**JUSTIFY: Jurnal Sistem Informasi Ibrahimy**
Vol. 3, No. 1, Juli 2024, hal. 38-45
E-ISSN: 2962-3642 | P-ISSN: 2962-3871
DOI: 10.35316/justify.v3i1.5107

# Optimasi Keamanan Data Penerimaan Mahasiswa Menggunakan AES-256, SHA-256, dan Base64

**Ahmad Halimi[1], Abu Tholib[2], Moh. Ainol Yaqin[3]**

[1] Teknologi Informasi, Fakultas Teknik, Universitas Nurul jadid, Indonesia
[2,3] Teknik Informatika, Fakultas Teknik, Universitas Nurul Jadid, Indonesia

**Info Artikel**

**Riwayat Artikel:**
Diterima : **Tanggal-Bulan-Tahun**
Direvisi : **Tanggal-Bulan-Tahun**
Disetujui : **Tanggal-Bulan-Tahun**

**Kata Kunci:**

Keamanan Sistem,
Enkripsi,
Hash,
Sistem Informasi

**ABSTRAK**

Di era teknologi informasi saat yang luar biasa berkembang menjadi prioritas keamanan data terutama proses penerimaan mahasiswa baru (PMB) di perguruan tinggi. Proses ini melibatkan pengumpulan data pribadi sensitif dari ribuan calon mahasiswa setiap tahun. Untuk melindungi data ini, penelitian ini menerapkan metode enkripsi *Advanced Encryption Standard* (AES) 256-bit, *Secure Hash Algorithm* 256 (SHA-256), dan Base64. AES-256-CBC dikenal efektif dalam menjaga keamanan data dengan tingkat keamanan yang tinggi. SHA-256 meningkatkan keamanan lebih lanjut dengan menghasilkan hash unik yang memverifikasi integritas data. Sementara itu, Base64 mengubah data biner menjadi format teks yang lebih mudah dikelola. Penelitian ini juga mencakup pengujian kecepatan enkripsi dan verifikasi menggunakan framework laravel. Implementasi metode ini diharapkan dapat meningkatkan kepercayaan dan memenuhi standar keamanan data yang ketat dalam sistem informasi PMB, memastikan perlindungan data yang komprehensif dan meningkatkan integritas sistem.

***Keywords*:**

*System Security,*
*Encryption,*
*Hash,*
*Information System*

***ABSTRACT***

*In this era of extraordinary information technology, data security is a priority, especially the process of admitting new students (PMB) to tertiary institutions. This process involves collecting sensitive personal data from thousands of prospective students each year. To protect this data, this research applies 256-bit Advanced Encryption Standard (AES), Secure Hash Algorithm 256 (SHA-256), and Base64 encryption methods. AES-256-CBC is known to be effective in maintaining data security with a high level of security. SHA-256 enhances security further by generating a unique hash that verifies data integrity. Meanwhile, Base64 converts binary data into a more manageable text format. This research also includes testing encryption and verification speed using the Laravel framework. The application of this method is expected to increase trust and meet strict data security standards in the PMB information system, guarantee comprehensive data protection and improve system integrity.*

**Penulis Korespondensi:**
Ahmad Halimi,
Teknologi Informasi,
Universitas Nurul Jadid
Email: ahmadhalimi@unuja.ac.id

## 1. PENDAHULUAN

Di era tekonologi infromasi yang sangat luar biasa berkembang menjadi prioritas utama terkait keamanan data di bidang pendidikan. Proses penerimaan mahasiswa baru (PMB) di perguruan tinggi melibatkan pengumpulan informasi pribadi yang sangat sensitif dari ribuan calon mahasiswa setiap tahunnya, termasuk data pribadi, orang tua, atau wali sebagai bagian dari pengisian biodata diri[1]. Oleh karena itu, perlindungan data dalam proses ini merupakan kewajiban hukum yang sangat penting untuk menjaga kepercayaan dan integritas sistem informasi penerimaan mahasiswa baru[2].

Penelitian ini menggabungkan metode simetris, hashing, dan base64 sebagai langkah perlindungan data yang akan dienkripsi. Keamanan data lebih efektif dan tersimpan dengan baik dalam sistem informasi. Metode yang digunakan adalah *Advanced Encryption Standard* (AES), yang diakui oleh National Institute of Standards and Technology (NIST), sangat efektif dalam melindungi data dengan kunci enkripsi hingga 256-bit, memberikan tingkat keamanan tinggi yang sulit ditembus. Namun, keamanan AES sangat bergantung pada kunci yang digunakan[3][4]. Jika kunci tidak dijaga dengan baik dan jatuh ke tangan yang salah, enkripsi AES tidak lagi aman. Oleh karena itu, dikombinasikan dengan *Secure Hash Algorithm* 256 (SHA-256) algoritma lebih baik dari pendahulunya yang efisien dalam memverfikasi integritas data dengan menghasilkan hash unik sepanjang 256-bit[5]. Serta penggunan base64 untuk menjadi format teks ASCII yang telah di presentasikan dalam bentuk data biner.

