ANALISIS ENKRIPSI DATA DENGAN METODE *ADVANCED ENCRYPTION STANDARD* (AES) MENGGUNAKAN BORLAND DELPHI

Richard Yesaya Simanjuntak[1], Amrullah[2], Wahidaturrahmi[3], Sudi Prayitno[4]
[1,2,3,4]Pendidikan Matematika FKIP Universitas Mataram
[1]richardyesaya18@gmail.com

ABSTRACT

The Technological developments caused by the COVID-19 pandemic have forced people to understand how to use the existing technology, the education sector is also experiencing the impact, for example using distance or online learning. In this case, it does not rule out the possibility of theft of personal data which is detrimental to society, such as the rise of cases of online loans using other people's data. This study aims to obtain an application that can be used to protect data, in this study using the AES algorithm with the Borland Delphi programming language. The method used is to design an application that can encrypt 30 text files which are divided into small, medium, and large categories. The results obtained are an average increase of 10 small files of 96.4%, an average increase in the size of 10 medium-sized files of 60.7%, and an average increase in the size of 10 large files of 53.3%. The conclusion obtained in this study is that Borland Delphi can be used to protect data and the size of the data before it is encrypted affects the size of the encryption results and the smaller the data size, the greater the percentage increase in size.

Keywords: Enryption, AES, Delphi

ABSTRAK

Perkembangan teknologi yang disebabkan oleh pandemi COVID-19 telah membuat masyarakat harus paham meggunakan teknologi yang ada, sektor pendidikan juga merasakan dampaknya contohnnya digunakan pembelajaran jarak jauh atau daring. Dalam hal ini tidak menutup kemungkinan terjadinya pencurian data pribadi yang merugikan bagi masyarakat seperti maraknya kasus pinjaman online namun menggunakan data orang lain. Penelitian ini bertujuan untuk mendapatkan suatu aplikasi yang dapat digunakan untuk melindungi data, dalam penelitian ini menggunakan algoritma AES dengan bahasa pemograman Borland Delphi. Adapun metode yang digunakan adalah merancang sebuah aplikasi yang dapat mengenkripsi 30 file teks yang terbagi dalam kategori kecil, menegah, dan besar. Hasil yang didapatkan adalah rata – rata kenaikan 10 file berukuran kecil 96,4 %, rata – rata kenaikan ukuran 10 file berukuran menengah 60,7 %, dan rata – rata kenaikan ukuran 10 file berukuran besar 53,3 %. Kesimpulan yang didaptkan dalam penelitian ini adalah Borland Delphi dapat digunakan unutk melindungi data dan ukuran data sebelum dienkripsi mempengaruhi ukuran hasil enkripsinya serta semakin kecil ukuran data maka persentase kenaikan ukurannya semakin besar.

Kata Kunci: Kriptografi, AES, Delphi

A. Pendahuluan

Pandemi COVID-19 yang melanda dunia, termasuk Indonesia mengakibatkan masyarakat lebih mngikuti perkembangan teknologi, dikarenakan peraturan yang ditetapkan oleh Pemerintah yaitu *social distancing* menyebabkan banyak sektor mulai berangsur beralih ke digital, Sektor pendidikan merupakan salah satu yang mengalami dampaknya. Hal ini dapat diliat dengan meningkatnya pembelajaran yang dilakukan secara *online* atau jarak jauh. Pembelajaran jarak jauh memberikan dampak yang signifikan termasuk hal yang negatif seperti meningkatnya *cybercrime* dalam hal ini cenderung dalam kasus pencurian data. Pencurian data sangat merugikan bagi korban karena data yang dicuri disalahgunakan seperti dipakai untuk pinjaman online. Hal ini disebabkan oleh kurangnya pehamaman masyarakat tentang pentingnya menjaga privasi data sendiri (Situmeang, 2021) . Untuk melindungi data – data ini membutuhkan ilmu untuk melindungi data yang penting, ilmu ini disebut dengan kriptografi (Rasidin & Nugroho, 2022). *Advanced Encryption Standard* atau AES merupakan salah satu algoritma kriptografi yang digunakan untuk mengamankan data. Proses mengamankan data atau *plain text* disebut dengan enkripsi, hasil dari enkripsi disebut dengan *ciphertext* sedangkan proses mengembalikan *ciphertext* ke *plain text* disebut deskripsi.

