Studi Literatur: Analisa Perbandingan Teori Tentang Tingkat Keamanan Antar Algoritma Simetris

I Made Adi Bhaskara[1] , Made Pasek Agus Ariawan[2], Ida Bagus Adisimakrisna Peling[3], I Putu Astya Prayudha[4]

[1]*Prodi Teknik Komputer, Fakultas Teknik dan Perencanaan, Universitas Warmadewa*

[2,3,4]*Program Studi Sarjana Terapan Teknologi Rekayasa Perangkat Lunak Jurusan Teknologi Informasi, Politeknik Negeri Bali*

Korespondensi Email : pasekagus@pnb.ac.id

Intisari— **Keamanan data menjadi isu penting di era digital, dan algoritma kriptografi berperan penting dalam menjaga kerahasiaan informasi. Algoritma simetris menawarkan kemudahan dan kecepatan, tetapi pemilihan algoritma yang tepat sangat penting untuk memastikan tingkat keamanan yang memadai Bidang ilmu kriptografi secara umum diketahui ada dua kategori algoritma enkripsi dan dekripsi suatu data salah satunya adalah algoritma simetris. Algoritma simetris banyak digunakan dalam suatu enkripsi data sehingga teori-teori baru banyak bermunculan. Jenis dari algoritma simetris bermacam-macam seperti algoritma DES, algoritmaAES atau rijndael, algoritma 3DES, dan lain-lain. Seiring dengan banyaknya teori algoritma simetris yang digunakan dalam bidang ilmu kriptografi, maka kualitas suatu algoritma dengan algoritma yang lain perlu dibandingkan untuk mencari algoritma simetris yang paling aman terhadap serangan. Berdasarkan studi literatur ini didapatkan hasil bahwa algoritma AES merupakan algoritma yang paling aman dibandingkan DES dan 3DES.**

Kata kunci— Kriptografi, Enkripsi, Dekripsi, Algoritma Simetris, AES.

Abstract— **Data security has become a critical issue in the digital age, and cryptographic algorithms play a vital role in preserving information confidentiality. Symmetric algorithms offer convenience and speed, but choosing the right algorithm is crucial to ensuring an adequate level of security. Disciplines of cryptography is generally known, there are two categories of a data encryption and decryption algorithm one of which is a symmetric algorithm. Symmetric algorithms are widely used in the encryption of the data so that new theories are emerging. Types of symmetric algorithms are various algorithms such as DES algorithm, AES or Rijndael algorithm, 3DES algorithm and others. Along with the many theories of symmetric algorithms are used in the discipline cryptography, the security of an algorithm with other algorithms need to be compared to find the most appropriate against attack. Based on this literature study results obtained that the AES algorithm is the most secure algorithm compared to DES and 3DES.**

Keywords— Cryptography, Encryption, Decryption, Symmetric Algorithms, AES.

I. PENDAHULUAN

Keamanan data menjadi isu penting dalam era digital, terutama terkait dengan kerahasiaan informasi. Algoritma kriptografi berperan penting dalam menjaga keamanan data dengan menyenkripsi data sebelum transmisi atau penyimpanan. Algoritma simetris menggunakan kunci yang sama untuk enkripsi dan dekripsi, menawarkan kemudahan dan kecepatan dalam pengolahan data. Namun, pemilihan algoritma simetris yang tepat sangat penting untuk memastikan tingkat keamanan yang memadai.

Bidang ilmu kriptografi secara umum diketahui ada dua kategori algoritma enkripsi dan dekripsi suatu data salah satunya adalah algoritma simetris. Algoritma simetris merupakan suatu algoritma dimana kunci yang digunakan untuk mengenkripsi dan mendekripsi suatu pesan menggunakan kunci yang sama. Seiring pesatnya kemajuan ilmu tentang pengenkripsian suatu pesan pada ilmu kriptografi memunculkan banyak algoritma. Jenis algoritma yang menggunakan teori algoritma simetris bermacam-macam seperti algoritma DES, algoritma AES atau rijndael, algoritma TEA, algoritma Twofish, algoritma Serpent, algoritma Blowfish, algoritma MARS, algoritma RC6, A5, IDEA dan lain-lain.

