas Pendidikan Indonesia. Bandung*.
- Hajar, I. (2022). Pengamanan Arsip dengan Algoritma Enkripsi AES-256 untuk Web App E-Arsip Yayasan Universitas Islam Sumatera Utara. *Jurnal Ilmu Komputer*, 76-89. <https://doi.org/10.56211/helloworld.v1i2.13>
- Harianja, M. H. (2024). Analisa Fungsi Hash Untuk Mendeteksi Otentikasi File Video Menerapkan Metode N-Hash. *Buletin Ilmiah Informatika Teknologi*, 104-108. <https://doi.org/10.58369/biit.v2i3.56>
- Herstein, S. N. (1975). *Topics in Algebra (2nd ed.)*. New York: John Willey and Sons Inc.
- Hidayatulloh, N. W., Tahir, M., Amalia, H., Basyar, N. A., Prianggara, A. F., & Yasin, M. (2023). Mengenal Advance Encrytion Standard (AES) Sebagai Algoritma Kriptografi Dalam Mengamankan Data. *Digital Transformation*

Technology (Digitech), Vol.3 No.1, 1-10.
<https://doi.org/10.47709/digitech.v3i1.2293>

- Hutahaean, J. (2015). *Konsep Sistem Informasi*. Jakarta: Deepublish.
- Lutz, M. (2001). *Programming Python* (L. Lewin, F. Willison, & E. Quill (eds.) ; 2nd ed.). California: O'Reilly & associates, inc.
- Menezes, A. J., Oorschot, P. C., & Vanstone, S. A. (1996). *Handbook of Applied Cryptography*. CRC Press.
- Menezes, B. (1996). *Applied Cryptography: Protocols, Algorithms, and Source Code in C*. New York: John Wiley and Sons.
- Munir, R. (2019). *Kriptografi Edisi Kedua*. Bandung: Informatika Bandung.
- Neyman, S. N., Isnaini, M. F., & Nurdianti, S. (2013). Penerapan Sistem E-Voting pada Pemilihan Kepada Daerah di Indonesia (The Application of E-Voting Systems in the Local Elections in Indonesia). *Jurnal Sains Terapan Edisi III* Vol.3, 35-49. <http://repository.ipb.ac.id/handle/123456789/68494>
- Pratama, F., & Pertiwi, A. (2022). Pembuatan Website E-Voting (Studi Kasus: Pemilihan Ketua OSIS SMA dan Sederajat). *JURNAL JUKIM* Vol 1 No. 3, 104-112. <https://doi.org/10.56127/jukim.v1i03.206>
- Putri, M. P., dkk. (2022). *Algoritma dan Struktur Data*. Bandung: Widina Bhakti Persada Bandung.
- Putri, W. C., Marwati, R., & Gozali, S. M. (2023). Penggabungan Kriptografi Rivest Shamir Adleman (RSA) dan Advanced Encryption Standard (AES) pada Aplikasi Pengirim E-Mail. *INTERVAL: Jurnal Ilmiah Matematika*, 92-101. <https://doi.org/10.33751/interval.v3i2.8845>
- Saputra, I., & Nasution, S. D. (2019). Analisa Algoritma SHA-256 Untuk Mendeteksi Orisinalitas Citra Digital. *Prosiding Seminar Nasional Riset Information Science (SENARIS)*, 164-178. <http://dx.doi.org/10.30645/senaris.v1i0.20>
- Schneier, B. (1996). *Applied Cryptography: Protocols, Algorithms, and Source Code in C* (2nd ed.). New York: Wiley.
- Setiawan, D., Andrianingsih, & Soepriyono, G. (2023). Rancang Bagun Website Pengamanan Database E-Voting dengan Menerapkan Algoritma Rivest

- Shamir Adleman (RSA). *Jurnal Teknologi Informatika dan Komputer MH. Thamrin Volme 9 No.2*, 1341-1355. <https://doi.org/10.37012/jtik.v9i2.1687>
- Sitorus, M., & Antonieta, C. (2021). Perancangan Sistem Pemilihan Ketua BEM (Badan Eksekutif Mahasiswa) Berbasis E-Voting Dengan Metoed Crud Sebagai Digitalisasi Organisasi di BRI Institute. *Infotech: Journal of Technology Information Vol.7 No.2*, 125-132. <https://doi.org/10.37365/jti.v7i2.122>
- Srinath, K. (2017). Python - The Fastest Growing Programming Language. *International Journal of Computer Sciences Issues*, 354-357. <https://www.irjet.net/archives/V4/i12/IRJET-V4I1266.pdf>
- Stinson, D. R. (2006). *Cryptography: Theory dan Practice (3rd ed.)*. Boca Raton: Chapman & Hall/CRC.
- Sulastri, S., & Putri, R. D. (2018). Implementasi Enkripsi Data Secure Hash Algorithm (SHA-256) dan Message Digest Algorithm (MD5) pada Proses Pengamanan Kata Sandi Sistem Penjadwalan. *Jurnal Teknik Elektro Vol.10 No.2*, 70-74. <https://doi.org/10.15294/jte.v10i2.18628>
- Susanti, D. (2020). Analisis Modifikasi Metode Playfair Cipher Dalam Pengamanan Data Teks. *Indonesian Journal of Data and Science Vol.1 No.1*. 11-18. <https://doi.org/10.33096/ijodas.v1i1.4>
- Yafi, A., Arhandi, P., Firdaus, V., Ismail, A., & Batubulan, K. (2023). Sistem Keamanan E-Voting Menggunakan Arsitektur Publik Blockchain Ethereum. *KLIK: Kajian Ilmiah Informatika dan Komputer Vol.4 No.3*, 1313-1322. <https://doi.org/10.30865/klik.v4i3.1423>