Penelitian kriptografi AES telah banyak dilakukan sebelumnya, masing – masing penelitian menggunakan algoritma AES dengan berbagai cara, penelitian oleh Voni Yuniati, dkk (2009)dengan judul enkripsi dan deskripsi dengan algortima AES 256 untuk semua jenis file, didapatkan kesimpulan bahwa waktu enkripsi dan deskripsi berbeda dikarenakan adanya pemakaian *resources* computer, kemudian ada penelitian dari Aditia Rahmat Tulloh ,dkk (2016) dengan judul kriptografi *advanced encryption standard* (AES) untuk penyandian file dokumen,dalam penelitian ini menarik kesimpuan bahwa MATLAB membantu proses enkripsi dan deskripsi dengan cepat tepat dan efisien. Pada penelitian ini akan berfokus pada penyandian file teks dengan AES 128 *bytes* sebagai

dengan Bahasa pemograman delphi yang diharapkan dapat digunakan untuk penyimpanan data – data teks yang penting dalam bidang pendidikan.

B. Metode Penelitian

Penelitian ini menggunakan pendekatan metode eksperimen. Penelitian eksperimen merupakan suatu metode penelitian yang digunakan untuk mencari pengaruh perlakuan tertentu terhadap yang lain dalam kondisi yang terkendalikan (Sugiyono, 2013). Penelitian akan berlangsung di laboratorium FKIP Universitas Mataram selama semester genap 2023. Adapun Langkah penelitian ini sebagai berikut :

1. Studi Literatur

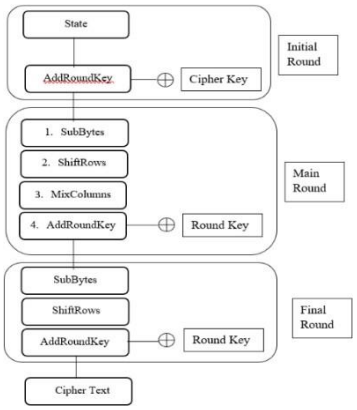
   Studi literatur digunakan sebagai pembanding penelitian yang akan dilakukan. Studi literatur dapat dilakukan dengan membaca buku, tesis, karya ilmiah dan jurnal yang berkaitan dengan permasalahan yang diangkat oleh peneliti. Penelitian ini menggunakan karya ilmiah, dan jurnal yang membahas kriptografi khususnya kriptografi AES sebagai studi literatur yang relevan untuk mendukung peneliti.

2. Perancangan Aplikasi

   Aplikasi dirancang menggunakan algoritma AES dan diimplementasikan dengan Bahasa pemograman delphi, rancangan aplikasi akan memperhatikan algoritma AES dengan diagram alir sebagai berikut

   a. Enkripsi

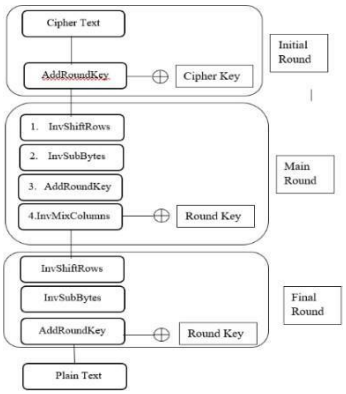
      Enkripsi AES memiliki beberapa tahapan yaitu *AddroundKey* (penambahan *round key* dengan *state* menggunakan operasi XOR), *Subbytes* (penggantian *byte* dari *state* menggunakan tabel S-box), *ShiftRows* (penggeseran baris – baris *array state*), dan *MixColumns* (pengacakansetiap elemen pada masing- masing *array state*), dan dilakukan dengan dengan 10 ronde (Sihombing et al., 2019)



Gambar 1. Skema enkripsi AES

b. Deskripsi

Deskripsi AES memiliki beberapa tahapan yaitu menggunakan *AddRoundKey*, *InvShiftsRows* (pergeseran pada tahap ini di geser ke kanan), *InvSubbytes* (penggantian yang dilakukan menggunakan tabel *Inverse S-Box*), dan *InvMixColumns.* dan dilakukan dengan dengan 10 ronde (Prameshwari & Sastra, 2018)