Penelitian yang dilakukan Maya, dkk penelitian ini bertujuan untuk membangun sistem keamanan data nilai siswa menggunakan algoritma DES (Data Encryption Standard) untuk mencegah akses dan manipulasi data oleh pihak yang tidak berkepentingan. Algoritma DES merupakan algoritma cipher blok simetrik yang aman dan efisien untuk mengenkripsi dan dekripsi data. Sistem ini diharapkan dapat membantu SD Negeri 064979 Medan dalam mengamankan data nilai siswa dan meningkatkan kepercayaan pada sistem penyimpanan data [1].

Penelitian yang dilakukan Khoirunnisa dan Djuniadi mensimulasikan pengamanan rekam medis dengan AES dan hasilnya menunjukkan bahwa AES dapat menjadi rekomendasi untuk perlindungan data. Data dienkripsi menjadi bentuk yang tidak dimengerti dan hanya bisa diakses dengan dekripsi, sehingga meningkatkan keamanannya [2].

Metode TrippleDes merupakan metode penyandian yang aman untuk data pada Flash Disk. Kata kunci dienkripsi terlebih dahulu dan disimpan, kemudian didekripsi saat verifikasi. Hanya Flash Disk yang memiliki Key yang sama

DOI : 10.52771/bangkitindonesia.v13i1.278
p-ISSN: 2337-4055 **e-ISSN:** 2776-9267

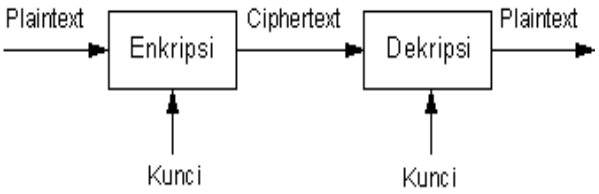
yang dapat diakses. Metode ini menggunakan algoritma DES sebanyak tiga kali dengan tiga kunci 56-bit (total 168-bit), membuatnya lebih aman daripada DES. Proses enkripsi dan dekripsi hanya dapat dilakukan dengan Flash Disk yang dikenali, meningkatkan keamanan data [3].

Menurut beberapa teori yang ada masing-masing dari algoritma simetris memiliki kelebihan dan kekurangan satu dengan yang lainnya. Oleh sebab itu, Tujuan pembuatan jurnal ini membahas kelebihan dan kekurangan antar algoritma simetris dari segi keamanan terhadap serangan sebagai referensi dalam pemilihan algoritma mana yang lebih baik dalam melakukan implementasi pada suatu sistem

II. STUDI PUSTAKA

A. *Kriptografi*

Kriptografi, berasal dari bahasa Yunani "kryptos" (tersembunyi) dan "graphein" (tulisan), merupakan ilmu yang awalnya digunakan untuk menyembunyikan pesan. Seiring perkembangannya, kriptografi menjadi ilmu yang menyelesaikan masalah keamanan seperti privasi dan otentikasi dengan teknik matematis. Kriptografi tidak hanya menyembunyikan pesan, tetapi juga memastikan integritas dan keaslian data, serta melindungi informasi dari akses yang tidak sah. [4]



Gambar 1. Proses Enkripsi dan Dekripsi

Sistem kriptografi mempunyai tiga karakteristik yaitu sebagai berikut :

1) Jenis operasi yang digunakan pada umumnya adalah substitusi dimana setiap elemen – elemen dari plaintext dipetakan ke elemen lain dan transposisi dimana unsur-unsur dalam plaintext yang disusun kembali. Persyaratan mendasar adalah bahwa tidak ada informasi yang hilang (yaitu, bahwa semua operasi yang reversibel). Kebanyakan sistem, disebut sebagai sistem produk, melibatkan beberapa tahapan substitusi dan transposisi. Operasi ini digunakan untuk mengubah plaintext ke chipertext.
2) Jumlah kunci yang akan digunakan dalam proses enkripsi dan deskripsi. Kunci yang sama digunakan oleh pengirim dan penerima, sistem ini disebut sebagai simetris, single-key, secret-key atau bisa disebut enkripsi konvensional. Pada kasus berbeda jika kunci yang digunakan berbeda pada pengirim dan penerima, sistem ini disebut sebagai asimetris, dua kunci, atau enkripsi kunci publik.
3) Cara plaintext diproses. Satu blok elemen input akan diproses oleh sebuah blok chipper yang akan menghasilkan sebuah blok output yang didapat dari setiap input. Elemen input yang diproses oleh stream cipher secara terus menerus akan menghasilka output satu elemen pada suatu waktu pada saat berjalan bersama.

