Journal of Science and Social Research ISSN 2615 – 4307 (Print)
Feb 2024, VII (1): 301 – 306 ISSN 2615 – 3262 (Online)
Available online at http://jurnal.goretanpena.com/index.php/JSSR

PENGAMANAN DATA TEKS MENGGUNAKAN METODE DIGITAL SIGNATURE ALGORITHM (DSA) DAN ADVANCED ENCRYPTION STANDARD (AES)

Mhd Reza Alfani[1], Mhd Furqan[2], Yusuf Ramadhan Nasution[3]
Universitas Islam Negeri Sumatera Utara, Medan
e-mail: [1]dragflast@gmail.com

Abstract: *The issue of data security and confidentiality are two important aspects of an information system. This is closely related to how important the information is sent and received by interested people. Cryptography is a field of science that aims to maintain the confidentiality of messages from unauthorized parties. The cryptographic algorithm that will be used is the Digital Signature Algorithm (DSA) asymmetric cryptography algorithm and combined with the Advanced Encryption Standard (AES) symmetric algorithm. DSA as authentication using a hash function cannot perform encryption and decryption, with a combination of Advanced Encryption Standard (AES) cryptography to enable encryption and decryption. Advanced Encryption Standard (AES) is a block cipher algorithm and has a symmetrical nature that uses a symmetric key during the encryption and decryption process. The text file type to be used is in the format (*.xlsx). Files that have been encrypted still use the same extension as the previous file but cannot be opened. Encrypted files have a size change of 30%. The decrypted file is exactly the same as the initial file before the encryption process is carried out.*

Keywords: *cryptography, digital signature algorithm, advanced encryption standard, text data*

Abstrak: Masalah keamanan dan kerahasiaan data merupakan dua aspek penting dalam sistem informasi. Hal ini erat kaitannya dengan pentingnya informasi yang dikirimkan dan diterima oleh masyarakat yang berkepentingan. Kriptografi merupakan bidang ilmu yang menjaga kerahasiaan pesan dari pihak yang tidak berkepentingan. Algoritma kriptografi yang akan digunakan adalah algoritma kriptografi asimetris Digital Signature Algorithm (DSA) dan dikombinasikan dengan algoritma simetris Advanced Encryption Standard (AES). DSA sebagai autentikasi menggunakan fungsi hash tidak dapat melakukan enkripsi dan dekripsi, dengan kombinasi kriptografi Advanced Encryption Standard (AES) agar dapat melakukan enkripsi dan dekripsi. Advanced Encryption Standard (AES) merupakan algoritma enkripsi blok dan memiliki sifat simetris yang menggunakan kunci simetris selama enkripsi dan dekripsi. Jenis file teks yang akan digunakan berformat (*.xlsx). File yang telah dienkripsi masih memakai ekstensi seperti file sebelumnya namun tidak dapat dibuka. File hasil enkripsi memiliki perubahan ukuran sebesar 30%. File hasil dekripsi sama persis seperti file awal sebelum dilakukan proses enkripsi.

Kata kunci: kriptografi, digital signature algorithm, advanced encryption standard, data teks

PENDAHULUAN

Pertukaran data sudah menjadi suatu hal yang sering dilakukan. Pertukaran data bisa dilakukan dimana saja dan kapan saja. Karena mudahnya hal pertukaran data maka rawannya masalah pemalsuan data. Masalah keamanan dan kerahasiaan data merupakan dua aspek penting dalam

sistem informasi. Hal ini erat kaitannya dengan pentingnya informasi yang dikirimkan dan diterima oleh masyarakat yang berkepentingan. Informasi akan tidak berguna lagi apabila di tengah jalan informasi itu disadap atau dibajak oleh orang yang tidak berhak. Perlunya suatu sistem yang mampu untuk mengatasi masalah pemalsuan data agar data yang kira kirim aman untuk keasliannya.

Sungguh syari'at Islam telah mengumpulkan seluruh jenis kebaikan; Islam menjaga syari'at dan tuntunan, melindungi dan memelihara akal-akal manusia, mensucikan harta benda, memberi keamanan kepada jiwa-jiwa manusia, dan menebarkan segala bentuk keselamatan, ketenangan, rahmat dan kesejahteraan. Rasulullâh shollallâhu 'alaihi wa 'alâ âlihi wa sallam bersabda,

مَنْ أَصْبَحَ مِنْكُمْ آمِنًا فِيْ سِرْبِهِ مُعَافًى فِيْ جَسَدِهِ عِنْدَهُ قُوتُ يَوْمِهِ فَكَأَنَّمَا حِيْزَ تْ لَهُ الدُّنْيَا