Gambar 2. Skema Deskripsi AES

3. Pengujian Aplikasi

Pengujian aplikasi memiliki tujuan untuk menjamin program berjalan dengan lancar sehingga dapat menunjukkan hasil yang sesuai dengan hasil dari analisis yang telah dipaparkan

4. Analisis Data

Analisis data dilakukan dengan mengambil 30 file teks secara random yang akan dibagi menjadi 3 yaitu 10 file ukuran kecil dengan range 1 – 100 *bytes*, 10 file ukuran menengah dengan range 101 – 600 *bytes*, dan 10 ukuran besar dengan range 601 – 10000 *bytes* (10 kB). Data dianalisis dengan mengunakan uji ANOVA satu jalur dengan hipotesis yaitu :

H_0 = tidak terdapat perbedaan rata – rata antara ketiga kategori file ukuran data

H_1 = terdapat perbedaan rata – rata antara ketiga kategori file ukuran data

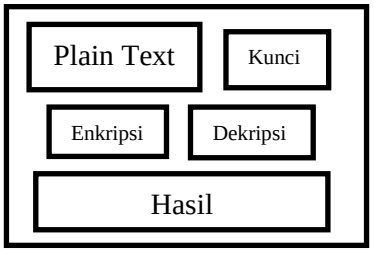
Statisik uji yang digunakan adalah $p - value$, dimana H_0 ditolak apabila nilai $p - value < \alpha$ yang berarti bahwa terdapat perbedaan rata – rata, sebaliknya jika $p - value > \alpha$ maka H_0 diterima yang berarti tidak terdapat perbedaan rata – rata.

5. Kesimpulan

Hasil yang didapatkan dalam penelitian ini akan disimpulkan apakah sesuai dengan tujuan yang diharapkan oleh penulis.

C.Hasil Penelitian dan Pembahasan

Penelitian dimulai dengan peneliti merancangkan aplikasi yang akan dibuat, aplikasi akan dibuat memiliki 5 komponen utama yaitu, Plain Text Box, Cipher Key Box, Tombol Enkripsi, Tombol Deskripsi, dan Hasil Enkripsi/Deskripsi Box. Rancangan dapat dilihat pa**d**a gambar 3

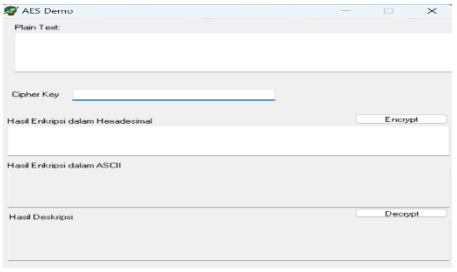


Gambar 3. Rancangan Aplikasi

dengan keterangan :

1. Plain Text Box adalah tempatuntuk *input* teks yang ingin dienkripsi atau dideskripsi
2. Cipher Key Box / Kunci adalah tempat untuk *input* kata kunci
3. Enkripsi Button adalah tombol untuk menjalankan perintah enkripsi
4. Deskripsi Button adalah tombol untuk menjalankan perintah deskripsi
5. Hasil Enkripsi / Deskripsi Box adalah tempat untuk menampilkan enkripsi atau dekripsi setelah perintah dari button dijalankan.

Kemudian rancangan akan diimplemtasikan dengan bahasa pemograman Borland Delphi menggunakan algoritma AES. Hasil dapat dilihat pada Gambar 4



Gambar 4. Hasil Implementasi

Kemudian dilakukan penelitian terhadap 30 file teks yang dibagi menjadi 3 kategori yaitu file berukuran kecil, menengah, dan besar yang dapat dilihat pada tabel 1, 2, dan 3

Tabel 1 Tabel File Berukuran Kecil (1 – 100 *bytes*)

