KETIK : Jurnal Informatika
ISSN: 3026- 183X (Media Online)
Vol. 01, No. 05, Mei 2024 Hal. 26-32
Faatuatua Media Karya
jurnal.faatuatua.com/index.php/KETIK

Perbandingan Metode*data Encryption Standard (DES)* Dan *Advanced Encryption Standard (AES)* Pada Keamanan Jaringan Komputer Di SMK Willibrodus Betun

Yunita Luruk Ulu[1*], Yampi R. Kaesmetan[2]

[1]Sekolah Tinggi Manajemeni Informatika Kupang (STIKOM Uyelindo Kupang), Indonesia, email: yuniulu09@gmail.com*
[2]Sekolah Tinggi Manajemeni Informatika Kupang (STIKOM Uyelindo Kupang), Indonesia, email: kaesmetanyampi@.gmail.com
**coressponding author)*

Info Artikel

Diajukan: *15 Mei 2024*
Diterima: *15 Mei 2024*
Diterbitkan: *30 Mei 2024*

Kata Kunci:
Advanced Encryption Standard;
Data Encryption Standard;
Keamanan;
Jaringan Komputer;
SMK Willibrodus Betun.

Keywords:
Advanced Encryption Standard;
Data Encryption Standard;
Security;
Computer Network;
SMK Willibrodus Betun.

Abstrak

Dalam era digital ini, pemenfaatan teknologi informasi telah menjadi bagian integral dari kehidupan sehari-hari, baik itu instasi pendidikan maupun disekolah-sekolah.Salah satunya di SMK Willibrodus Betun. Pertumbuhan penggunaan jaringan komputer dalam lingkungan pendidikan membuka peluang besar untuk akses informasi yang lebih cepat dan berbagai kemudahan.Tujuan keamanan jaringan komputer meliputi perlindungan informasi dari pihak yang tidak berkepentingan dengan tetap memudahkan akses dan penggunaan oleh para pengguna. Keamanan jaringan komputer kini dipandang sebagai salah satu tugas dan masalah penting yang harus diatasi untuk melindungi aset-aset dan informasi.permasalahan utama seperti akses tidak sah,dan serangan cyber lainnya. Salah satu pelindung yang dibutuhkan untuk mendapatkan akses yang aman ketika berhubungan dengan jaringan komputer, baik dari luar internet maupun dari dalam internet dengan cara membuat aturan tertentu pada DES dan AES. Salah satu cara untuk meningkatkan keamanan jaringan komputer yaitu melalui penggunaan metode enkripsi data. Seperti metode Data Encryption Standard (DES) dan AES (Advanced Encryption Standard).Tujuan utama dari penelitian ini yaitu Mengidentifikasi perbedaan keamanan antara metode Data Encryption Standard (DES) dan Advanced Encryption Standard (AES) dalam konteks jaringan komputer di SMK Willibrodus Betun. Bertujuan untuk memahami tingkat keamanan relatif dari masing-masing metode enkripsi data dan menentukan mana yang lebih cocok untuk diterapkan dalam lingkungan jaringan komputer.

Abstract

In this digital era, the use of information technology has become an integral part of everyday life, both in educational institutions and in schools. One of them is at Willibrodus Betun Vocational School. The growth in the use of computer networks in educational environments opens up great opportunities for faster access to information and various conveniences. The goal of computer network security includes protecting information from unauthorized parties while still facilitating access and use by users. Computer network security is now seen as one of the important tasks and problems that must be addressed to protect assets and information. main problems such as unauthorized access and other cyber attacks. One of the safeguards needed to gain safe access when dealing with computer networks, both from outside the internet and from inside the internet, is by making certain rules in DES and AES. One way to improve computer network security is through the use of data encryption methods. Such as Data Encryption Standard (DES) and AES (Advanced Encryption Standard) methods. The main objective of this research is to identify security differences between the Data Encryption Standard (DES) and Advanced Encryption Standard (AES) methods in the context of computer networks at Willibrodus Betun Vocational School. Aims to understand the relative level of security of each data encryption method and determine which is more suitable for application in a computer network environment.