Artinya: "Barangsiapa di antara kalian mendapatkan rasa aman di rumahnya (pada diri, keluarga dan masyarakatnya), diberikan kesehatan badan, dan memiliki makanan pokok pada hari itu di rumahnya, maka seakan-akan dunia telah terkumpul pada dirinya." (HR. Tirmidzi no. 2346, Ibnu Majah no. 4141)

Ada beberapa cara untuk meningkatkan keamanan pada data salah satunya adalah kriptografi. Kriptografi merupakan bidang ilmu yang menjaga kerahasiaan pesan dari pihak yang tidak berkepentingan. Terdapat berbagai algoritma enkripsi yang dapat digunakan, bergantung pada karakteristik kuncinya. Algoritma dapat diklasifikasikan menjadi dua kategori berbeda: algoritma simetris, yang hanya bergantung pada satu kunci rahasia, dan algoritma asimetris (kadang-kadang disebut sebagai algoritma kunci publik), yang memanfaatkan kombinasi kunci publik dan kunci rahasia.

Algoritma kriptografi yang digunakan dalam penelitian ini adalah teknik Digital Signature (DSA) yang merupakan teknik kriptografi asimetris dan Advanced Encryption Standard (AES) yang merupakan algoritma simetris. Algoritma Tanda Tangan Digital (DSA) adalah algoritma kriptografi yang digunakan untuk memverifikasi keab sahan identifikasi pengirim dalam pesan atau identitas penanda tangan dalam dokumen digital. Tanda tangan memiliki tujuan ganda dalam menjaga integritas informasi dan mencegah penolakan oleh pihak terkait. Penggunaan tanda tangan digital menjamin integritas pesan atau dokumen digital yang dikirimkan, memastikan bahwa isinya tetap tidak berubah selama transit hingga diterima oleh penerima yang dituju.

Algoritma DSA memerlukan penggunaan fungsi hash, yaitu fungsi matematika yang mengubah string masukan dengan panjang sembarang menjadi string keluaran dengan panjang yang telah ditentukan. Hasil konversi pesan akan dibandingkan dengan hasil dekripsi prosedur kriptografi DSA, yang berfungsi untuk mengautentikasi dan memastikan integritas dan keaslian pesan. DSA sebagai autentikasi menggunakan fungsi hash tidak dapat melakukan enkripsi dan dekripsi, dengan kombinasi kriptografi Advanced Encryption Standard (AES) agar dapat melakukan enkripsi dan dekripsi.

Advanced Encryption Standard (AES) adalah teknik blok cypher yang menunjukkan fitur simetris, kunci simetris digunakan untuk proses enkripsi dan dekripsi. Institut Standar dan Teknologi Nasional (NIST) menciptakan Advanced Encryption Standard (AES) pada tahun 2001 sebagai standar algoritma kriptografi kontemporer, yang dimaksudkan untuk menggantikan algoritma Data Encryption Standard (DES) yang kuno. Algoritma AES merupakan teknik kriptografi yang digunakan untuk tujuan enkripsi dan dekripsi data, memanfaatkan panjang kunci 128 bit, 192 bit, dan 256 bit.

Pada sekolah SMA Swasta Dharma Utama pada sistem pengiriman hasil nilai ujian siswa yang diberikan oleh pengajar kepada pihak sekolah belum ada sistem pengamanannya atau masih rentan terhadap pemalsuan data. Maka perlunya membangun sistem keamanan untuk menghindari pemalsuan data tersebut.

Jenis file teks yang akan digunakan berformat (*.xlsx).

Dari penelitian sebelumnya yang dilakukan Arpan dan Nova Mayasari melakukan penelitian yang berjudul Membangkitkan Digital Signature dengan Algoritma MD5 dan Algoritma RSA untuk Memastikan Keaslian File. Pada penelitian masih menggunakan fungsi hash MD5 yang sudah cukup rentan dalam pengamanannya, karena sudah banyak cara untuk membuka dekripsi dari hasil hash MD5 tersebut. Disini penulis akan menggunakan Algoritma DSA yang akan dikombinasikan dengan Algoritma AES.

METODE

Metode Penelitian

Untuk memperoleh informasi yang relevan, bukti-bukti yang menguatkan dan landasan teoritis untuk tujuan merum uskan proposal tesis ini, sangat penting untuk menggunakan metodologi pengum pulan data yang tepat. Strategi pengum pulan data yang digunakan dalam peneli tian ini diuraikan di bawah ini:

Penelitian Kepustakaan

Dalam penelitian keputusan ini penulis melakukan dengan cara mencari Jurnal dan Ebook untuk mempelajari dan menambah wawasan serta mengumpulkan referensi dasar teori yang diambil dari berbagai artikel dan jurnal pada internet yang dibutuhkan dalam penelitian.