NO	Nama File	Ukuran sebelum Enkripsi (*bytes)*	Ukuran Setelah Enkripsi (*bytes)*	Persentase Kenaikan (%)
1	FILE 1	10	26	**160**
2	FILE 2	20	51	**155**
3	FILE 3	24	49	**104,17**
4	FILE 4	34	77	**126,47**
5	FILE 5	46	75	**63,04**
6	FILE 6	60	106	**76,67**
7	FILE 7	63	99	**57,14**
8	FILE 8	75	128	**70,67**
9	FILE 9	86	149	**73,26**
10	FILE 10	99	170	**71,71**
Rata – rata perubahan ukuran data				**96,4**

Tabel 1 menunjukkan hasil penelitian untuk kategori fileberukuran kecil dengan range 1 – 100 *bytes* sebanyak 10 file teks telah dienkripsi menggunakan algoritma AES dan didapatkan hasil file 1 memiliki persentase kenaikan ukuran terbesar dan file 7 memiliki persentasekenaikan terkecil. Kategori file berukuran kecil memiliki rata – rata 96,4 %.

Tabel 2 Tabel File Berukuran Menengah (101 – 600 *bytes*)

NO	Nama File	Ukuran sebelum Enkripsi (*bytes)*	Ukuran Setelah Enkripsi (*bytes*)	Persentase Kenaikan (%)
1	FILE 11	102	181	**77,45**
2	FILE 12	152	236	**55,26**
3	FILE 13	249	395	**58,63**
4	FILE 14	275	468	**70,18**
5	FILE 15	343	544	**58,60**
6	FILE 16	351	547	**55,84**
7	FILE 17	432	666	**54,17**
8	FILE 18	465	742	**59,57**
9	FILE 19	504	783	**55,36**
10	FILE 20	586	951	**62,29**
Rata – rata perubahan ukuran data				**60,7**

Tabel 2 menunjukkan hasil penelitian untuk kategori file berukuran menegah dengan range 101 – 600 *bytes* sebanyak 10 file teks telah dienkripsi menggunakan algoritma AES dan didapatkan hasil file 11 memiliki persentase kenaikan ukuran terbesar dan file 12 memiliki persentase kenaikan terkecil. Kategori file berukuran menengah memiliki rata – rata 60,7 %.

Tabel 3 Tabel File Berukuran Besar (601 – 10000 *bytes*)

NO	Nama File	Ukuran sebelum Enkripsi (*bytes*)	Ukuran Setelah Enkripsi (*bytes*)	Persentase Kenaikan (%)
1	FILE 21	615	989	**60,81**
2	FILE 22	683	1069	**56,52**
3	FILE 23	740	1021	**37,97**
4	FILE 24	792	1272	**60,60**
5	FILE 25	828	1206	**45,65**
6	FILE 26	876	1354	**54,57**
7	FILE 27	924	1452	**57,14**
8	FILE 28	985	1431	**45,28**
9	FILE 29	3450	4881	**41,48**
10	FILE 30	8330	14400	**72,87**
Rata – rata perubahan ukuran data				**53,3**

Tabel 3 menunjukkan hasil penelitian untuk kategori file berukuran besar dengan range 601 – 10000 *bytes* sebanyak 10 file teks telah dienkripsi menggunakan algoritma AES dan didapatkan hasil file 30 memiliki persentase kenaikan ukuran terbesar dan file 29 memiliki persentase kenaikan terkecil. Kategori file berukuran besar memiliki rata – rata 53,3 %.

Kemudian data hasil penelitian akan diuji menggunakan uji ANOVA satu jalur untuk memmbandingkan persentase kenaikan antara ketiga kelompok yang telah dianalisis, hasil uji ANOVA dapat dilihat pada tabel 4

Tabel 4.5 Tabel ANOVA

Source of Variation	*SS*	*df*	*MS*	*F*	*P-value*	*F crit*
Between Groups	10314	2	5156,99	9,39	0,000798	3,35
Within Groups	14814,91	27	548,70			
Total	25128,9	29				