Penelitian yang dirujuk oleh [6] Ferzha Putra Utama dalam "implementasi algoritma AES 256 CBC, Base64, dan SHA-256 dalam pengamanan dan validasi data ujian online," digunakan untuk mengamankan data ujian online berbasis website. Pengujian dilakukan menggunakan MERN(MongoDB, Express, React, dan Node.js) [7]sebagai server web, menunjukkan hasil yang baik dengan waktu enkripsi rata-rata 1,1115 ms, bergantung pada koneksi internet dan ukuran data. Namun, penelitian ini menggunakan framework Laravel dan database MySQL. Jika dibandingkan dengan MongoDB, MySQL menawarkan kecepatan data yang lebih baik, meskipun MongoDB juga mendukung relasi antar tabel yang diperlukan untuk tampilan data yang kompleks[8].

Dalam sistem informasi penerimaan mahasiswa baru (PMB), optimalisasi keamanan data dicapai dengan kombinasi AES-256-CBC sebagai enkripsi data, SHA-256 sebagai hashing pada kode unik pendaftar yang berfungsi sebagai kunci AES, dan Base64 untuk mengubah data biner ke dalam format teks yang akan disimpan di basis data dan storage jika berupa file. Proses ini melibatkan analisis risiko, enkripsi data, verifikasi integritas data, penerapan kontrol akses yang ketat, serta pemantauan dan audit rutin. Implementasi ini menjamin perlindungan data yang komprehensif dari awal hingga akhir, meningkatkan kepercayaan antara mahasiswa dan institusi pendidikan, serta memenuhi standar keamanan data yang ketat.

## 2. METODE PENELITIAN

Dengan pendekatan kuantitatif serta penggunakan metode kriptografi pada penelitian ini, maka dilakukan analisis keamanan data dari aspek sistem infromasi PMB. Metode yang akan digunakan adalah sebagai berikut:

1. *Advanced Encryption Standard* (AES)

   Dalam algoritma AES, data dan kata kunci diolah menjadi array yang menghasilkan state atau yang dikenal sebagai ciphertext. Proses enkripsi melibatkan langkah AddRoundKey, SubBytes, ShiftRows, dan MixColumns, kecuali pada putaran terakhir di mana MixColumns tidak diaplikasikan. Proses dekripsi mirip dengan enkripsi, tetapi dilakukan secara terbalik. Setiap tahap memerlukan subkey, sehingga total bit yang diperlukan dapat mencapai ribuan, sementara kunci awal hanya berkisar antara 128 hingga 256 bit. Total subkey yang diperlukan adalah Nb(Nr+1), di mana Nb merupakan pengelompokan data dalam bentuk satuan kata yang diproses dalam algoritma. AES adalah metode enkripsi simetris yang memerlukan kunci yang sama untuk enkripsi dan dekripsi. Terdapat tiga varian kunci dalam AES, yaitu AES 128, 192, dan 256, masing-masing dengan karakteristik dan hasil yang berbeda. [9][10].

   Proses enkripsi dengan AES-128 melibatkan 10 putaran operasi yang ketat untuk mengamankan data:

   1. Menggabungkan data dengan kunci awal melalui operasi XOR di sebut AddRoundKey
   2. Masing-masing putaran sebanyak 9 ini terdiri dari empat langkah penting:
      a. Menerapkan tabel substitusi yang mengubah setiap byte disebut SubBytes.

b. Menggeser baris data secara berurutan untuk meningkatkan keamanan disebut ShiftRows.

c. Menggabungkan data dalam setiap kolom melalui operasi aljabar yang kompleks di sebut MixColumns.

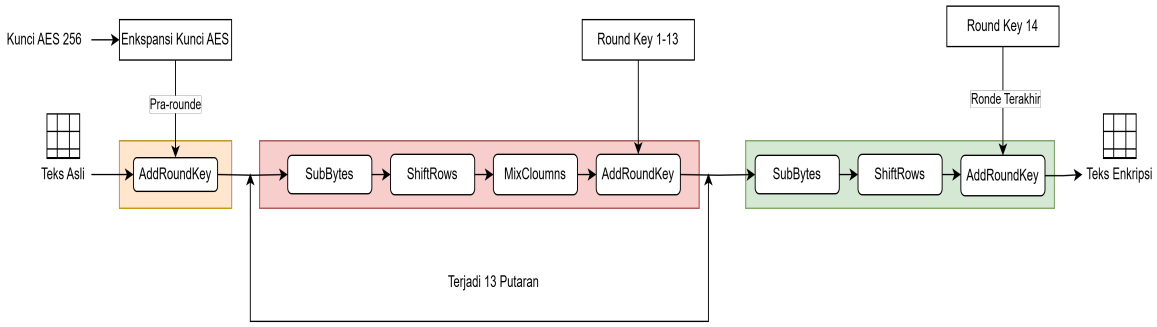
d. Menambahkan kunci putaran yang dihasilkan dari kunci awal disebut AddRoundKey.