Studi Literatur

Studi Pustaka (Literatur) merupa kan serangkaian yang berkenaan metode pengumpulan daftar pustaka, membaca dan mencatat, serta mengolah bahan penelitian atau menemukan referensi terkait kasus atau isu yang berkaitan dengan tugas akhir. Tujuannya untuk memberikan ide-ide untuk pengembangan kerangka konseptual pada metode penelitian berdasarkan tinjauan pustaka.

Observasi

Pengamatan (Observasi) merupa kan salah satu teknik pengumpulan data yang efektif untuk mempelajari suatu sistem. Hal ini dilakukan dengan pengamatan secara langsung terhadap proses pengamanan yang dilakukan menggunakan metode DSA dan Kompresi Huffman.

Algoritma Digital Signature Algorithm (DSA)

Algoritma kriptografi yang biasa disebut sebagai Digital Signature Algor ithm (DSA) digunakan untuk menghasil kan dan memverifikasi tanda tangan digital. Algoritma DSA merupakan meto de kriptografi yang memanfaatkan enkripsi kunci publik. Algoritma DSA, bersama dengan AES, Blowfish, DES, IDEA, RC4, dan algoritma kriptografi lainnya, telah dipelajari dan didokumen tasikan secara ekstensif.

DSA (Digital Signature Algorithm) adalah metode kriptografi yang termasuk dalam kategori kriptografi kunci publik. Biasanya digunakan untuk tujuan otentikasi, perlindungan data, dan mekanisme anti penyangkalan. Penggun aan sistem kriptografi DSA tidak diguna kan untuk enkripsi. Algoritma Tanda Tangan Digital (DSA) adalah algoritma kriptografi yang dirancang dan distanda risasi untuk tujuan menghasilkan dan memverifikasi tanda tangan digital. Pembuatan kunci dalam sistem kriptografi DSA memerlukan pemanfaatan program perangkat lunak khusus. Namun, kekhawatiran besar yang muncul dalam konteks ini berkaitan dengan tingkat kepercayaan pengguna terhadap program tersebut. Parameter yang digunakan terdiri dari parameter kunci publik dinamis dan kunci privat, dimana nilai berbeda diberikan pada setiap fase produksi tanda tangan digital. DSA memiliki dua tujuan utama:

1. Pembentukan tanda-tangan (signatu re generation), dan
2. Pemeriksaan keabsahan tanda-tangan (signature verification).

Digital Signature Algorithm (DSA) menggunakan fungsi hash Secure Hash Algorithm (SHA) untuk tujuan mengubah komunikasi menjadi intisari pesan dengan panjang 160 bit. Algoritma tanda tangan digital, termasuk DSA, mencakup tiga langkah utama, yaitu:

1. Pembangkitan pasangan kunci (Key Pair Generation)
2. Pembangkitan tanda-tangan digital (Digital Signature Generation)
3. Verifikasi tanda-tangan digital (Digital Signature Verification)

Parameter DSA

DSA dikembangkan dari algoritma ElGamal. DSA mempunyai properti berupa parameter sebagai berikut.

1. p, adalah bilangan prima dengan panjang L bit, yang dalam hal ini $512 \leq L \leq 1024$ dan L harus kelipatan 64. Parameter p bersifat publik dan dapat digunakan bersama oleh orang di dalam kelompok.
2. q, bilangan prima 160 bit, merupakan faktor dari p – 1. Dengan kata lain, (p – 1) mod q = 0. Parameter q bersifat publik.
3. g = h(p-1)/q mod p, yang dalam hal ini h < p – 1 sedemikian sehingga h(p-1) / q mod p > 1. Parameter g bersifat publik.
4. x, adalah bilangan bulat kurang dari q. Parameter x adalah kunci privat.
5. y = gx mod p , adalah kunci publik.
6. m, pesan yang akan diberi tanda-tangan.

Algoritma Advanced Encryption Standard (AES)

Algoritma Advanced Encryption Standard (AES) adalah suatu algoritma block chiper dan mempunyai sifat simetri yang menggunakan kunci simetri pada waktu proses enkripsi dan dekripsi. Pada tahun 2001, AES digunakan sebagai standar algoritma kriptografi terbaru yang dipublikasikan oleh NIST (National Institute of Standard and Technology) sebagai pengganti algoritma DES (Data Encryption Standard) yang sudah berakhir masa penggunaannya.