Berdasarkan hasil penelitian yang telah dilakukan terhadap 30 file teks yang dapat dilihat pada tabel 1, 2, dan 3 menunjukkan bahwa rata – rata kategori file berukuran kecil adalah 96,4 %, rata – rata kategori file berukuran menengah adalah 60,7 %, rata – rata kategori file berukuran besar adalah 53,3 %. Dapat dilihat bahwa rata – rata persentase kenaikan ukuran file teks menurun setiap kategori, sehingga dapat disimpulkan bahwa ukuran awal data mempengaruhi persentase kenaikan ukuran data setelah dilakukan enkripsi, kemudian terlihat juga bahwa persentase data pada kategori menengah dan besar terlihat konstan pada angka ± 55 %. Hal ini serupa dengan peneltian Aji Fitrah Marisman dan Anita Hidayati (2015) yang membandingkan penggunaan aplikasi enkipsi *caesar cipher* dan AES dan menghasilkan kesimpulan bahwa ukuran file setelah dienkripsi menggunakan AES persentase tejadi kenaikan ukuran, kemudian Yuniati (2009) juga mengatakan bahwa adanya pertambahan ukuran disebabkan oleh saat melakukan enkripsi, ditambahkan *header* untuk menyimpan informasi file sumber sehingga pada penelitian Yuniati, hasil enkripsinya bertambah dengan catatan bahwa ketika hasil deskripsi dikembalikan maka ukurannya juga akan kembali seperti semula, Veronica Lusiana (2011) juga mengatakan semakin besar ukuran file dan panjang kunci AES menyebabkan semakin besar ukuran file enkripsi yang dihasilkan.Kemudian dilakukan uji ANOVA satu jalur dan didapatkan nilai P-*value* < 0,05, sehingga didapatkan hasil bahwa ketiga kategori file memiliki perbedaan persentase yang signifikan.

D. Kesimpulan

Berdasarkan hasil penelitian yang didapat, kesimpulan yang dapat ditarik adalah semakin kecil ukuran data maka semakin besar persentase kenaikan ukurannya setelah dienkripsi namun semakin besar ukuran data maka persentase kenaikannya akan terlihat konstan

DAFTAR PUSTAKA

Lusiana, V. (2011). Implementasi Kriptografi Pada File Dokumen Menggunakan Algoritma Aes-128. *Dinamika Informatika: Jurnal Ilmiah Teknologi Informasi*, *3*(2), 79–83. https://doi.org/https://doi.org/10.35315/informatika.v3i2.1313

Marisman, A. F., & Hidayati, A. (2015). Pembangunan Aplikasi Pembanding Kriptografi Dengan Caesar Cipher Dan Advance Encryption Standand (Aes) Untuk File Teks. *Jurnal Penelitian Komunikasi Dan Opini Publik*, *19*(3), 213–222. https://doi.org/https://doi.org/10.33299/jpkop.19.3.348

Prameshwari, A., & Sastra, N. P. (2018). Implementasi Algoritma Advanced Encryption Standard (AES) 128 Untuk Enkripsi dan Dekripsi File Dokumen. *Eksplora Informatika*, *8*(1), 52. https://doi.org/10.30864/eksplora.v8i1.139

Rasidin, A., & Nugroho, A. J. (2022). *Analisa Penggunaan Teknik Advanced Encryption (AES) dalam Kriptografi*. *April*, 21–29. https://doi.org/http://dx.doi.org/10.31000/dinamika.v7i1.8059

Sihombing, M., Sitompul, J. N., & Putri, T. A. (2019). Implementasi Metode Kriptografi Advanced Encryption Standard (AES) untuk Proteksi Pesan Audio. *MEANS (Media Informasi Analisa Dan Sistem)*, *4*(1), 37–45. https://doi.org/10.54367/means.v4i1.317

Situmeang, S. M. T. (2021). Penyalahgunaan Data Pribadi Sebagai Bentuk Kejahatan Sempurna Dalam Perspektif Hukum Siber. *Sasi*, *27*(1), 38. https://doi.org/10.47268/sasi.v27i1.394

Sugiyono, D. (2013). *Metode Penelitian Kuantitatif, Kualitatif, dan Tindakan* (19th ed.).

Alfabeta, CV.

Tulloh, A. R., Permanasari, Y., & Harahap, E. (2016). Kriptografi Advanced Encryption Standard (AES) Untuk Penyandian File Dokumen. *Matematika*, *15*(1), 7–14.

Yuniati, V., Indriyanta, G., & Rachmat c, A. (2009). Enkripsi dan dekripsi dengan algoritma aes 256 untuk semua jenis file. *JURNAL INFORMATIKA*, *5*(1).