SENAFTI
SEMINAR NASIONAL MAHASISWA
FAKULTAS TEKNOLOGI INFORMASI

6th Seminar Nasional Mahasiswa Fakultas Teknologi Informasi (SENAFTI)
20 September 2025 – Jakarta, Indonesia
Volume 4, Nomor 2, September 2025 - ISSN 2962-8628 (*online*)

PENERAPAN KRIPTOGRAFI AES-128 UNTUK KEAMANAN DATA PEGAWAI PADA PERUSAHAAN LOGISTIK DI JAKARTA

Prasetyo Ari Nugroho[1], Rizky Pradana[2*]

[1,2] Teknik Informatika, Fakultas Teknologi Informasi, Universitas Budi Luhur, Kota Tangerang, Indonesia

Email: [1]2111501421@student.budiluhur.ac.id, [2*]rizky.pradana@budiluhur.ac.id
(* : corresponding author)

Abstrak-Sebuah perusahaan logistik di Jakarta masih menjalankan sistem keamanannya secara manual. Hal ini terjadi karena perusahaan tidak memiliki basis data yang aman. Akibatnya, kriptografi, suatu bidang ilmu yang bertujuan untuk mengamankan data, digunakan. Kriptografi adalah bidang yang melindungi kerahasiaan dan integritas pesan dengan menggunakan persamaan matematika untuk membuat isi pesan tidak dapat dibaca. Penelitian ini akan menggunakan *Advanced Encryption Standard* (AES), salah satu metode kriptografi yang paling umum digunakan untuk mengenkripsi dan mendekripsi data. Ini akan melindungi basis data karyawan perusahaan sehingga orang yang tidak berwenang tidak dapat membaca data atau catatan yang disimpan. Jika kunci yang tepat digunakan, data dapat didekripsi atau dilihat secara lengkap.

Kata Kunci: Keamanan, Kriptografi, Advanced Encryption Standard (AES), Enkripsi, Dekripsi, Basis Data, Data Pegawai

IMPLEMENTATION OF AES-128 CRYPTOGRAPHY FOR EMPLOYEE DATA SECURITY IN A LOGISTICS COMPANY IN JAKARTA

Abstract- *The security system used by a logistics company in Jakarta is still implemented manually. This is because the business does not currently have a database in place to safely store data. Therefore, a field of science called cryptography is applied to secure data. Cryptography can be defined as the science of maintaining the confidentiality and integrity of messages by using mathematical equations so that the message content is transformed into an unreadable form. For data encryption and decryption, one of the most popular cryptographic methods is the Advanced Encryption Standard (AES). In order to prevent unauthorised parties from reading the company's employee database, this technique will also be used in this study. The data can also be decrypted and viewed in its entirety if the correct key is used.*

Keywords*: Security, Cryptography, Advanced Encryption Standard (AES), Encryption, Decryption, Database, Employee Data*

1. PENDAHULUAN

Saat ini, manusia sudah memasuki masa dimana data dan informasi sangat mudah untuk diakses. Data yang bisa diakses juga beragam, mulai dari yang bersifat umum hingga sensitif. Dengan data dan informasi yang mudah diakses, kita bisa melakukan aktivitas dengan nyaman dan lancar. Namun, seringkali kita diperlihatkan oleh banyaknya kasus tentang penyalahgunaan dan kehilangan data. Maka dari itu, diperlukan sistem keamanan data untuk mencegahnya.

Keamanan data ini dimaksudkan agar seluruh data dan informasi yang bersifat sensitif atau krusial dapat terjaga dan terlindungi dari pihak yang tidak bertanggung jawab. Karena jika data dapat diakses oleh pihak yang tidak bertanggung jawab, pihak/perusahaan yang memiliki data dan informasi tersebut akan sangat dirugikan. Data-data penting milik perusahaan dapat diubah, dihilangkan, bahkan diperjualbelikan. Ini menyebabkan konsumen hilang kepercayaan sehingga perusahaan tersebut mengalami kerugian yang cukup besar seperti kebanyakan kasus yang terjadi dalam beberapa tahun terakhir.

Banyak kasus peretasan data yang terjadi di Indonesia akhir-akhir ini seperti yang terjadi pada ASN (Aparatur Sipil Negara) pada tahun 2024 lalu. Jumlah data yang diretas mencapai 4,7 juta data yang mencakup data-data ASN, seperti NIP, nama, tempat/tanggal lahir, golongan, jabatan, dan lain sebagainya. Diketahui juga bahwa seluruh data yang diretas dibanderol oleh peretas di sebuah forum jual beli hasil peretasan sebesar USD 10 ribu atau senilai dengan Rp 159,4 juta. Sampel berisi data 128 ASN juga dibagikan oleh peretas di berbagai instansi di Aceh [1].