B. *Enkripsi*

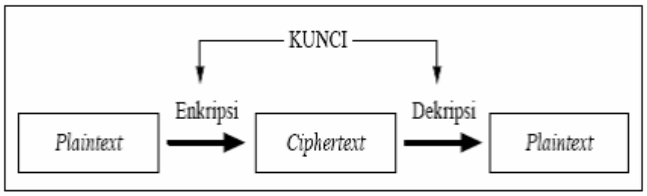
Enkripsi merupakan bagian dari kriptografi dan merupakan bagian yang sangat penting fungsi dari enkripsi adalah mengamankan data yang dikirim dapat dijaga kerahasiaannya. Enkripsi bisa dapat diartikan dengan chipper atau kode dimana plaintext akan dirubah menjadi kode-kode tersendiri sesuai metode yang telah disepakati oleh pengirim dan penerima. Enkripsi adalah metode pengamanan informasi dengan membuatnya tidak terbaca. Proses ini menggunakan dua kunci berbeda: kunci publik untuk enkripsi dan kunci privat untuk dekripsi. Kunci publik tidak sama dengan kunci privat, sehingga informasi yang dienkripsi dengan kunci publik hanya dapat didekripsi dengan kunci privat yang sesuai. Hal ini memastikan keamanan informasi dan mencegah akses yang tidak sah. [5].

C. *Dekripsi*

Dekripsi merupakan proses kebalikan dari enkripsi yaitu pembuatan kembali sandi–sandi atau informasi menggunakan kunci atau kode kebentuk file aslinya.

D. *Algoritma Simetris*

Algoritma Simetris atau sering disebut juga Algoritma Kriptografi konvensional. Kunci yang digunakan pada proses enkripsi dan dekripsinya adalah kunci yang sama.



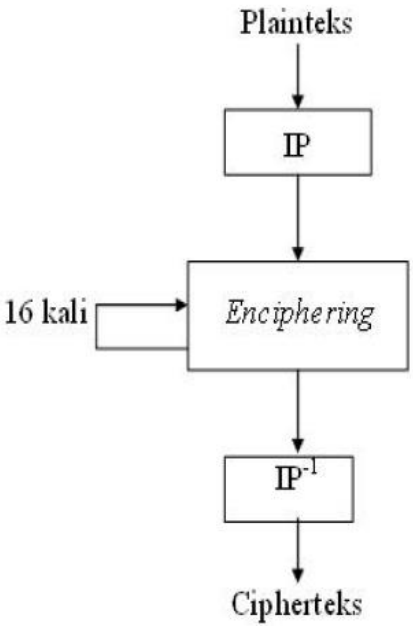
Gambar 2. Proses Enkripsi dan Dekripsi Algoritma Simetris

E. *Algoritma DES*

DES adalah algoritma kriptografi yang dikembangkan oleh IBM. DES merupakan modifikasi dari algoritma Lucifer. Lucifer merupakan algoritma yang dapat digunakan dalam satu chip yang terdiri dari 64bit untuk blok masukan dan ukurun kunci sebesar 128 bit. DES pertama kali dipublikasikan pada 17 maret 1975 oleh federal register. DES merupkan algoritma cipher block yang memiliki sebesar 64 bit dengan ukuran kunci 48 bit. Pengurangan pada bit kunci algoritma DES agar mekanisme algoritma dapat berjalan pada satu chip. Pada 15 januari 1977 DES diadopsi sebagai standar algoritma yang digunakan oleh NBS. Algoritma DES kemudian banyak digunakan didunia terutama dalam

DOI : 10.52771/bangkitindonesia.v13i1.278
p-ISSN: 2337-4055 **e-ISSN:** 2776-9267

melindungi data informasi yang tersebar di dunia sehingga tidak bisa dibaca orang lain.