3. Putraan terakhir yang memilikikan point 2 untuk selesaikan proses enkripsi.

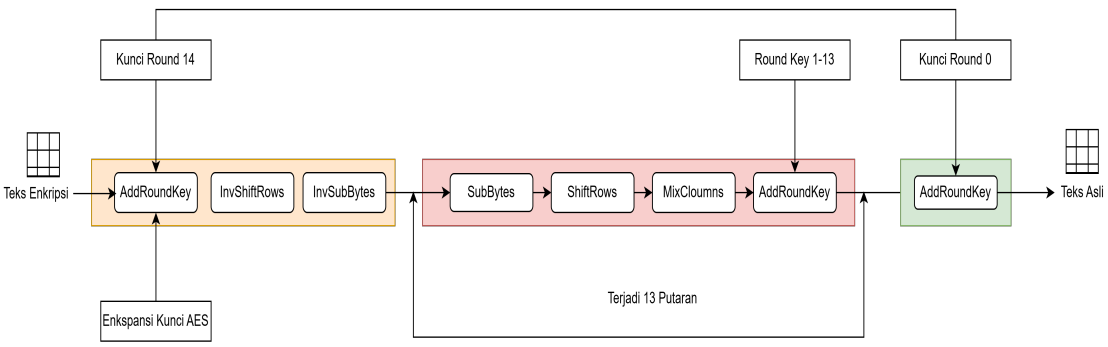
Dekripsi AES-128 merupakan kebalikan dari proses enkripsi, dengan 10 putaran yang denkripsi:

1. Langkah awal yang sama, menggunakan kunci akhir dari proses enkripsi disebut AddRoundKey
2. Setiap 9 putaran mengembalikan data dilakukan:
   a. Mengembalikan geseran baris ke posisi semula disebut InverseShiftRows
   b. Menggunakan tabel substitusi terbalik untuk mengembalikan byte disebut InverseSubBytes
   c. Menambahkan kunci putaran yang berurutan disebut AddRoundKey
   d. Melakukan operasi aljabar terbalik dari MixColumns disebut InverseMixColumns
3. Putraan terakhir yang memilikikan point 2 untuk selesaikan proses menjadi teks aslinya.

Varian AES-128, 192, 256 memiliki proses perputran yang bebeda dengan tingginya nilai bit dimiliki. Seperti AES-192 hanya 12 kali putaran serta AES-256 hanya 14 kali putaran. Dari diagaram alir gambar 1 dan 2 menjelaskan proses dalam enkripsi dan dekripsi data yang sesuai bit.




**Gambar 1. Enkripsi AES**

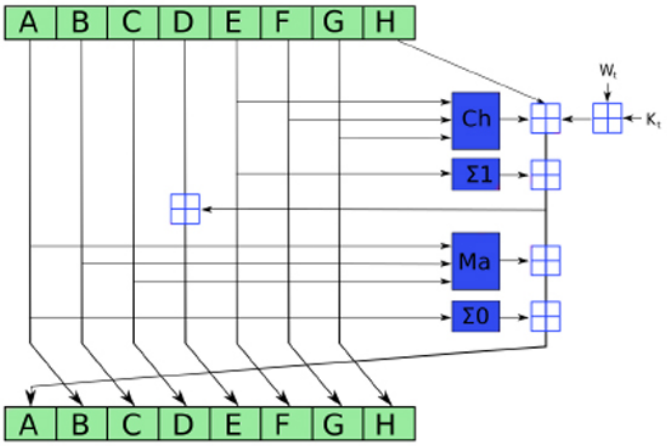



**Gambar 2. Denkripsi AES**

2. *Secure Hash Algorithm* 256

Algoritma hash SHA-256 adalah salah satu varian dari keluarga SHA-2 yang menghasilkan hash atau digest sepanjang 256 bit. Algoritma SHA-256 didasarkan pada MD4 yang dikembangkan oleh Ronald L. Rivest dari MIT. SHA-256 menggunakan enam operasi logika dasar: AND, OR, XOR,