1. PENDAHULUAN

Dalam era digital ini, pemenfaatan teknologi informasi telah menjadi bagian integral dari kehidupan sehari-hari, baik itu instasi pendidikan maupun di sekolah-sekolah.Salah satunya di SMK Willibrodus Betun. Pertumbuhan penggunaan jaringan komputer dalam lingkungan pendidikan membuka peluang besar untuk akses informasi yang lebih cepat dan berbagai kemudahan.Tujuan keamanan jaringan komputer meliputi perlindungan informasi dari pihak yang tidak berkepentingan dengan tetap memudahkan akses dan penggunaan oleh para pengguna[1][2][3][4]. Keamanan jaringan komputer merupakan proses pencegahan yang dilakukan oleh penyerang untuk terhubung ke dalam jaringan komputer melalui akses yang tidak sah, atau penggunaan secara ilegal dari komputer. Salah satu metode yang umum digunakan untuk mengamankan data dalam jaringan komputer yaitu dengan menggunakan metode Data Encryption Standard (DES) dan AES (Advanced Encryption Standard) yang telah terbukti efektif[5].

Keamanan jaringan komputer kini dipandang sebagai salah satu tugas dan masalahpenting yang harus diatasi untuk melindungi aset-aset dan informasi[6]. Keamanan jaringan komputer merupakan proses untuk mencegah dan mengidentifikasi penggunaan yang tidak sah dari jaringan komputer. Tujuan dari Keamanan jaringan komputer yaitu untuk mengantisipasi resiko pada jaringan komputer berupa bentuk ancaman fisik maupun logik baik langsung ataupun tidak langsung mengganggu aktivitas yang sedang berlangsung dalam jaringan komputer. selain itu, untuk menjaga data pada sistem komputer agar aman dari berbagai ancaman[1].

Di SMK Willibrodus Betun, muncul permasalahan utama seperti akses tidak sah,dan serangan cyber lainnya. Salah satu pelindung yang dibutuhkan untuk mendapatkan akses yang aman ketika berhubungan dengan jaringan komputer, baik dari luar internet maupun dari dalam internet dengan cara membuat aturan tertentu pada DES dan AES. Salah satu cara untuk meningkatkan keamanan jaringan komputer yaitu melalui penggunaan metode enkripsi data. Seperti *metode Data Encryption Standard* (DES) dan AES *(Advanced Encryption Standard)*[7][8].

Tujuan utama dari penelitian ini yaitu Mengidentifikasi perbedaan keamanan antara metode *Data Encryption Standard* (DES) dan *Advanced Encryption Standard* (AES) dalam konteks jaringan komputer di SMK Willibrodus Betun. Bertujuan untuk memahami tingkat keamanan relatif dari masing-masing metode enkripsi data dan menentukan mana yang lebih cocok untuk diterapkan dalam lingkungan jaringan komputer.

Berdasarkan latar belakang yang diuraikan maka peneliti tertarik untuk melakukan penelitian yang berkaitan dengan keamanan jaringan yang berjudul Perbandingan Metode *Data Encryption Standard (DES) dan Advanced Encryption Standard (AES)* Pada Keamanan Jaringan Komputer di SMK Willibrodus Betun.

2. METODE PENELITIAN

Metode penelitian yang akan digunakan dalam Tugas Akhir ini adalah Algoritma *Data Encryption Standard (DES)* dan *Advanced Data Encryption Standard* (AES) penggunaannya dalam keamanan jaringan secara umum. Metode penelitian meliputi studi literatur untuk memahami konsep dasar Algoritma DES, dan Algoritma AES, dan penerapan Algoritma DES dan AES dalam berbagai skenario[9]. Penulis juga akan melakukan evaluasi keamanan algoritma ini dan menyajikan beberapa studi kasus penggunaannya dalam lingkungan nyata. Tujuan penelitian ini yaitu menyajikan informasi komprehensif tentang Algoritma DES dan AES relevansinya dalam menjaga keamanan jaringan komputer di era digital yang kompleks dan rawan[10].