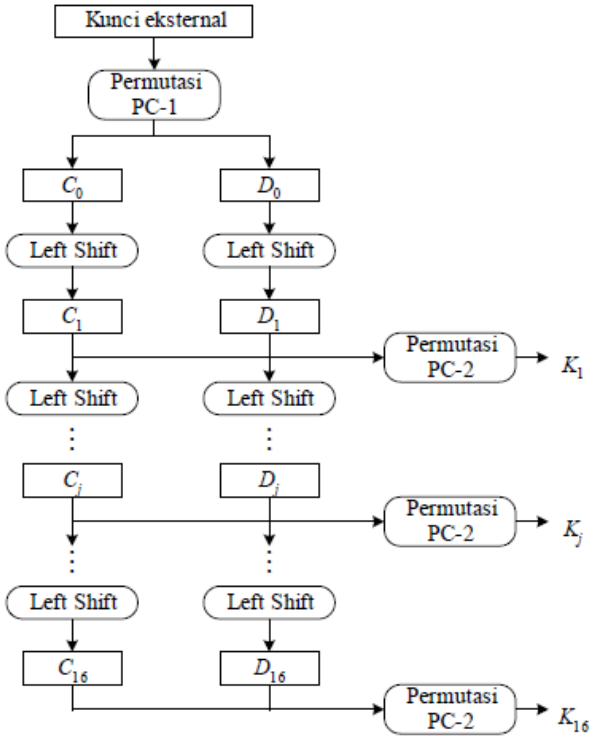


Gambar 3. Skema Global Algoritma DES

Pada tahapan awal algoritma DES perlu adanya pembentukan kunci internal untuk membantu dalam proses algoritma DES tersebut. Kunci internal didapatkan dengan beberapa proses yang dilakukan pada kunci eksternal. Tahapan yang dilakukan untuk proses pembentukan kunci internal disebut dengan key schedule.

Proses Key schedule dilakukan dengan beberapa tahapan yaitu sebagai berikut :

1) Masukkan nilai kunci eksternal ke dalam tabel PC-1
2) Nilai dari hasil proses PC-1 dibagi menjadi 2 bagian yang sama yaitu bagian kiri (C0) dan bagian kanan (D0).
3) Masing-masing bagian yaitu bagian kiri (C0) dan bagian kanan (D0) di geser ke kanan sesuai tabel pergeseran bit tiap putaran. Proses ini disebut dengan left shift. Left shift dilakukan sebanyak 16 kali putaran.
4) Hasil dari setiap putaran dari proses left shift dimasukkan kedalam tabel permutasi PC-2 sehingga membentuk kunci internal. Kunci internal yang didapatkan sejumlah 16 sebab hasil dari proses left shift sebanyak 16 yang dimana selanjutnya diubah kedalam tabel permutasi PC-2.