Algoritma Advanced Encryption Standard (AES) tidak hanya digunakan untuk keamanan tetapi juga untuk tujuan kecepatan tinggi. Ini algoritma adalah standar enkripsi yang direkomendasikan oleh NIST (Lembaga Standar dan Teknologi Nasional) untuk menggantikan DES. Mengenkripsi blok data 128 bit dalam 10, 12 dan 14 putaran tergantung pada ukuran kuncinya. Dapat diimpleme ntasikan pada berbagai platform terutama di perangkat kecil dan sudah hati-hati diuji untuk banyak aplikasi keamanan.

Algoritma AES adalah algoritma kriptografi yang dapat mengenkripsi dan mendekripsi data dengan panjang kunci yang bervariasi, yaitu 128 bit, 192 bit, dan 256 bit. Perbedaan dari ketiga urutan tersebut adalah panjang kunci yang mempengaruhi jumlah round (perputaran) yang dapat digambarkan dalam bentuk tabel :

Tabel 1 Urutan Data Algoritma AES

Bit Panjang Kunci	Panjang Blok	Jumlah Putaran	
AES-128	4	4	10
AES-192	6	4	12
AES-256	8	4	14

Pada Tabel 1 dijelaskan mengenai tipe dari algoritma AES dengan panjang kunci, panjang blok dan jumlah putaran yang berbeda-beda. Algoritma AES menggunakan empat proses penting dalam pengolahan pengamanan data, operasi utama dari algoritma enkripsi yang terdri dari 4 transformasi dari algoritma AES yaitu: SubBytes, ShiftR ows, MixColumns dan AddRoundKey..

HASIL DAN PEMBAHASAN

Tampilan Halaman *Login*

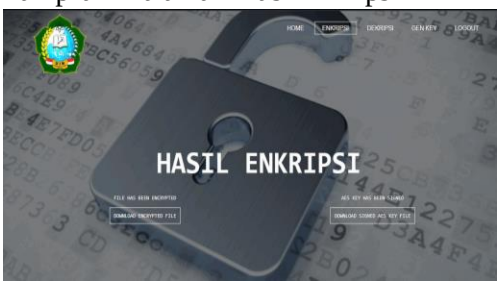
Pada halaman *login* terdapat kolom *username* dan *password*, yang dimana pengguna harus memasukan *username* dan *password* yang telah dimiliki sebelumnya. Pengguna dapat *login* sebagai admin dengan memasukan *username* = admin dan *password* admin. Tampilan halamannya sebagai berikut:

Journal of Science and Social Research ISSN 2615 – 4307 (Print)
Feb 2024, VII (1): 301 – 306 ISSN 2615 – 3262 (Online)
Available online at http://jurnal.goretanpena.com/index.php/JSSR

Tampilan Halaman Hasil Generate Key

Gambar 4 Halaman Hasil *Generate Key*

Tampilan Halaman Hasil Enkripsi



Gambar 6 Halaman Hasil Enkripsi

Tampilan Halaman Hasil Dekripsi

Gambar 8 Halaman Hasil Dekripsi

SIMPULAN

Pengkombinasian algoritma AES dan DSA menggunakan dua kali proses enkripsi dan dekripsi yang mengasilkan data dengan aman, file yang telah dienkripsi masih memakai ekstensi seperti file sebelumnya namun tidak dapat dibuka, file hasil enkripsi memiliki perubahan ukuran sebesar 30% dan file hasil dekripsi sama persis seperti file awal sebelum dilakukan proses enkripsi.

DAFTAR PUSTAKA

R. Oddang and I. Islamiyah, "Implementasi Algoritma Kriptografi Kunci Publik Menggunakan Metode RSA Pada Teks File Dengan Algoritma The Sieve Of Erathothenes Untuk Membangkitkan Bilangan Prima," *d'ComPutarE J. Ilm. Inf. Technol.*, vol. 4, no. 2, pp. 70–79, 2019.

Y. W. Arum, "EFEKTIVITAS PROGRAM BUMDES BRAYAN MULYA UNTUK MEWUJUDKAN KEMANDIRIAN DESA (Studi Kasus Desa Glempang Kecamatan Pekuncen)." UIN Prof. KH Saifuddin Zuhri, 2022.