2.1. *Data Encryption Standard (DES)*

Algoritma DES merupakan algoritma enkripsi yang paling banyak digunakan di dunia yang diadopsi oleh NIST *(National Institue of Standards and Technology)* sebagai standar pengolah informasi Federal AS. DES dirancang oleh tim IBM yang dipimpin Horst Feistel dengan bantuan dari NSA *(National Security Agency)*. DES menggunakan kunci sebesar 64 bit untuk mengenkripsi blok juga sebesar 64 bit. Akan tetapi karena 8 bit dari kunci digunakan sebagai parity, kunci efektif hanya 65 bit. Dalam DES, penomoran bit adalah dari kiri kekanan dengan bit 1 menjadi *most significant bit*, untuk 64 bit, bit 1 mempunyai 263[10]. Permutasi menggunakan inintial permutation dilakukan terhadap input sebesar 64 bit. Hasil permutasi dibagi menjadi dua blok L0 dan R0, masing-masing sebesar 32 bit, dimana L0 merupakan 32 bit pertama dari hasil permutasi dan R0 merupakan 32 bit sisanya (bit 33 bit hasil permutasi menjadi bit 1 R0). Sebanyak 16 putaran enkripsi dilakukan menggunakan fungsi cipher f dan setiap putaran menggunakan kunci 48 bit yang berbeda dan dibuat berdasarkan kunci DES. Efeknya adalah setiap blok secara bergantian dienkripsi, masing-masing

sebanyak 8 kali. Pada setiap putaran, blok sebesar 32 bit dienkripsi menggunakan rumus[9] Menjelaskan secara detail langkah-langkah penelitian yang didalamnya termasuk desain penelitian, prosedur penelitian, prosedur pengujian. Penulisan sub bab dapat dilihat contoh dibawah ini.

Algoritma *encryption* ataupun *decryption* pada DES terdiri dari proses *intialpermutation round* final *permutation*. Dimana masing-masing *round* akan menggunakan *sub key* yang berbeda-beda. Proses *key schedule* dilakukan untuk menghasilkan *sub key* pada masing-masing round (Devara 2020).

2.2. *Advanced Encryption Standard(AES)*

Advanced Encryption Standard (AES) merupakan sistem penyandian blok yang bersifat non-Feistel karena AES menggunakan komponen yang selalu memiliki invers dengan panjang blok 128 bit. Kunci AES dapat memiliki panjang kunci bit 128, 192, 256 bit. Penyandian AES menggunakan proses yang berulang yang disebut dengan ronde. Jumlah ronde yang digunakan oleh AES tergantung dengan panjang kunci yang digunakan. Setiap ronde membutuhkan kunci ronde dan masukan dari Kelebihan dan Kelemahan DES ronde berikutnya. Kunci ronde dibangkitkan berdasarkan kunci yang diberikan. Relasi antara jumlah ronde dan panjang[8].

2.3. Keamanan Jaringan Komputer

Keamanan jaringan komputer merupakan salah satu aspek penting dari sebuah sistem informasi Keamanan Sering kali masalah keamanan berada diurutan kedua atau bahkan urutan terakhir dalam daftar hal-hal yang dianggap penting[6]. Keamanan jaringan juga dapat diartikan sebagai proses untuk mengidentifikasi dan mencegah adanya *user* yang tidak mempunyai izin penyusup dari sistem jaringan komputer. Tujuan dibangunnya suatu sistem keamanan jaringan adalah untuk menanggulangi dan mencegah ancaman dari jaringan luar yang dapat berupa ancaman logik atau fisik. Ancaman logik adalah sebuah ancaman yang berupa pengambilan data secara tidak sah atau pencurian data oleh penyusup dengan cara mencari celah yang terbuka pada sistem keamanan jaringan, sedangkan ancaman fisik yaitu sebuah ancaman yang bertujuan untuk merusak sistem jaringan dari sisi *hardware* sebuah komputer[7].

3. HASIL DAN ANALISIS

Analisis data merupakan suatu proses yang melakukan hal seperti pemeriksaan, pembersihan, tranformasi, dan juga pemodelan data dengan tujuan untuk dapat menemukan informasi yang berguna dan untuk menginformasikan sebuah kesimpulan yang mendukung dalam melakukan pengambilannya.