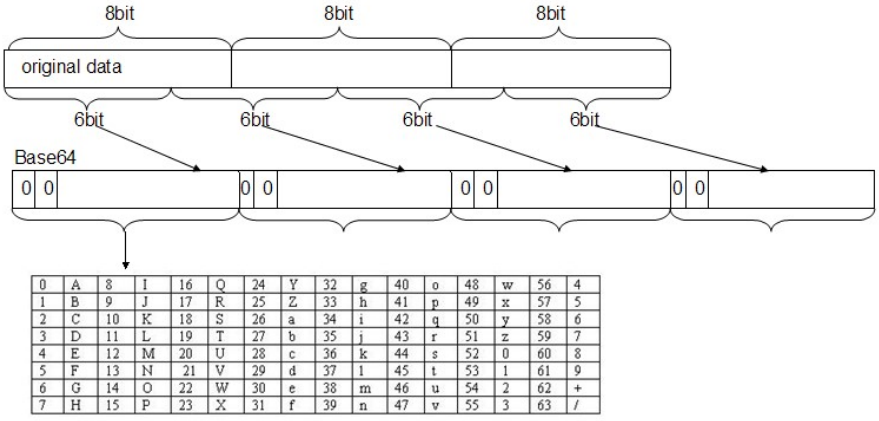
pergeseran bit ke kanan (shift right), dan rotasi bit ke kanan (rotate right) [11][12]. Algoritma ini memproses pesan melalui sebuah message schedule yang terdiri dari 64 elemen 32-bit, delapan variabel 32-bit, serta delapan variabel penyimpan nilai hash 32-bit. Proses ini menghasilkan message digest sepanjang 256 bit[13]. SHA-256 mengubah pesan masukan menjadi message digest berukuran 256 bit. Berdasarkan Secure Hash Standard (SHS) yang diterbitkan oleh National Institute of Standards and Technology (NIST) [14], pesan masukan yang panjangnya kurang dari 2^64 bit dipecah menjadi blok-blok 512 bit sebelum diproses. Hasil akhir dari proses ini adalah message digest sepanjang 256 bit, yang memberikan tingkat keamanan tinggi dalam aplikasi kriptografi dan keamanan informasi. Jalur Komputasi SHA-256 dapat dilihat pada Gambar 3.




**Gambar 3. Jalur Komputasi SHA-256**

### 3. Algoritma Base64

Base64 adalah metode yang mengubah data biner menjadi teks ASCII melalui proses encoding dan decoding. Dalam konteks penggunaan internet, metode ini sering dipilih untuk mengirim data karena hasilnya berbentuk teks, yang lebih mudah dikirim dibandingkan data biner. Proses ini sangat bermanfaat saat ada kebutuhan untuk mengodekan data biner guna penyimpanan atau transmisi melalui platform yang hanya mendukung data teks[15][16]. Selain itu, Base64 juga digunakan untuk menyamarkan atau mengamankan data biner selama pengiriman. Hasil dari encoding Base64 terdiri dari huruf-huruf dari A sampai Z (baik kapital maupun kecil), angka dari 0 sampai 9, dan termasuk dua simbol tambahan: "+" dan "/". Simbol "=" berfungsi untuk menyesuaikan dan melengkapi data biner, memastikan bahwa output Base64 dapat ditransfer dan diterima secara akurat. Base64 menggunakan kunci simetris di mana kunci enkripsi dan dekripsi adalah identik. Diagram alur dari proses ditampilkan pada Gambar 4.




| | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | A | 8 | I | 16 | Q | 24 | Y | 32 | g | 40 | o | 48 | w | 56 | 4 |
| 1 | B | 9 | J | 17 | R | 25 | Z | 33 | h | 41 | p | 49 | x | 57 | 5 |
| 2 | C | 10 | K | 18 | S | 26 | a | 34 | i | 42 | q | 50 | y | 58 | 6 |
| 3 | D | 11 | L | 19 | T | 27 | b | 35 | j | 43 | r | 51 | z | 59 | 7 |
| 4 | E | 12 | M | 20 | U | 28 | c | 36 | k | 44 | s | 52 | 0 | 60 | 8 |
| 5 | F | 13 | N | 21 | V | 29 | d | 37 | l | 45 | t | 53 | 1 | 61 | 9 |
| 6 | G | 14 | O | 22 | W | 30 | e | 38 | m | 46 | u | 54 | 2 | 62 | + |
| 7 | H | 15 | P | 23 | X | 31 | f | 39 | n | 47 | v | 55 | 3 | 63 | / |