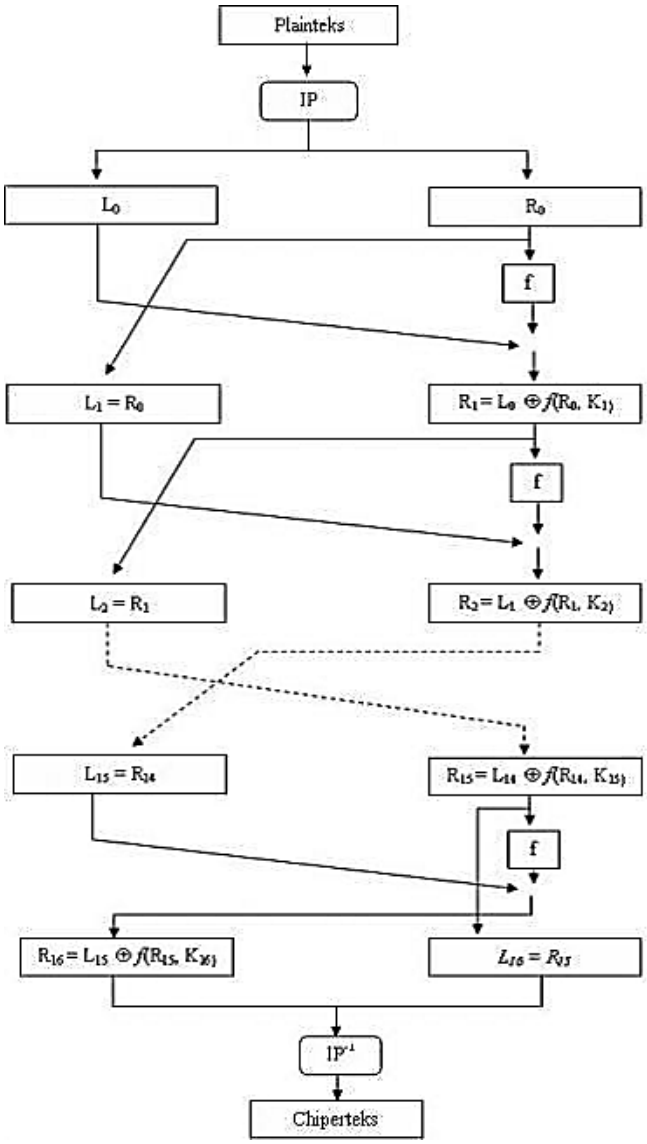
Gambar 4. Proses Key Schedule

Tahapan berikutnya adalah tahap pembentukan algoritma DES. Proses yang dilakukan dengan algoritma DES yaitu mengubah plainteks menjadi cipherteks (teknik enkripsi/enciphering) dan mengubah cipherteks menjadi plainteks (teknik dekripsi/deciphering).

Berikut adalah tahapan pembentukan cipherteks menjadi plainteks dengan algoritma DES:

1) Masukkan nilai plainteks ke dalam tabel IP
2) Nilai yang didapatkan didalam tabel IP dibagi menjadi 2 bagian dengan jumlah yang sama yaitu bagian kanan (L0) dan bagian kiri (R0).
3) proses dengan fungsi f pada bagian kanan (R0). Fungsi F digunakan untuk mengXORkan R0 dengan kunci eksternal. Kunci eksternal yang digunakan disesuaikan dengan jumlah putaran yang sedang dilakukan.
4) Hasil dari proses pada fungsi f di XOR-kan dengan L0 untuk memperoleh R1 dan L1=R0.
5) Proses dari memperoleh bagian kanan dan bagian kiri dilanjutkan terus hingga 16 kali putaran (16 iterasi).
6) Pada iterasi ke-16, ubah posisi yaitu R16 pada bagian kiri dan L16 pada bagian kanan.
7) Cipherteks didapatkan dari hasil dari penyatuan 2 bagian tersebut dimasukkan kedalam tabel invers permutation.

DOI : 10.52771/bangkitindonesia.v13i1.278
p-ISSN: 2337-4055 **e-ISSN:** 2776-9267



Gambar 5. Proses Plainteks menjadi Cipherteks dengan Algoritma DES

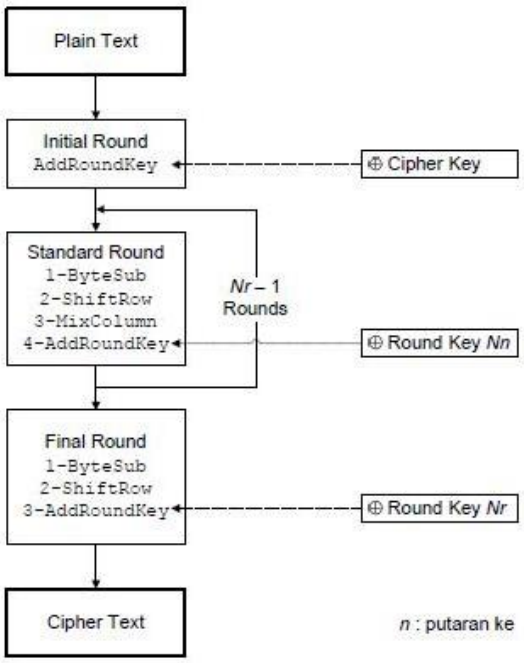
Pada proses decipher merupakan kebalikan dari proses encipher. Proses awal decipher menggunakan cipherteks yang kemudian dimasukkan ke tabel invers permutation. Selanjutnya mengikuti langkah-langkah kebalikan dari encipher dengan kunci dan iterasi dari iterasi ke-16 dan lanjut ke-15, ke-14.... hingga iterasi ke-0. Pada proses decipher left shift diubah menjadi right shift yang menggeser ke kanan jumlah bit. Tahap terakhir dari proses memasukkan iterasi ke-0 pada tabel initial permutation sehingga hasilnya berupa plainteks.