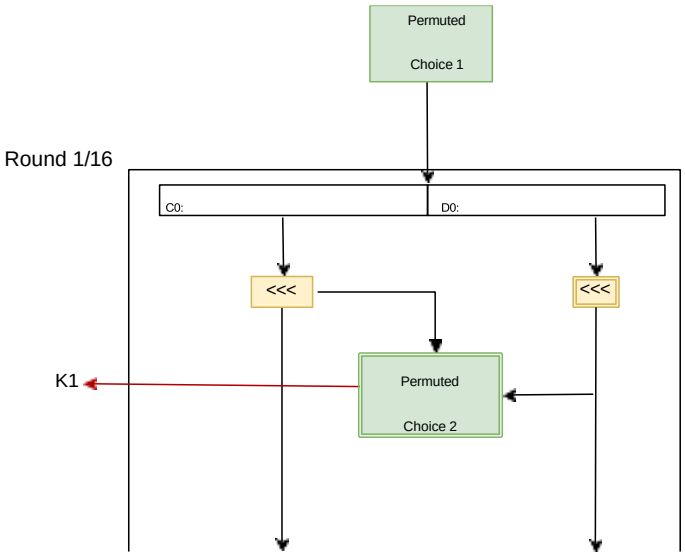
Perhitungan algoritma DES. Jika kita memiliki data yang akan *diencrypt* seperti contoh. HELOSMK (dalam bentuk *ASCII*), kita ubah ke bentuk *HEX* menjadi *plaintext*: 48, 54, 4c, 4f, 42, 55, 44, 59. Key: 11, 22, 33, 44, 55, 66, 77, 88.

a. *Key Schedule*

Pertama-tama kita akan melakukan proses *key schedule*. Kita perlu merubah *key* yang ada menjadi dalam biner:

Key: 00010001 00100010 00110011 01000100 01010101 01100110 01110111 10001000.

Key akan dimulai proses *permuted choice* 1 (PC-1-) *Cyclic Shift. PermutedChoice* 2 (PC-2) untuk mendapatkan *sub key* pada setiap *round*.



Gambar 1. Proses Key Schedule

b. Selanjutnya kita akan memberikan *index* dari masing-masing *key* yang ada seperti berikut.

Tabel 1. *Key Index*

0	0	0	1	0	0	0	1	0	0	1	0	0	0	1	0
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
0	0	1	1	0	0	1	1	0	1	0	0	0	1	0	0
17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32
0	1	0	1	0	1	0	1	0	1	1	0	0	1	1	0
33	34	35	36	37	38	39	40	41	42	42	44	45	46	47	48
0	1	1	1	0	1	1	1	1	0	0	0	1	0	0	0
49	50	51	52	53	54	55	56	57	58	59	60	61	62	63	64

c. Setelah itu kita akan melakukan proses *permuted Choice* 1 (PC-1). Dengan menggunakan tabel referensi sebagai berikut:

Tabel 2. *Pc.1 DES Left*

57	49	41	33	25	17	9
1	58	50	42	34	26	18
10	2	59	51	43	35	27
19	11	3	60	52	44	36

Right

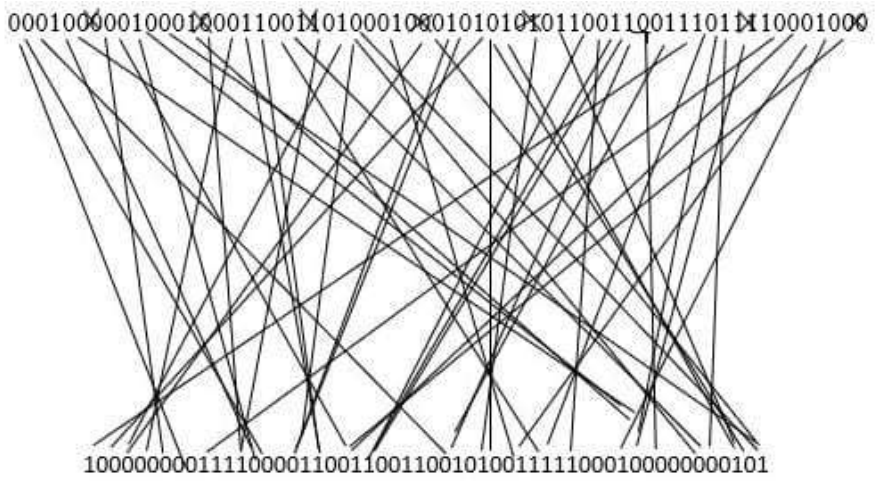
63	55	47	39	31	23	15
7	62	54	46	38	30	22
14	6	16	53	45	37	29
21	13	5	28	20	12	4