K. B. Ziliwu, A. Maslan, and H. Kremer, "IMPLEMENTASI CAESAR CIPHER PADA ALGORITMA KRIPTOGRAFI KLASIK DALAM PENYANDIAN PESAN," *Comput. Sci. Ind. Eng.*, vol. 7, no. 2, pp. 117–126, 2022.

S. Ardi and M. Kom, *ANDROID & KRIPTOGRAFI ALGORITMARIVEST CODE 6: REKAYASAPERANGKAT LUNAK SMS (SHORT MESSAGES SERVICE)*, vol. 1. CV. Sentosa Deli Mandiri, 2020.

O. Y. Naibaho, N. B. Nugroho, and N. Y. L. Gaol, "Penerapan Digital Signature Menggunakan Metode DSA Untuk Verifikasi Surat Keterangan Keaslian Ijazah Di SMA RK Swasta Lubuk Pakam," *J. Cyber Tech*, vol. 4, no. 5, 2021.

A. H. Barkatullah, *Hukum Transaksi Elektronik di Indonesia: sebagai pedoman dalam menghadapi era digital Bisnis e-commerce di Indonesia*. Nusamedia, 2019.

A. Aristo Jansen Sinlae, "Analisis Kriptosistem Menggunakan Digital Signature Berbasis Algoritma SHA-512 dan RSA." Magister Sistem Informasi Program Pascasarjana FTI-UKSW, 2012.

S. P. Ananda and S. Lukman, "Analisa Metode Kriptografi Modern Advance

Encryption Standard (AES) 128 Bit dalam Mengenkripsi dan Mendekripsi File Dokumen Digital: Array," *J. Ilm. KOMPUTASI*, vol. 21, no. 3, pp. 333–344, 2022.

M. Azhari, D. I. Mulyana, F. J. Perwitosari, and F. Ali, "Implementasi Pengamanan Data pada Dokumen Menggunakan Algoritma Kriptografi Advanced Encryption Standard (AES)," *J. Pendidik. Sains dan Komput.*, vol. 2, no. 01, pp. 163–171, 2022.

B. K. Hutasuhut, S. Efendi, and Z. Situmorang, "Digital Signature untuk Menjaga Keaslian Data dengan Algoritma MD5 dan Algoritma RSA," *InfoTekJar (Jurnal Nas. Inform. dan Teknol. Jaringan)*, vol. 3, no. 2, pp. 164–169, 2019.

M. Fadhli, S. T. Muttaqin, S. T. Janner Simarmata, and M. Kom, *Panduan Belajar Manajemen Referensi dengan Mendeley*. Yayasan Kita Menulis, 2020.

C. Casro, Y. Purwati, G. Setyaningsih, and A. P. Kuncoro, "Rancang Bangun Aplikasi Pengaduan Pelanggan Berbasis Web Menggunakan Framework Codeigniter Di Indotechno Purwokerto," *J. Sains dan Inform.*, vol. 6, no. 2, pp. 166–174, 2020, doi: 10.34128/jsi.v6i2.244.

I. Irwanto, "Perancangan Sistem Informasi Sekolah Kejuruan dengan Menggunakan Metode Waterfall (Studi Kasus SMK PGRI 1 Kota Serang-Banten)," *Lect. J. Pendidik.*, vol. 12, no. 1, pp. 86–107, 2021, doi: 10.31849/lectura.v12i1.6093.

A. Saepulrohman and T. P. Negara, "Implementasi algoritma tanda tangan digital berbasis kriptografi kurva eliptik Diffie-Hellman," *Komputasi J. Ilm. Ilmu Komput. dan Mat.*, vol. 18, no. 1, pp. 22–28, 2021.

S. Ramadani, D. Diana, and S. Sauda, "Penerapan Algoritma AES dan DSA Menggunakan Hybrid Cryptosystem untuk Keamanan Data," *JURIKOM (Jurnal Ris. Komputer)*, vol. 7, no. 4, pp. 523–529, 2020.

B. E. Widodo and A. S. Purnomo, "Implementasi Advanced Encryption Standard Pada Enkripsi Dan Dekripsi Dokumen Rahasia Ditintelkam Polda Diy," *J. Tek. Inform.*, vol. 1, no. 2, pp. 69–77, 2020.

R. Munir and D. Heri Kurniawan, "Double Chaining Algorithm," International Conference On Advanced Informatics, 2016.

A. Prameshwari and N. P. Sastra, "Implementasi Algoritma Advanced Encryption Standard (AES) 128 Untuk Enkripsi dan Dekripsi File Dokumen," *Eksplora Inform.*, vol. 8, no. 1, p. 52, 2018, doi: 10.30864/eksplora.v8i1.139.