Kasus yang berkaitan dengan keamanan data juga terjadi di perusahaan yang dijadikan tempat riset oleh penulis. Perusahaan kerap mendapatkan informasi mengenai penyalahgunaan data pegawai. Data tersebut seringkali dijadikan jaminan untuk pinjaman online (pinjol). Selain itu, perusahaan juga tidak mempunyai basis data untuk menyimpan data, khususnya data pegawai. Ini menyebabkan data lebih mudah hilang atau rusak, bahkan disalahgunakan. Oleh karenanya, setiap perusahaan harus menerapkan sistem keamanan data dengan sebuah teknik yang biasa disebut Kriptografi.

Kriptografi adalah seni dan ilmu yang menggunakan berbagai teknik matematika untuk menjaga data dan informasi aman. Dengan kata lain, kriptografi adalah cara untuk menjaga kerahasiaan dan integritas pesan dengan mengubah isi pesan menjadi bentuk yang tidak dapat dijelaskan. Karena metode ini, data atau informasi menjadi sulit untuk dipecah atau diterjemahkan jika Anda tidak tahu kuncinya [2]. Kriptografi juga memiliki sejarahnya sendiri. Kata kriptografi (cryptography) berasal dari kata Yunani crypto, yang berarti rahasia, dan graphia, yang berarti tulisan. Istilah "kriptografi" mengacu pada seni mengirimkan pesan dengan aman. Kata "seni" digunakan karena banyak orang memiliki cara unik untuk merahasiakan pesan [3].

Kriptografi terdiri dari dua tahap: enkripsi dan dekripsi. Dibandingkan dengan dekripsi, enkripsi adalah proses mengubah pesan asli (*plaintext*) menjadi pesan dalam bentuk kode yang rumit, dan dekripsi adalah proses mengembalikan pesan tersembunyi (ciphertext) menjadi pesan asli (*plaintext*) [4]. Istilah "*ciphertext*" digunakan untuk menggambarkan bentuk pesan yang dimaksud. Pesan *plaintext* adalah pesan berupa data atau informasi yang dapat dibaca dan dipahami maknanya, dan belum disamarkan oleh proses enkripsi.

Dalam penerapannya, kriptografi memiliki beberapa aspek penting yang harus diperhatikan, yaitu *confidentiality*, *integrity*, *authentication*, *availability*, dan *access control*. Aspek dalam kriptografi memiliki kaitannya masing-masing terhadap data. *Confidentiality* (kerahasiaan) berkaitan dengan batasan data yang diberikan, *integrity* (integritas) berfokus kepada keutuhan data, *authentication* (autentikasi) berkaitan dengan pembuktian untuk mengakses data, *availability* (ketersediaan) berfokus terhadap ketersediaan data dan informasi, dan *access control* (kendali akses) berkaitan dengan pengaturan atau perizinan akses data dan informasi [6].

Selain itu, kriptografi terbagi menjadi dua jenis utama: simetris dan asimetris. Kriptografi asimetris menggunakan algoritma yang terbatas dan membutuhkan waktu yang lama, tetapi dianggap lebih aman daripada kriptografi simetris karena menggunakan kunci yang berbeda untuk enkripsi dan dekripsi. Kriptografi simetris dianggap lebih aman jika kunci yang digunakan terdiri dari kombinasi angka dan huruf yang rumit. Menggunakan kunci yang lebih panjang juga pasti lebih aman [7].

Kriptografi dapat digunakan untuk mengunci dan mengamankan data dari akses yang tidak sah. Dengan menerapkan kriptografi, data dan informasi menjadi lebih aman dari peretasan dan serangan oleh pihak yang tidak bertanggung jawab. Kriptografi juga memiliki banyak metode. Namun, penelitian ini akan menggunakan AES-128 sebagai algoritmanya.

Salah satu algoritma kriptografi blok, *Advanced Encryption Standard* (AES), menggunakan blok dengan panjang 128-bit dan menggunakan kunci yang sama untuk enkripsi dan dekripsi. AES juga simetris, yang berarti menggunakan kunci yang sama untuk enkripsi dan dekripsi [8].

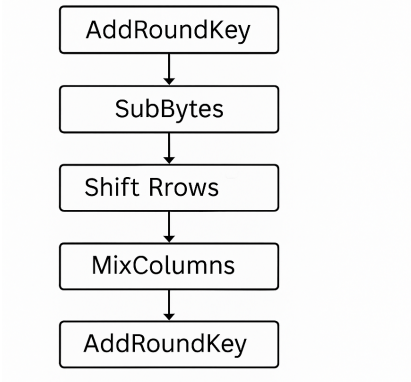
AES (*Advanced Encryption Standard*) merupakan algoritma yang saat ini sering digunakan sebagai sistem keamanan data. Hal itu terjadi karena algoritma ini telah dijadikan standar enkripsi global karena memiliki tingkat keamanan yang tinggi sehingga sangat efisien untuk mengamankan data. Algoritma AES juga sangat efektif untuk digunakan karena AES akan mengubah data ke dalam bentuk yang rumit sehingga sulit untuk dipecahkan.