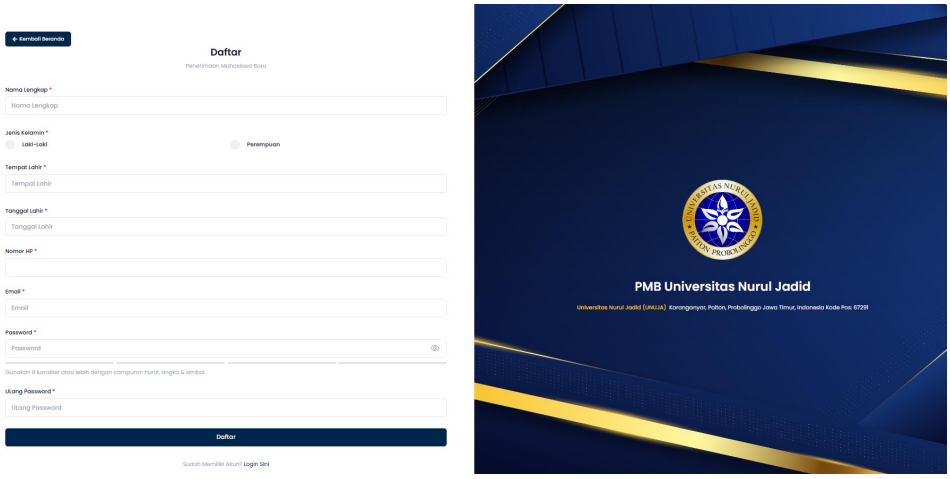
**Gambar 4. Blok Diagram Base64**

## 3. HASIL DAN ANALISIS

Pada tahapan ini, dilakukan proses penerapan AES-256-CBC sebagai enkripsi data, SHA-256 sebagai hashing pada kode unik pendaftar yang berfungsi sebagai kunci AES, dan Base64 untuk mengubah data biner ke dalam format teks yang akan disimpan di basis data dan storage jika berupa file. Berikut tahapan yang telah diterapkan sistem infromasi (PMB):

1. Halaman Pendaftaran Calon Mahasiswa Baru

   Pengujian dalam penelitian di tahap awal melakukan pendaftaran sebagai calon mahasiswa baru untuk. Berikut tampilan halaman pendaftaran




**Gambar 5. Halaman Pendaftaran**

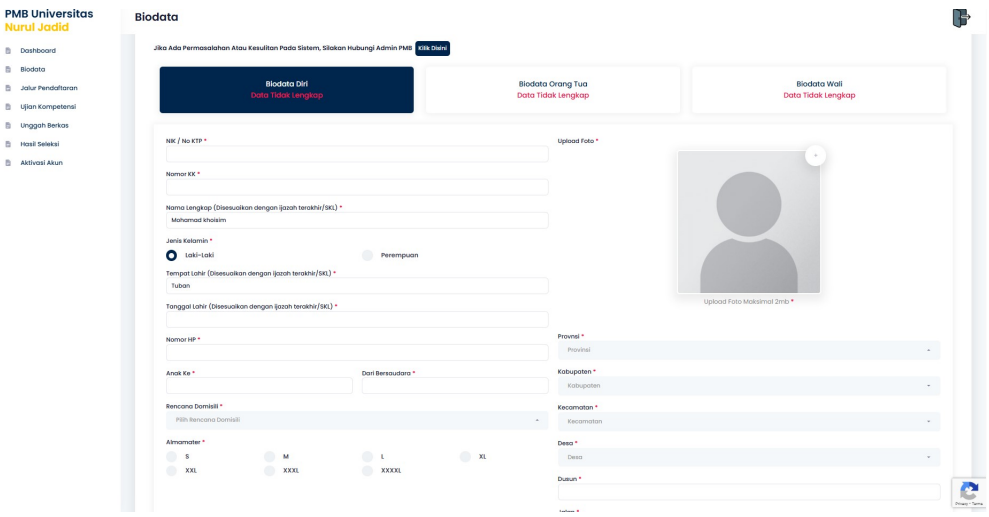
Setelah melakukan pendaftar, maka secara otomatis memiliki kode unik untuk pendaftar akan digunakan sebagai kata kunci AES yang telah di SHA-256 untuk enkripsi data indentitas yang penting nik, nomor kk, kontak orang tua dan wali, serta berkas pendukung untuk persyaratan PMB.

| | id_pendaftar | uid_pendaftar | nama | jk | nik | nomor_kk | domisili | foto |
|---|---|---|---|---|---|---|---|---|
| Edit Copy Delete | 3678 | 069e7adc-0669-4397-85a4-8597de569193 | Mohamad khoisim | L | NULL | NULL | NULL | NULL |
| Edit Copy Delete | 3671 | 12db639e-1c68-4f1d-af88-1f01959f34ca | Devita sari | P | NULL | NULL | NULL | NULL |
| Edit Copy Delete | 3669 | 27f92eba-35e5-4d71-a35b-e177e2aec47e | Fayiz ramzy pramuditya | L | NULL | NULL | NULL | NULL |
| Edit Copy Delete | 3668 | f9bef5dd-e566-4cbc-90d5-0bdf9d7d29af | Asyifa zahrotul hasanah | P | NULL | NULL | NULL | NULL |