F. Algoritma AES atau Rijndael

Advanced Encryption Standard (AES) merupakan algoritma *cryptographic* yang dapat digunakan untuk mengamakan data. Blok chipertext pada algoritma AES berbentuk simetris yang dapat mengenkripsi dan dekripsi informasi. Chippertext merupakan data yang telah dirubah melalui proses enkripsi data biasanya tidak bisa dikenali. Plaintext merupakan data asli atau data yang telah melalui proses dekripsi. Algoritma

AES menggunakan kunci kriptografi 128, 192, dan 256 bits untuk mengenkripsi dan dekripsi data pada blok 128 bits. [6]

1) Pada algoritma AES plaintext diproses melalui serangkaian transformasi chiper, yang terdiri dari transformasi SubBytes, ShiftRows, MixColumns, dan AddRoundKey dengan menggunakan kunci kriptogenik rahasia yaitu cipher key.[7]
2) Chipertext yang akan dikonversikan kembali menjadi plaintext melalui transformasi InvShiftRows, InvSubBytes, AddRoundKey, dan InvMixColumns.



Gambar 6. Skema Algoritma Rijndael

Tahapan algoritma Rijndael yang beroperasi 128bit dengan kunci 128bit adalah sebagai berikut:

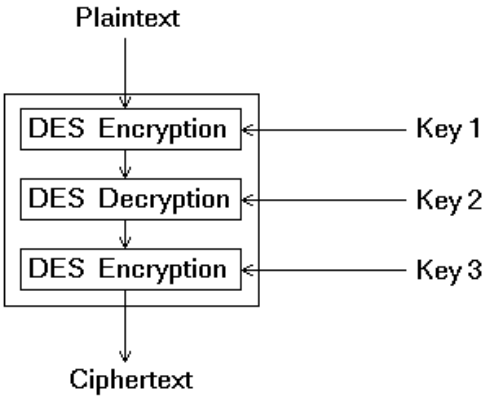
1) Pertama AddRoundKey: Proses initial round dengan men-XOR-kan antara plaintext dengan cipher key.
2) Kedua Putaran sebanyak Nr - 1x. Proses yang dilakukan setiap putaran adalah:
   a. ByteSub yaitu substitusi byte menggunakan tabel substitusi (S-Box).
   b. ShiftRows yaitu pergeseran baris-baris array state secara wrapping.
   c. MicColumn yaitu mengacak data masing-masing di kolom arrat state.
   d. AddRoundkey yaitu melakukan XOR antara state sekarang dengan round key.

DOI : 10.52771/bangkitindonesia.v13i1.278
p-ISSN: 2337-4055 **e-ISSN:** 2776-9267

3) Ketiga Final Round: Proses untuk putaran terakhir:
   a. ByteSub
   b. ShiftRow
   c. AddRoundKey

G. Algoritma 3DES

Algoritma 3DES adalah algoritma yang dikembangkan dari algoritma DES. Perbedaannya terletak pada seberapa panjang kunci yang akan digunakan pada proses enkripsi dan dekripsi. Algoritma 3DES panjang kunci yang akan digunakan lebih panjang dari DES. Pada DES digunakan satu kunci yang panjangnya 56-bit, sedangkan untuk 3DES menggunakan 3 kunci yang panjangnya 168- bit. Tiga kunci yang digunakan memiliki sifat yang saling bebas (K1 ≠ K2 ≠ K3) atau bisa juga dua buah kunci yang saling memiliki sifat saling bebas dan satu kunci lainnya sama dengan kunci pertama (K1 ≠ K2 dan K3 = K1). Pengguna algoritma 3DES dianggap lebih aman dari DES karena kunci yang digunakan lebih panjang.



Gambar 7. Skema Algoritma 3DES

Penjelasan dari Algoritma 3DES yaitu sebagai berikut:

Tahap pertama, plaintexts yang diinputkan akan dilakukan proses dekripsi menggunakan algoritma DES dengan kunci eksternal pertama (K1) sehingga menghasilkan pra-cipherteks

Tahap kedua pra-cipherteks tahap pertama dilakukan proses dekripsi dengan menggunakan kunci eksternal kedua (K2). Proses dekripsi menggunakan algoritma DES hasil dari proses ini adalah pra-cipherteks kedua.

Tahap ketiga pra-cipherteks tahap kedua dilakukan proses dekripsi dengan kunci eksternal ketiga (K3) proses dekripsi menggunakan algoritma DES hasil dari proses ini menghasilkan cipherteks (C).