Pada PC-1 ini kita akan membagi bit-bit menjadi dua bagian: left (C0) dan *Right* (DO). Contohnya untuk baris pertama pada C0 dengan urutan 57, 49, 41, 33, 25, 17, dan 9. Disini kita akan lihat pada tabel PC-1 dengan *key index* sebelumnya.

Tabel 3. PC-1

57->1
49->0
41->0
33->0
25->0
17->0
9->0

Sehingga hasilnya seperti ini:



Gambar 2. Hasil pc-1.

Jadi disini kita tidak menggunakan LBS pada masing-masing *byte key* maka pada index (8, 16, 24, 32, 40, 48, 56, 64) nilainya tidak digunakan.

Tabel 4. Urutan Data Algoritma AES.

	Panjang Kunci	Panjang Blok	Jumlah Putaran
AES-128	4	4	10
AES-129	6	4	12
AES-256	8	4	14

Pada Tabel di atas dijelaskan mengenai tipe dari algoritma AES dengan panjang kunci, panjang blok dan jumlah putaran yang berbeda-beda. Untuk penelitian ini digunakan AES-128 bit dengan jumlah putaran enkripsi sebanyak 10 kali.

Terdapat 4 transformasi putaran pada proses enkripsi dan dekripsi.

a. *SubBytes* Berfungsi untuk menukar isi dari *byte* dengan menggunakan tabel substitusi.
b. *ShiftRows* Proses pergeseran blok per baris pada state array.

c. *MixColumn* Proses mengalikan blok data (pengacakan) di masing-masing state array dengan rumus sebagai berikut: $A(x)$ = {03}x 2 + {01}x 2 +{01}x +{02}
d. *AddRoundKey* Mengombinasikan state array dan round key dengan hubungan *XOR*.
Pada proses dekripsi algoritma AES:
a. *InvShiftRows* Melakukan pergeseran bit ke kanan pada setiap blok baris.
b. *InvSubBytes* Setiap elemen pada state dipetakan dengan tabel Inverse *Box.*
c. *InvMixColumn* Setiap kolom dalam state dikalikan dengan matriks AES.
d. *AddRoundKey* Mengombinasikan state array dan round key dengan hubungan *XOR*.
Penggambaran proses transformasi putaran dapat dilihat pada gambar diatas.

Tabel 5. Proses input bytes, state array, output bytes

Input bytes				*State array*				*output bytes*			
in0	*in4*	*in8*	*in12*	*S0,0*	*S0,1*	*S0,2*	*S0,2*	*Out0*	*Out4*	*Out8*	*Out12*
in1	*in5*	*in9*	*in13*	*S1,0*	*S1,1*	*S1,2*	*S1,3*	*Out1*	*Out5*	*Out9*	*Out13*
in2	*in6*	*In10*	*in14*	*S2,0*	*S2,1*	*S2,2*	*S2,3*	*Out2*	*Out6*	*Out10*	*Out14*
In3	*in7*	*in11*	*in15*	*S3,0*	*S3,2*	*S3,2*	*S3,3*	*Out3*	*Out7*	*Out11*	*Out15*

Dari Gambar dapat dijelaskan bahwa algoritma AES ini ada dasarnya, algoritma AES ini merupakan *array of bytes* dengan dua dimensi yang disebut dengan state. Rumus ukuran dari state adalah $NROWSxNCOLS$, dari state ini akan diproses enkripsi dan dekripsi yang hasilnya akan dimasukkan ke dalam *array of state*. Pada awal proses enkripsi data dimasukkan ke dalam input bytes yang kemudian akan di salin kedalam *array state,* pada proses ini nantinya akan dilakukan enkripsi dan dekripsi, hasil keluarannya akan ditampung dalam *output bytes.*