**Gambar 6. Table Pendaftaran**

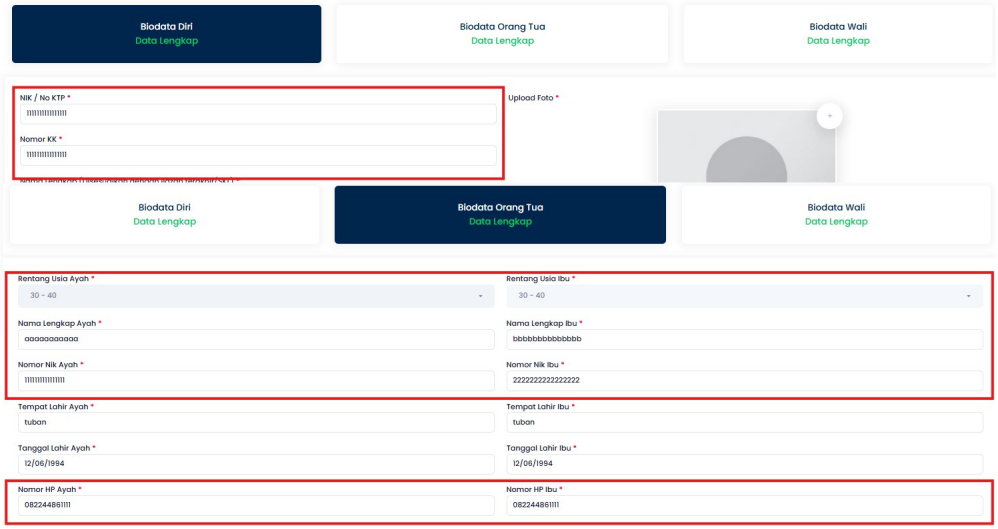
2. Halaman Pengisian Biodata

   Berikut halaman pengisi biodata yang terdiri dari biodata diri, oranng tua dan wali:



**Gambar 6. Halaman Biodata**

Berikut data yang akan dilakukan pengujian enkrpsi data dengan segi waktu dalam penggunan AES-256-CBC, SHA-256 dan Base64 dengan data yang di tandai dengan warna merah:




**Gambar 7. Input biodata yang di enkripsi**

Dari hasil pengujian yang dilakukan, memilik berapa segi waktu dan ukuran yang sangat variasi.

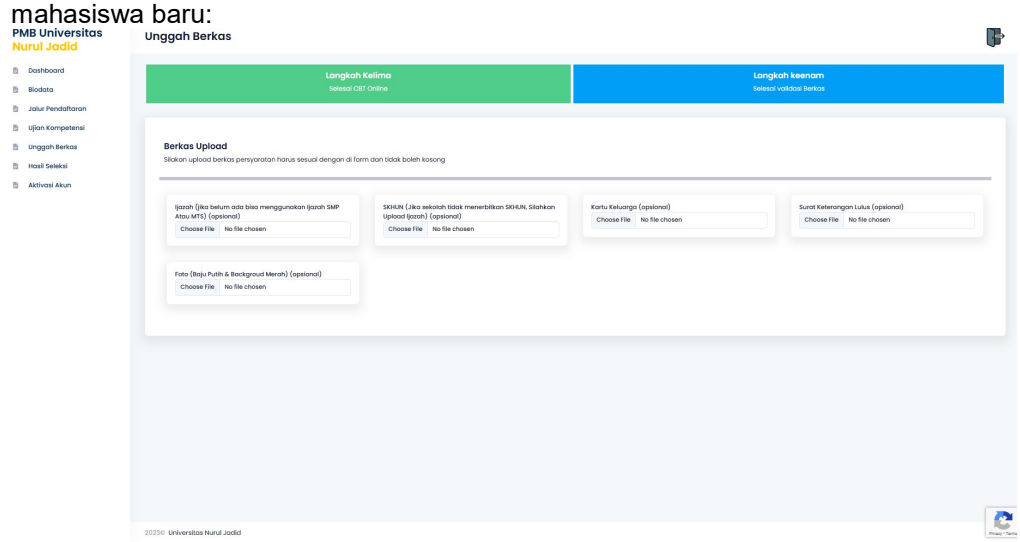
**Tabel 1. Pengujian dan Hasil Enkripsi teks**