Penelitian ini akan memfokuskan pengamanan basis data pegawai di sebuah perusahaan logistik di Indonesia. Algoritma AES juga akan diikutsertakan dalam penelitian sebagai sistem yang akan mengamankan dan mengunci datanya. Penelitian ini dilakukan agar perusahaan terhindar dari kasus peretasan dan kebocoran data yang terjadi dalam beberapa tahun terakhir. Selain itu, penelitian ini menggunakan beberapa referensi berupa penelitian serupa yang telah dilakukan dalam beberapa tahun terakhir seperti penelitian [9].

Penelitian tersebut melakukan pengamanan data *purchase order* menggunakan AES-128. Selain itu, penelitian [10] juga melakukan hal yang serupa, yaitu mengamankan *database* aplikasi kepelangganan. Seluruh data yang tersimpan dalam basis data berhasil terenkripsi dengan baik. Selain itu, tingkat linearitas jumlah karakter hasil enkripsi terhadap karakter aslinya mencapai 70,3%. Ini menunjukkan bahwa data yang ditampilkan telah dienkripsi dengan baik oleh algoritma yang diterapkan.

2. METODE PENELITIAN

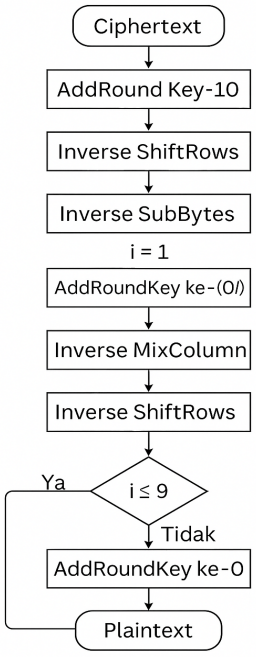
AES (*Advanced Encryption Standard*) 128-bit akan digunakan untuk mengamankan data penelitian ini. Beberapa proses utama yang perlu dilakukan termasuk *AddRoundKey, SubBytes, ShiftRows, MixColumns*, dan diakhiri dengan *AddRoundKey*. Setiap data yang masuk akan dienkripsi secara berurutan, sehingga *ciphertext* akan menjadi hasil output yang aman.



Gambar 1. Metode Penelitian Enkripsi AES-128

Selain enkripsi, proses dekripsi juga akan dilakukan menggunakan metode AES-128 untuk mengembalikan ciphertext menjadi data asli (*plaintext*). Terdapat tahapan yang harus dilalui secara bertahap dalam proses dekripsi, yaitu *AddRoundKey*, *Inverse ShiftRows*, *Inverse SubBytes*, *Inverse MixColumns* hingga data kembali ke bentuk semula.

Ketika data telah terenkripsi, proses dekripsi dapat digunakan untuk mengembalikannya ke bentuk awal. Hal tersebut biasanya dilakukan untuk keperluan tertentu, seperti ditampilkan kepada pengguna atau digunakan sistem untuk proses internal. Kunci yang digunakan harus sama seperti enkripsi untuk melakukan proses dekripsi.



Gambar 2. Metode Penelitian Dekripsi AES-128

2.1 Data Penelitian

Penelitian ini akan menggunakan data pegawai dari salah satu perusahaan logistik dengan inputan berupa *varchar*, *integer*, *text* dan *date*. Terdapat 13 jenis data yang akan diamankan, yaitu nama, sertifikat kompetensi, *rank*, nomor sertifikat, nomor telepon, tempat dan tanggal lahir, status, npwp, alamat npwp, jamsostek, nomor rekening, serta tanggal masuk pegawai (*sign on*). Masing-masing *field* memiliki ciri-ciri yang berbeda. Berikut rincian spesifikasinya:

Tabel 1. Spesifikasi Basis Data

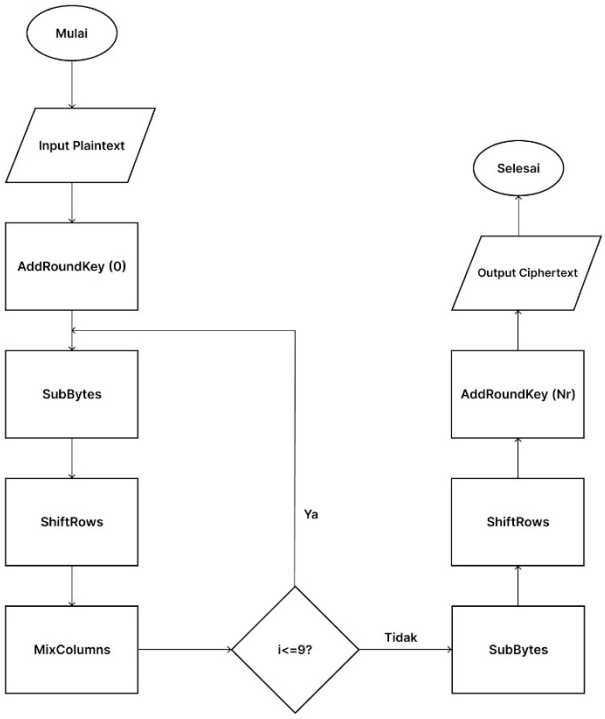
Nama *Field*	Tipe Data	Ukuran	Keterangan
id_pegawai	*integer*	11	id pegawai
nama	*varchar*	255	Nama
notelp	*varchar*	255	Nomor Telepon
tmplahir	*varchar*	100	Tempat Lahir
tgllahir	*varchar*	255	Tanggal Lahir
npwp	*varchar*	255	NPWP
alamatnpwp	*text*	-	Alamat NPWP
jamsostek	*varchar*	255	JAMSOSTEK
norek	*varchar*	255	Nomor Rekening
kompetensisertif	*varchar*	50	Sertifikat Kompetensi
rank	*varchar*	50	Rank
nosertif	*varchar*	255	Nomor Sertifikat
status	*varchar*	50	Status

Keseluruhan data pada tabel di atas akan dilakukan proses enkripsi dan dekripsi, kecuali id_pegawai. Hasil dari proses enkripsi akan tersimpan dalam basis data. Sedangkan, hasil dari proses dekripsi akan ditampilkan dalam aplikasi.

2.2 Flowchart

2.2.1 Flowchart Enkripsi

Flowchart untuk proses enkripsi AES-128 dijabarkan sebagai berikut:



Gambar 3. Flowchart Proses Enkripsi AES-128

Sebelum memulai proses enkripsi, data asli (*plaintext*) akan dimasukkan ke dalam sistem. Setelah itu, sistem akan melakukan empat proses enkripsi, yaitu *AddRoundKey*, *SubBytes*, *ShiftRows*, dan *MixColumns*. Keempat proses tersebut dilakukan secara berurutan sebanyak 10 kali perulangan. Untuk perulangan yang terakhir, proses *MixColumns* tidak dijalankan. Hasil dari proses enkripsi berbentuk *ciphertext*, yaitu bentuk data yang rumit dan sulit terbaca.

2.2.2 Flowchart Dekripsi

Selain enkripsi, proses dekripsi juga dijabarkan dalam bentuk flowchart. Berikut penggambaran prosesnya:

Gambar 4. Flowchart Proses Dekripsi AES-128

Dalam gambar di atas, dekripsi dilakukan dalam empat tahap: *inverse ShiftRows*, *inverse SubBytes, inverse MixColumns, dan AddRoundKey*. Jika tahap mixcolumns tidak dijalankan pada perulangan pertama, maka *inverse MixColumns* tidak dijalankan pada perulangan pertama. Proses dekripsi menghasilkan data asli yang mudah dibaca, atau *plaintext*.

3. HASIL DAN PEMBAHASAN

3.1 Hasil Pengujian Enkripsi

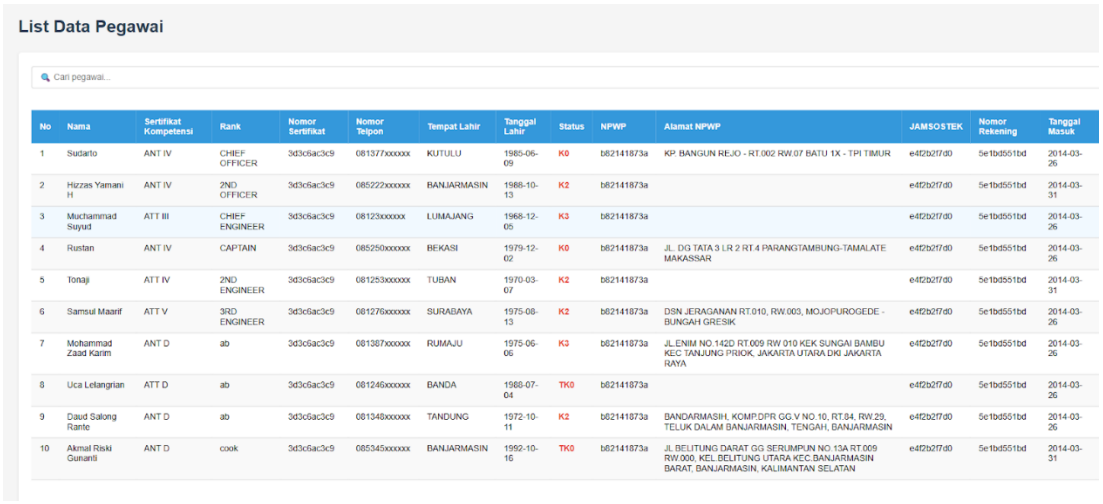
Setelah proses enkripsi dilakukan, data akan tampil dalam bentuk yang sulit dibaca atau biasa disebut dengan *ciphertext*. Berikut tampilan hasil dari proses enkripsi:

nama	kompetensisertif	rank	nosertif
63c66e60c563247c7a012004212263dc	d83647cacf5d85406c736b8c2e643cd2	7878cf8762979839966f4f333c4af1a7b	09f93e2c9ef8239878efa1a2a0c84036cea63ebf7d9456c929...
d2bb0e8bb53c4698080a224989b1ee10482f78e9688013181e...	d83647cacf5d85406c736b8c2e643cd2	6d94bb55b085ad67384ec6c18e3e89a8	183495f5b5f7a65eca65363b8e8bf55b96552a3f026e8be286...
74da06b7332e5662bee461edcf79f81b7ffcb2cf26efeb6fd4...	d83647cacf5d85406c736b8c2e643cd2	1b49481d04a2ac978cfa9be69375aa42	c04425a90835c3304455f684d5319fd120771c37c7cdbb719f...
fb0e19c4dca92613ccdcc27f5b0d3858ae48cd81f5701833a5...	599691979060f34d5f6056599dc35b2c	218c1da96da900348eb42c49fe2e3c42	82acb23f0599628f82154e63ac18df3e49287f43b8d49b0985...
181a02eb3096270d7da5085f0e9e0f97ed5e805c468974b167...	a3c7552cf7708bf31eaa4a62a44bd4b6	fae3fa34b87093f8fc36f92590b879e7	6510f2368179426969e7e78bd6506577e5d283b14de0743558...
dc678c580a9882a0ffa4d9b3d2347d5488217e8d0f400d5ecd...	dcd7cff0dbcdfef140baedea4145ef91	3ccb0684a242cc90088f0fda31db5aa8	430af5c152c22b0085a70a9844084d85ec2221bbe0e984862b...
bc2ccacb3687703d2cd3d03b6fceb5d302c39a826691b35b6c...	bcf7e1cc0087d62bc92da553263081cd	3ccb0684a242cc90088f0fda31db5aa8	6e71d393cad6575dea652b69a5da0bfa
48e0386cabac330b3d119eda3988db2a6e9ce2d8bcc3d437d0...	dcd7cff0dbcdfef140baedea4145ef91	3ccb0684a242cc90088f0fda31db5aa8	525a4cbd2fb3d6b13c47dbab2d66a0827357c8106248660752...
8b706521e2130d3eb949c30527f076d715fbb0da2fa85a4ff2...	dcd7cff0dbcdfef140baedea4145ef91	1b49481d04a2ac978cfa9be69375aa42	3d3c6ac3c961589a33019521d2c41488888565cce28be7ee92...

Gambar 5. Hasil Pengujian Enkripsi

3.2 Hasil Pengujian Dekripsi

Data yang telah terenkripsi dapat kembali terbaca dengan melalui proses dekripsi. Hasil dari proses dekripsi biasa disebut dengan *plaintext*. Berikut tampilan hasil dari proses dekripsi:



No	Nama	Sertifikat Kompetensi	Rank	Nomor Sertifikat	Nomor Telpon	Tempat Lahir	Tanggal Lahir	Status	NPWP	Alamat NPWP	JAMSOSTEK	Nomor Rekening	Tanggal Masuk
1	Sudarto	ANT IV	CHIEF OFFICER	3d3c6ac3c9	081377xxxxxx	KUTULU	1985-06-09	K0	b82141873a	KP. BANGUN REJO - RT.002 RW.07 BATU 1X - TPI TIMUR	e4f2b2f7d0	5e1bd551bd	2014-03-26
2	Hizzas Yamani H	ANT IV	2ND OFFICER	3d3c6ac3c9	085222xxxxxx	BANJARMASIN	1988-10-13	K2	b82141873a		e4f2b2f7d0	5e1bd551bd	2014-03-31
3	Muchammad Suyud	ATT III	CHIEF ENGINEER	3d3c6ac3c9	08123xxxxxx	LUMAJANG	1968-12-05	K3	b82141873a		e4f2b2f7d0	5e1bd551bd	2014-03-26
4	Rustan	ANT IV	CAPTAIN	3d3c6ac3c9	085250xxxxxx	BEKASI	1979-12-02	K0	b82141873a	JL. DG TATA 3 LR 2 RT.4 PARANGTAMBUNG-TAMALATE MAKASSAR	e4f2b2f7d0	5e1bd551bd	2014-03-26
5	Tonaji	ATT IV	2ND ENGINEER	3d3c6ac3c9	081253xxxxxx	TUBAN	1970-03-07	K2	b82141873a		e4f2b2f7d0	5e1bd551bd	2014-03-31
6	Samsul Maarif	ATT V	3RD ENGINEER	3d3c6ac3c9	081276xxxxxx	SURABAYA	1975-08-13	K2	b82141873a	DSN JERAGANAN RT.010, RW.003, MOJOPUROGEDE - BUNGAH GRESIK	e4f2b2f7d0	5e1bd551bd	2014-03-26
7	Mohammad Zaad Karim	ANT D	ab	3d3c6ac3c9	081387xxxxxx	RUMAJU	1975-06-06	K3	b82141873a	JL.ENIM NO.142D RT.009 RW.010 KEK SUNGAI BAMBU KEC.TANJUNG PRIOK, JAKARTA UTARA,DKI JAKARTA RAYA	e4f2b2f7d0	5e1bd551bd	2014-03-26
8	Uca Lelangrian	ATT D	ab	3d3c6ac3c9	081246xxxxxx	BANDA	1988-07-04	TK0	b82141873a		e4f2b2f7d0	5e1bd551bd	2014-03-26
9	Daud Salong Rante	ANT D	ab	3d3c6ac3c9	081348xxxxxx	TANDUNG	1972-10-11	K2	b82141873a	BANDARMASIH, KOMP.DPR GG.V NO.10, RT.84, RW.29, TELUK DALAM BANJARMASIN, TENGAH, BANJARMASIN	e4f2b2f7d0	5e1bd551bd	2014-03-26
10	Akmal Riski Gunanti	ANT D	cook	3d3c6ac3c9	085345xxxxxx	BANJARMASIN	1992-10-16	TK0	b82141873a	JL.BELITUNG DARAT GG.SERUMPUN NO.13A RT.009 RW.000, KEL.BELITUNG UTARA KEC.BANJARMASIN BARAT, BANJARMASIN, KALIMANTAN SELATAN	e4f2b2f7d0	5e1bd551bd	2014-03-31

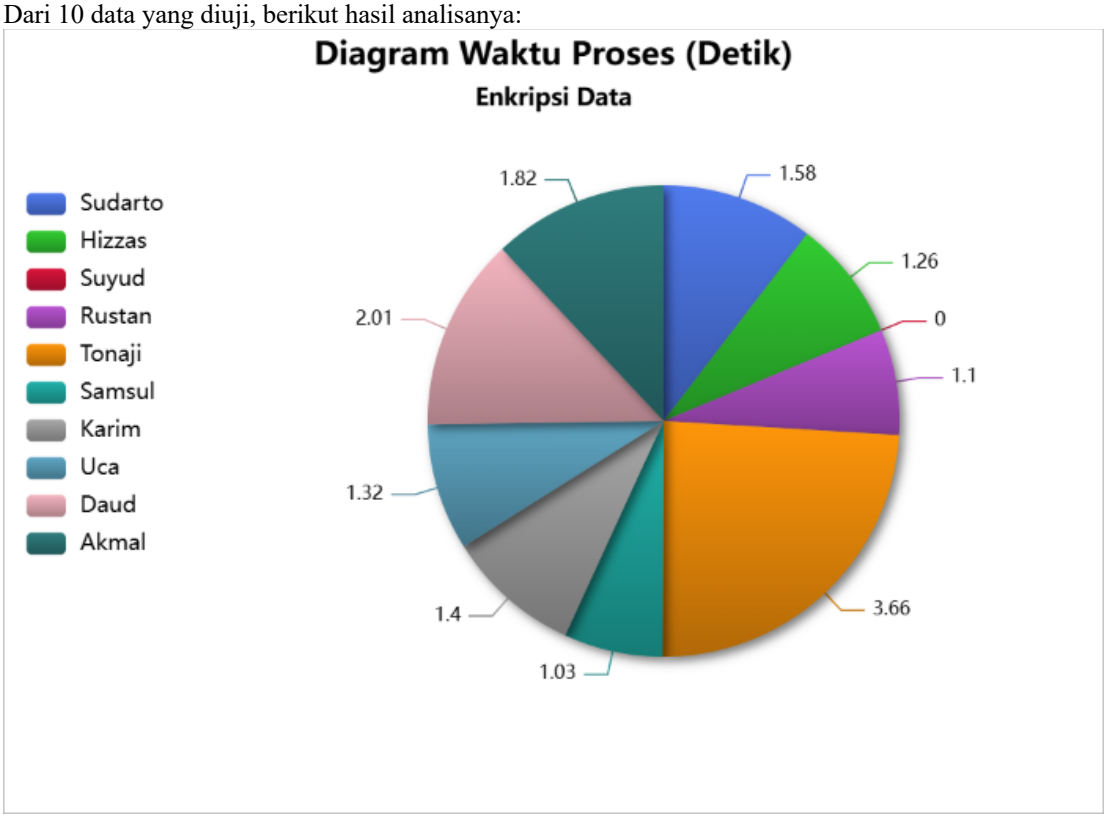
Gambar 6. Hasil Pengujian Dekripsi

3.3 Analisa Hasil

Hasil analisa dari dua pengujian yang telah dilakukan digambarkan sebagai berikut:

3.3.1 Analisa Pengujian Enkripsi

Dari 10 data yang diuji, berikut hasil analisanya:

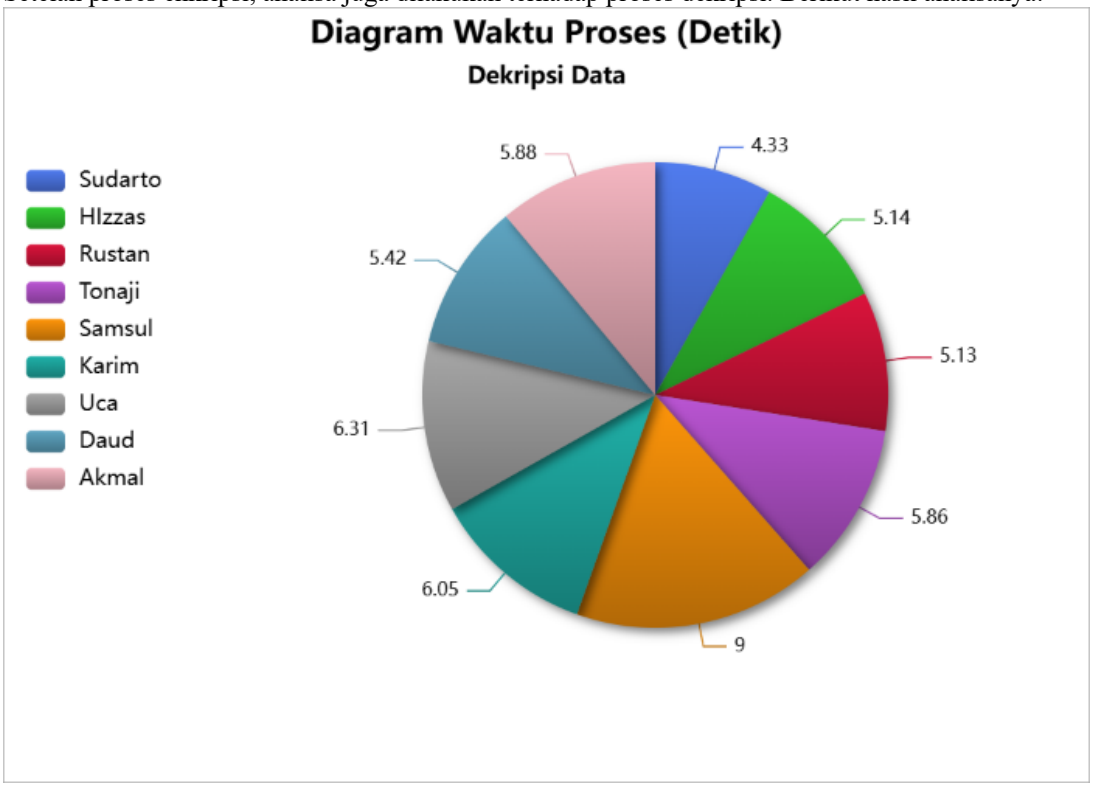


Gambar 7. Hasil Analisa Pengujian Enkripsi

Berdasarkan diagram tersebut, 9 dari 10 data berhasil terenkripsi dalam waktu yang cukup singkat, yakni selama 1 hingga 4 detik. Sebagian besar data melalui proses enkripsi selama 1 atau 2 detik. Berbeda dengan informasi data pegawai yang dimiliki oleh Tonaji yang berhasil diproses dalam waktu 3.66 detik. Hal ini mungkin saja terjadi karena ukuran atau karakteristik datanya lebih kompleks daripada data yang lain. *Delay* sistem juga bisa menjadi penyebab lamanya waktu proses. Namun, kondisi tersebut masih dalam batas wajar dan tidak mengindikasikan gagalnya proses enkripsi.

3.3.2 Analisa Pengujian Dekripsi

Setelah proses enkripsi, analisa juga dilakukan terhadap proses dekripsi. Berikut hasil analisanya:



Gambar 8. Hasil Analisa Pengujian Dekripsi

Waktu yang ditempuh untuk menjalankan proses dekripsi berlangsung lebih lama daripada proses dekripsi, yakni berkisar antara 4 hingga 10 detik. Hal tersebut mungkin terjadi karena besarnya ukuran data yang telah terenkripsi pada basis data. Sistem akan melakukan proses dekripsi dengan membaca seluruh isi basis data keseluruhan walaupun *user* memasukkan data string yang berukuran pendek. Selain itu, spesifikasi perangkat keras juga cukup berpengaruh pada jalannya proses dekripsi.