Pada awal proses enkripsi, input yang telah disalin ke dalam state akan mengalami transformasi *AddRoundKey.* Setelah itu state akan mengalami transformasi *SubBytes,ShiftRows, MixColumns*, dan *AddRoundKey* secara berulang-ulang sebanyak *round/putaran* (Nr). Proses ini dalam algoritma AES disebut sebagai *round function*. *Round* yang terakhir, *state* tidak diberikan *transformasi MixColumns*. Ilustrasi proses awal enkripsi dengan menggunakan algoritma AES -128 dijelaskan pada Gambar.

4. KESIMPULAN

Dalam menjaga keamanan jaringan komputer di SMK Willibrodus Betun, pemilihan metode enkripsi yang tepat menjadi krusial. Dalam studi ini, kami membandingkan metode *Data Encryption Standard* (DES) dan *Advanced Encryption Standard* (AES) untuk mengevaluasi keefektifan, keamanan, dan kinerja keduanya. Melalui analisis yang kami lakukan, kami menemukan bahwa AES memiliki keunggulan yang signifikan dibandingkan dengan DES dalam hal keamanan dan kinerja. AES menawarkan tingkat enkripsi yang lebih tinggi dan resistensi yang lebih baik terhadap serangan kriptoanalisis dibandingkan dengan DES. Selain itu, AES memiliki dukungan yang lebih luas dan dianggap sebagai standar de facto dalam enkripsi data saat ini.Kesimpulan harus ada di bagian ini, dengan Font Size 10 dan jenis huruf Arial. Tidak diperbolehkan menggunakan sub judul atau penomoran, sampaikan kesimpulan dalam paragraf dan hindari penggunaan data statistik.

REFERENSI

[1] Akbar, M., Pramana A.T., dan Fauzi A.I.M., 2021. Analisis Keamanan Jaringan Komputer Pada Sekolah Menengah Atas Negeri 04 Bandung. Jurnal Nasional Komputasi dan Teknologi Informasi.
[2] Arsalan, L. M., 2023. Keamanan Jaringan Wireless Fidelity (wifi) Terhadap Serangan *Packet Snifing* Menggunakan *Firewall Rule* (Pt Akurat Sentra Media). (Skripsi). Jakarta (ID): Teknik Informatika Fakultas Sains dan Teknologi, Universitas Islam Negeri Syarif Hidayatullah Jakarta.
[3] Bulolo, N., dan Sindar, A., 2020. Analisis dan Perancangan Keamanan Data Teks Menggunakan Algoritma Kriptografi DES (*Data Encryption Standard*).
[4] Dali, F., 2021. Sistem Keamanan Jaringan Menggunakan *Sisco AnyConnect* Dengan Metode *Network Access Manager*.
[5] Devara, K., 2020. Buku Data Encryption Standard (DES). Depok Jawa Barat Indinesia (ID): Universitas Indonesia.
[6] Dwipoyono, N. Khairil., dan Sudarsono A., 2023. Penerapan *Firewall* Pada Sistem Keamanan Jaringan Komputer di Sekolah SMK Negeri 5 Seluma. Jurnal Media Infotama.

[7] Fernandes, J., 2021. Analisis Keamanan Jaringan *Wireles* Lan di Dinas Perpustakaan dan Kearsipan Kota PekanBaru. (Skripsi). PekanBaru (ID): Teknik Informatika, Fakultas Teknik Universitas Islam Riau PekanBaru.
[8] Lukman, M. A., dan Bachtiar, Y., 2018. Analisis Sistem Pengelolaan Pemeliharaan dan Keamanan Jaringan Internet Pada IT Telkom Purwokerto. Jurnal Evalusi.
[9] Munir, R., 2021. Kriptografi Data Encryption Standard(DES). (Skripsi). Bandung (ID): Departemen Teknik Informatika, Institut Teknologi Bandung**.**
[10] Nasution, A. B., Efendi, S., dan Suwilo, S,. 2018. Algoritma Triple Data Encryption Standard 3DES dan Bit Terkecil yang Dimodifikasi (MLSB). Jurnal Fisika.