| No | Pengujian | Teks | Enkripsi | Size | Waktu |
|---|---|---|---|---|---|
| **1** | AES-256-CBC SHA-256 Base64 | 1111111111111111 (nik/kk) | 2+C7lc0X1IlAtH/RwjHdqkpzugcpAtPXz+LnPWEm6aRbx1IyoAc5UedkcHoUtOy4 | 64 bytes | 0.0361328125 ms |
| | | Ahmad Royhan Ali Rahman (nama orang tua / wali) | Qv50HXPkFkLCg1IJxiQZbw1Pc/bmqdnoBp+V1Q2AQUcXINtjuJOm4Wb4a/w0CpqH | 64 bytes | 0.0732421875 ms |
| **2** | AES-256-CBC dengan SHA-256 | 1111111111111111 (nik/kk) | 58324f2d0aa2f9bd8dac9225adf8c6e646e64bb19274c2ee4eaec6c99882b450c1fcf2993f7d4ce81e7517cf5302bdab | 48 bytes | 0.031005859375 ms |
| | | Ahmad Royhan Ali Rahman (nama orang tua / wali) | 026229ac35b2ac97303b38ad0cf96489d41563e49e064f9ad690d79df10800f88d10aa8c6211d70cd7a3d432bb0b4a65 | 48 bytes | 0.0341796875 ms |
| **3** | AES-256-CBC dengan Base64 | 1111111111111111 (nik/kk) | uyoPTGEJlaHlRRDrhhoruJwwneNHGGkPjUEvme3XVBvWWakTQA3Lc6Xx16zHETk9 | 64 bytes | 0.029052734375 ms |
| | | Ahmad Royhan Ali Rahman (nama orang tua / wali) | icTKi5xajJTafrNFOiSiv4FRrGaJAIB2g2P0+YwGX8TDvzXNecQPEkz8zLISuG43 | 64 bytes | 0.031005859375 ms |

Pada tabel 1. Metode AES-256-CBC dengan SHA-256 menunjukkan keunggulan dalam hal ukuran data yang dihasilkan setelah enkripsi, sementara AES-256-CBC dengan Base64 unggul dalam segi waktu ketika melakukan enkripsi data. Melalui tiga pengujian bertahap yang telah dilakukan, terlihat bahwa AES-256-CBC dengan SHA-256 lebih disarankan karena menghasilkan ukuran data yang lebih kecil dibandingkan metode lainnya. Sementara itu, ukuran yang lebih besar pada metode yang

menggunakan Base64 setelah enkripsi AES-256-CBC disebabkan oleh proses encoding Base64 yang menambahkan overhead tambahan pada data.

3. Halaman Unggah Berkas
   Berikut halaman untuk unggah berkas berdasarkan jalur pendaftaran yang pilih oleh calon mahasiswa baru:




**Gambar 8. Halaman Unggah Berkas**

Berikut yang akan dilakukan pengujian enkrpsi file dengan segi waktu dalam penggunan AES-256-CBC, SHA-256 dan Base64. akan tetapi file yang akan di upload hanya gambar dan pdf dengan maksimal size 2 mb.

**Tabel 2. Pengujian dan Hasil Enkripsi file**

| No | Pengujian | Tipe | Size File | Size Enkripsi | Waktu |
|---|---|---|---|---|---|
| **1** | AES-256-CBC SHA-256 Base64 | Gambar | 245 kb | 195 kb | 0.2119140625 ms |
| | | PDF | 1,415 kb | 1.886 kb | 2.1640625 ms |
| **2** | AES-256-CBC dengan SHA-256 | Gambar | 245 kb | 146 kb | 0.342041015625 ms |
| | | PDF | 1,415 kb | 1.414 KB | 3.740966796875 ms |
| **3** | AES-256-CBC dengan Base64 | Gambar | 245 kb | 195 kb | 0.2841796875 ms |
| | | PDF | 1,415 kb | 1.886 kb | 1.7900390625 ms |

Pada tabel 2. Metode AES-256-CBC dengan SHA-256 menunjukkan keunggulan dalam hal ukuran file yang dihasilkan setelah enkripsi, sementara AES-256-CBC, SHA-256 dengan Base64 unggul dalam segi waktu ketika melakukan enkripsi file. Melalui tiga pengujian bertahap yang telah dilakukan, terlihat bahwa AES-256-CBC dengan SHA-256 lebih disarankan karena menghasilkan ukuran data yang lebih kecil dibandingkan metode lainnya.

## 4. KESIMPULAN

Kesimpulan dari penelitian yang dilakukan penggunaan AES-256-CBC, SHA-256, dan Base64 sebagai sistem keamanan di penerimanan mahasiswa baru (PMB) menunjukkan hasil bagus dalam enkripsi data:

1. Penerapan AES-256-CBC dengan SHA-256 menghasilkan ukuran enkripsi teks yang efisien untuk disimpan dalam database.
2. Penggunaan AES-256-CBC dengan SHA-256 juga menghasilkan ukuran enkripsi file yang berbeda secara signifikan dari ukuran file asli. Namun, dari segi waktu, kombinasi AES-256-CBC, SHA-256, dan Base64 lebih unggul.

3. Penerapan sistem keamanan data seperti ini sangat membantu meningkatkan kepercayaan calon mahasiswa baru untuk melanjutkan proses pendaftaran hingga selesai.
4. Adapun dari saran penelitian selanjut untuk mengingkat keamanan data dan segi waktu enkripsi yang terbaik. Seperti Blake3 atau lain-lainnya.

## REFERENSI


[1] Sinaga and Putri, "Jurnal Rechts Vinding," *Formulasi Legis. Perlindungan Data Pribadi Dalam Revolusi Ind. 4.0 J. Rechts Vinding*, p. 237, 2020.