4. KESIMPULAN

Keberhasilan enkripsi basis data perusahaan adalah kesimpulan dari berbagai prosedur yang telah dilakukan. Itu disebabkan karena hasil dari enkripsi membuat data menjadi sulit untuk terbaca. Beberapa hal lain yang dapat ditarik kesimpulannya adalah waktu proses enkripsi dan dekripsi. Beberapa faktor seperti tingkat kompleksitas data, besarnya ukuran data, dan kondisi perangkat dapat mempengaruhi durasi kedua proses tersebut.

Memfokuskan data yang akan dienkripsi bisa menjadi saran untuk penelitian di masa depan. Itu disebabkan karena durasi proses dekripsi bergantung kepada banyaknya data yang terenkripsi. Semakin banyak data yang terenkripsi, semakin lama durasi untuk mendekripsinya. Maka dari itu, jalankanlah proses enkripsi kepada data yang dianggap krusial dan sensitif saja sehingga waktu proses enkripsi dan dekripsi serta ukuran basis data dapat diminimalisir.

DAFTAR PUSTAKA

[1] Arini, S. C. (2024, August 12). 4,7 Juta Data ASN diduga bocor, BKN Imbau segera ganti password. Detikcom. https://www.detik.com/sumbagsel/berita/d-7485273/4-7-juta-data-asn-diduga-bocor-bknimbau-segera-ganti-password

[2] Aryanto, M. B, Tahir, M, Devita S. I, Mustofa, Z. N, Ainiyah Q, & Sundoro, S. (2023). *Implementasi enkrip dan dekrip file menggunakan metode advance encryption standard (AES-128)*. Jurnal Ilmiah Sistem Informasi Dan Ilmu Komputer, *3*(1), 89–104. https://doi.org/10.55606/juisik.v3i1.434

[3] Sianipar, J. S., Nugroho, N. B., & Mariami, I. (2024). Pengamanan data gaji karyawan dengan menggunakan metode advanced encryption standard (AES). *Jurnal Sistem Informasi Triguna Dharma (JURSI TGD)*, *3*(1), 35–45. https://doi.org/10.53513/jursi.v3i1.5653

[4] Nanda Rahmat Herlambang, D., Nilma, Ni., & Pravitasari, N. (2024). Penerapan Kriptografi AESuntuk Keamanan Data Aplikasi Pemesanan Bibit Ternak pada BPSI UAT. *Remik : Riset Dan E-Journal Manajemen Informatika Komputer*, *8*(1).

[5] Imron, M., & Pratama, A. (2022). Pengamanan E-Dokumen Berbasis Steganografi Dengan Kombinasi Advanced Encryption Standard (AES) 128 Bit. *InfoTekJar : Jurnal Nasional Informatika Dan Teknologi Jaringan*, *6*(2).

[6] Widyawan, D., & Imelda, I. (2021). Pengamanan File Menggunakan Kriptografi Dengan Metode Aes-128 Berbasis Web Di Komite Nasional Keselamatan Transportasi. *Skanika*, *4*(1), 15–22. https://doi.org/10.36080/skanika.v4i1.2216

[7] Ravida, R., & Santoso, H. A. (2020). Advanced Encryption Standard (AES) 128 Bit untuk Keamanan Data Internet of Things (IoT) Tanaman Hidroponik. *Jurnal RESTI (Rekayasa Sistem Dan Teknologi Informasi)*, *4*(6). https://doi.org/10.29207/resti.v4i6.2478

[8] Alvian Winata, A., Syafrullah, M., & Irawan, I. (2024). Implementasi Algoritme Kriptografi Advanced Encryption Standard (AES-128) untuk Pengamanan Data Berbasis Web pada McDonald's Cabang T.B. Simatupang. *Jurnal Ticom: Technology of Information and Communication*, *12*(3), 91–96. https://doi.org/10.70309/ticom.v12i3.124

[9] Sutarjo, H., & Waluyo, S. (2024). Implementasi Kriptografi Aes-128 Untuk Pengamanan Data Purchase Order Pada Pt Antilope Madju Puri Indah. *Seminar Nasional Mahasiswa Fakultas Teknologi Informasi (SENAFTI)*, *3*(2).

[10] Linda, H., Sitorus, S. H., & Ristian, U. (2023). Penerapan Algoritma Advanced Encryption Standard (Aes)-128 Bit Pada Keamanan Database Aplikasi Kepelangganan (Studi Kasus: Perumda Air Minum Tirta Khatulistiwa). *Coding Jurnal Komputer Dan Aplikasi*, *11*(1), 128. https://doi.org/10.26418/coding.v11i1.58122