Triple DES merupakan algoritma enkripsi yang menggunakan DES sebanyak tiga kali untuk meningkatkan keamanan data. Hal ini dilakukan karena ukuran kunci DES 56-bit dirasa tidak aman lagi dengan semakin canggihnya teknologi. Triple DES menjadi solusi sederhana untuk meningkatkan keamanan tanpa perlu merancang algoritma baru.

III. HASIL DAN PEMBAHASAN

Berdasarkan hasil studi literatur yang dilakukan didapatkan informasi kelebihan dan kekurangan dalam segi keamanan beberapa algoritma kriptografi simetris DES, AES, dan 3DES, yakni dengan penjelasan sebagai berikut:

A. Algoritma DES (Data Encryption Standard)

Kelebihan dibandingkan penggunaan algoritma simetris lain yaitu:

Berdasarkan waktu yang dibutuhkan untuk memecahkan algoritma kriptografi, semakin lama waktu yang dibutuhkan untuk memecahkan algoritma tersebut maka semakin baik keamanan algoritma tersebut. Sesuai hasil percobaan sebanyak 4 kali pada teks yang berbeda, algoritma DES membutuhkan waktu yang lebih lama untuk dipecahkan dibanding algoritma 3DES. Namun algoritma 3DES dibandingkan AES membutuhkan waktu yang lebih singkat untuk dipecahkan yang lebih singkat untuk dipecahkan [8].

Kekurangan dibandingkan penggunaan algoritma simetris lain yaitu:

1) Algoritma DES lebih lemah melawan serangan brute force dibandingkan algoritma 3DES [9]
2) Algoritma DES mempunyai kunci yang relatif kecil yakni 56-bit sehingga rentan terhadap serangan brute force. [10]
3) Pada tahun 1997 DES untuk pertama kalinya, dokumen yang dienkripsi menggunakan DES di crack oleh publik. Setahun kemudian, sebuah dokumen yang dienkripsi menggunakan DES di crack dalam waktu 56 jam [11]

B. Algoritma AES (Advance Encryption Standard) /Rijndael

Kelebihan dibandingkan penggunaan algoritma simetris lain yaitu:

1) Keseluruhan kunci dari AES cukup untuk untuk melindungi informasi yang ada didalamnya. Tidak ada serangan besar yang membuktikan keberhasilan melawan algoritma AES sampai saat ini.[12]
2) Berdasarkan waktu yang dibutuhkan untuk memecahkan algoritma kriptografi, semakin lama waktu yang dibutuhkan untuk memecahkan algoritma tersebut maka semakin baik keamanan algoritma tersebut. Sesuai hasil percobaan sebanyak 4 kali pada teks yang berbeda, algoritma AES membutuhkan waktu yang paling lama untuk dipecahkan dibanding algoritma DES, dan 3DES. [13]
3) Algoritma AES membuktikan kekebalan melawan serangan. Sehingga, AES merupakan pilihan yang tepat untuk berbagai aplikasi wireless standar seperti Wi-Fi, ZigBee, dan WiMax, keamanan dari smart card dan keamanan bit-stream pada FPGAs [14][15].
4) Algoritma AES paling aman digunakan melawan serangan praktis, terutama menggunakan AES 256-bits [2]

DOI : 10.52771/bangkitindonesia.v13i1.278
p-ISSN: 2337-4055 **e-ISSN:** 2776-9267

C. Algoritma 3DES

Kelebihan dibandingkan penggunaan algoritma simetris lain yaitu:

Algoritma 3DES lebih kuat melawan serangan brute force dibandingkan algoritma DES [9]

Kekurangan dibandingkan penggunaan algoritma simetris lain yaitu:

1) Berdasarkan waktu yang dibutuhkan untuk memecahkan algoritma kriptografi, semakin lama waktu yang dibutuhkan untuk memecahkan algoritma tersebut maka semakin baik keamanan algoritma tersebut. Sesuai hasil percobaan sebanyak 4 kali pada teks yang berbeda, algoritma 3DES dibandingkan AES dan DES membutuhkan waktu yang lebih singkat untuk dipecahkan [13]
2) 3DES rentan terhadap serangan meet in the middle attacks karena menggunakan 3 kunci yang berbeda dengan ukuran kunci secara keseluruhan 168 bits. [9]
3) Algoritma 3DES mempunyai ukuran block 64 bits sehingga berpengaruh terhadap potensi kekuatan keamanan. [10].