[2] S. H. Loilatu, M. Rusdi, and M. Musyowir, "Penerapan Sistem Informasi Manajemen Pendidikan dalam Proses Pembelajaran," *J. Basicedu*, vol. 4, no. 4, pp. 1408–1422, 2020, doi: 10.31004/basicedu.v4i4.520.

[3] K. A. Mckay and D. A. Cooper, "Withdrawn NIST Technical Series Publication," no. 2001, pp. 27–28, 2001.

[4] N. A. Fauziah, E. H. Rachmawanto, D. R. I. M. Setiadi, and C. A. Sari, "Design and implementation of AES and SHA-256 cryptography for securing multimedia file over android chat application," in *2018 International Seminar on Research of Information Technology and Intelligent Systems, ISRITI 2018*, 2018. doi: 10.1109/ISRITI.2018.8864485.

[5] M. Alkhyeli, S. Alkhyeli, K. Aldhaheri, and H. Lamaazi, "Secure Chat Room Application Using AES-GCM Encryption and SHA-256," in *2023 15th International Conference on Innovations in Information Technology, IIT 2023*, 2023. doi: 10.1109/IIT59782.2023.10366418.

[6] F. P. Utama, G. Wijaya, R. Faurina, and A. Vatresia, "Implementasi Algoritma AES 256 CBC, BASE 64, Dan SHA 256 dalam Pengamanan dan Validasi Data Ujian Online," *J. Teknol. Inf. dan Ilmu Komput.*, vol. 10, no. 5, 2023, doi: 10.25126/jtiik.20231056558.

[7] "MERN Stack Explained | MongoDB." Accessed: Jun. 11, 2024. [Online]. Available: https://www.mongodb.com/resources/languages/mern-stack

[8] M. Silalahi, "PERBANDINGAN PERFORMANSI DATABASE MONGODB DAN MYSQL DALAM APLIKASI FILE MULTIMEDIA BERBASIS WEB," *Comput. Based Inf. Syst. J.*, vol. 6, no. 1, 2018, doi: 10.33884/cbis.v6i1.574.

[9] K. I. Santoso and W. Priyoatmoko, "Pengamanan Data Mysql pada E-Commerce dengan Algoritma Aes 256," *Semin. Nas. Sist. Inf. Indones.*, vol. 1, no. 1, 2016.

[10] S. Rahmawati, I. Taufik, and G. Sandi, "Implementasi Algoritma AES (Advanced Encryption Standard) 256 Bit Dan Kompresi Menggunakan Algoritma Huffman Pada Aplikasi Voice Recorder," *Prosiding-Seminar Nas. Tek. Elektro UIN Sunan Gunung Djati Bandung*, 2018.

[11] "USE OF CRYPTOGRAPHY IN CLOUD COMPUTING," *Int. Res. J. Mod. Eng. Technol. Sci.*, 2022, doi: 10.56726/irjmets31806.

[12] F. M. Rangkuti, N. Budi Nugroho, and Z. Panjaitan, "Implementasi Digital Signature Pada E-Invoice Di Uniqa Digital Invitation Menggunakan Algoritma SHA-256 (Secure Hash Algorithm-256) Dan RSA (Rivest Shamir Adleman)," *J. CyberTech*, vol. x. No.x, no. x, 2019, [Online]. Available: https://ojs.trigunadharma.ac.id/

[13] R. Beaulieu, S. Treatman-Clark, D. Shors, B. Weeks, J. Smith, and L. Wingers, "The SIMON and SPECK lightweight block cIPhers," in *Proceedings - Design Automation Conference*, 2015. doi: 10.1145/2744769.2747946.

[14] NIST, "SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions," 2015.

[15] S. Siswanto, M. Anif, and W. Gata, "Penerapan Algoritma Kriptografi TEA Dan Base64 Untuk Mengamankan Email Data Policy Asuransi," *J. ELTIKOM*, vol. 2, no. 1, 2018, doi: 10.31961/eltikom.v2i1.44.

[16] Azlin, F. Musadat, and J. Nur, "Aplikasi Kriptografi Keamanan Data Menggunakan Algoritma Base64," *J. Inform.*, vol. 7, no. 2, 2018.

[17] A. F. Cobantoro, M. B. Setyawan, and H. Oktavianto, "Rekayasa Aplikasi Eposal Menggunakan Algoritma Base64 Untuk Menyimpan Data Pengguna," *J. Komtika (Komputasi dan Inform.*, vol. 7, no. 1, 2023, doi: 10.31603/komtika.v7i1.8711.

[18] C. Jianli, S. Yongdao, and L. Xia, "The Research of Mobile phone Entrance Guard System Model based on the Encryption Two-dimensional Code," *TELKOMNIKA Indones. J. Electr. Eng.*, vol. 11, no. 9, 2013, doi: 10.11591/telkomnika.v11i9.3281.