IV. KESIMPULAN

Berdasarkan studi literatur yang membandingkan algoritma DES, AES/Rijndael, dan 3DES, algoritma AES keluar sebagai juara dalam hal keamanan. Algoritma ini menawarkan perlindungan data yang lebih kuat dan tahan terhadap serangan dibandingkan dengan dua pesaingnya. Bagi para pengembang dan profesional yang membutuhkan solusi enkripsi simetris yang aman, cepat, dan efisien, algoritma AES adalah pilihan terbaik. Algoritma ini telah teruji dan terbukti handal dalam berbagai aplikasi

REFERENSI

[1] W. R. Maya, A. Azanuddin, and E. Elfitriani, “Implementasi Kriptografi Pengamanan Data Nilai Siswa Menggunakan Algoritma DES,” Jurnal SAINTIKOM (Jurnal Sains Manajemen Informatika dan Komputer), vol. 21, no. 1, 2022, doi: 10.53513/jis.v21i1.4764.

[2] O. G. Khoirunnisa and D. Djuniadi, “Implementasi Algoritma AES untuk Keamanan Data Rekam Medis,” PETIR, vol. 15, no. 1, 2021, doi: 10.33322/petir.v15i1.1333.

[3] Ndruru and T. S. Alasi, “Algoritma Tripple Des Dalam Pengamanan File Dengan Usb Flashdisk,” Jurnal Informasi Komputer Logika, vol. 2, no. 4, 2022.

[4] Stallings, Williams., 2005, Cryptography and Network Security Principles and Practices Fourth Edition., USA: Prentice Hall..

[5] Khamsyar and Muh. Basri, “Aplikasi Enkripsi Gambar Menggunakan Metode (Rivest Shamir Adleman) Rsa,” Jurnal Sintaks Logika, vol. 2, no. 3, 2022, doi: 10.31850/jsilog.v2i3.1850.

[6] Surian, Didi "Algoritma Kriptografi AES Rijndael". TESLA Vol 8 No. 2, 97-101, Oktober 2006

[7] Kurniawan, Yusuf. "Desain AES (Advanced Encryption Standard)". INFOMATEK Vol 5 No. 2, Juni 2003.

[8] Ozunu, V.C., Pirvu, C.C., Leordeanu, C., Cristea, V., "Distributed Platform for the Analysis of Cryptographic Algorithms", 10th International Conference on Complex, Intelligent, and Software Intensive Systems, 2016

[9] Bahnasawi, M.A., Ibrahim, A., Mohamed, A., dkk, "ASIC-Oriented Comparative Review of Hardware Security Algorithms for Internet of Things Applications", IEEE Information and Communication Technologies 978-1-5090-5721-4, 2016

[10] Mandal, B.K., Bhattacharyya, D., Bandyopadhyay, S.K., "Designing and Performance Analysis of a Proposed Symmetric Cryptography Algorithm", International Conference on Communication System and Network Technologies, 2013

[11] Nadeem, “A performance comparison of data encryption algorithms,” IEEE Information and Communication Technologies, pp. 84-89, 2006.

[12] Saleh, M. A., Tahir, N. M., Hisham, E., Hashim, M., "An Analysis and Comparison for Popular Video Encryption Algorithms", IEEE Information and Communication Technologies 978-1-4799-8969, 2015

[13] Abood, O.G., Elsadd, M.A., Guirguis, S.K., "Investigation of Cryptography Algorithms used for Security and Privacy Protection in Smart Grid", Nineteenth International Middle East Power System Conference (MEPCON), Menoufia University, Egypt, December 2017

[14] S. Trimberger, "Security in SRAM FPGAs", IEEE Design and Test of Computers, vol. 24, no. 6, p. 581, Nov./Dec. 2007.

[15] F. Bibiola, T. U. Kalsum, and H. Alamsyah, “Penerapan Algoritma Advance Encryption Standard (AES) Untuk Pengamanan File Pada Aplikasi Berbasis WEB,” J. Surya Energy, vol. 8, no. 1, p. 35, 2023, doi: 10.32502/jse.v8i1.6461

DOI : 10.52771/bangkitindonesia.v13i1.278
p-ISSN: 2337-4055 **e-ISSN:** 2776-9267