Biner : Jurnal Ilmu Komputer , Teknik dan Multimedia
Volume 3, No. 3 Agustus 2025
ISSN 2828-2442 (media online)
Hal 275-287

Penerapan Kriptografi Dalam Keamanan Data Pada Layanan Cloud Computing

Muhamad Rosdiana, Erdi Sutriyatna

[12]Teknik Informatika, Ilmu Komputer, Universitas Pamulang
dosen02354@unpam.ac.id, dosen02352@unpam.ac.id

Abstrak- *Cloud computing telah menjadi solusi populer untuk penyimpanan dan pengelolaan data secara efisien tanpa membangun infrastruktur fisik sendiri. Meski demikian, keamanan data menjadi salah satu perhatian utama bagi para pengguna layanan ini. Data yang disimpan di server cloud rentan terhadap serangan siber, pencurian data, serta pelanggaran privasi, terutama karena akses jarak jauh melalui internet. Kriptografi merupakan salah satu pendekatan yang paling efektif untuk mengatasi masalah ini. Tujuan yaitu untuk mengidentifikasi dan mengevalusasi kekuatan dan kelemahan dari masing-masing algoritma kriptografi dalam perlindungan data di lingkungan cloud yang dinamis. Metode yang digunakan dalam penelitian ini mencakup eksplorasi berbagai algoritma kriptografi seperti AES (Advanced Encryption Standard), RSA (Rivest-Shamir-Adleman), dan ECC (Elliptic Curve Cryptography). Hasil penelitian menunjukkan bahwa penerapan algoritma kriptografi modern, seperti AES dan ECC, dapat secara signifikan meningkatkan tingkat keamanan data di cloud computing. AES, sebagai standar enkripsi simetris, menawarkan keamanan yang tinggi dengan kecepatan enkripsi yang relatif cepat. Di sisi lain, RSA dan ECC, sebagai enkripsi asimetris, memberikan keuntungan dalam hal otentikasi dan pengelolaan kunci yang lebih aman, meskipun memerlukan waktu pemrosesan yang lebih lama dibandingkan AES. Selain manfaat keamanan, penelitian ini juga mengidentifikasi sejumlah tantangan, termasuk peningkatan kebutuhan akan sumber daya komputasi dan potensi penurunan kinerja ketika enkripsi diterapkan secara luas. Penggunaan kriptografi juga membutuhkan pengelolaan kunci yang efektif untuk mencegah masalah seperti kehilangan kunci atau penyalahgunaan kunci. Namun, ada tantangan dalam hal performa dan efisiensi yang perlu diatasi agar kriptografi dapat diimplementasikan secara lebih luas dan efektif dalam layanan cloud computing.*

Kata Kunci: *Kriptografi, keamanan data, cloud computing, enkripsi, deskripsi;*

Abstract — Cloud computing has become a popular solution for efficient data storage and management without the need to build dedicated physical infrastructure. However, data security remains one of the main concerns for users of this service. Data stored on cloud servers is vulnerable to cyberattacks, data theft, and privacy breaches, particularly due to remote access over the internet. Cryptography is one of the most effective approaches to address these issues. The objective of this study is to identify and evaluate the strengths and weaknesses of various cryptographic algorithms in protecting data within a dynamic cloud environment. The methods employed in this research include an exploration of several cryptographic algorithms such as AES (Advanced Encryption Standard), RSA (Rivest–Shamir–Adleman), and ECC (Elliptic Curve Cryptography). The results indicate that the implementation of modern cryptographic algorithms, such as AES and ECC, can significantly enhance data security in cloud computing. AES, as a symmetric encryption standard, provides a high level of security with relatively fast encryption speed. Meanwhile, RSA and ECC, as asymmetric encryption techniques, offer advantages in authentication and more secure key management, although they require longer processing times compared to AES. In addition to security benefits, this study also identifies several challenges, including increased demand for computational resources and potential performance degradation when encryption is widely applied. The use of cryptography also requires effective key management to prevent issues such as key loss or misuse. Nevertheless, challenges in performance and efficiency must be addressed for cryptography to be more broadly and effectively implemented in cloud computing services.

Keywords: Cryptography, data security, cloud computing, encryption, decryption

1. PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi telah membawa perubahan signifikan dalam berbagai aspek kehidupan, termasuk dalam hal penyimpanan, pengolahan, dan distribusi data. Salah satu inovasi teknologi yang telah menjadi sorotan utama dalam beberapa tahun terakhir adalah cloud computing. Layanan cloud computing memungkinkan pengguna untuk menyimpan data secara virtual

Biner : Jurnal Ilmu Komputer , Teknik dan Multimedia
Volume 3, No. 3 Agustus 2025
ISSN 2828-2442 (media online)
Hal 275-287

di internet, mengurangi ketergantungan pada infrastruktur fisik yang mahal dan sulit dikelola. Dengan cloud computing, pengguna dapat mengakses data kapan saja dan di mana saja selama terhubung dengan internet, sehingga teknologi ini semakin diminati oleh perusahaan, institusi pendidikan, bahkan individu.

Namun, di balik kemudahan dan efisiensi yang ditawarkan oleh cloud computing, terdapat tantangan besar terkait dengan keamanan data. Data yang disimpan dalam layanan cloud seringkali mencakup informasi sensitif seperti data pribadi, informasi bisnis, dan dokumen rahasia. Ketika data tersebut diunggah ke server yang dikelola oleh pihak ketiga, risiko kebocoran data, peretasan, dan penyalahgunaan informasi meningkat. Berbagai insiden kebocoran data yang melibatkan perusahaan besar telah menciptakan kekhawatiran tentang sejauh mana keamanan data yang disimpan di cloud dapat terjamin.

Penerapan teknologi keamanan yang tepat menjadi sangat penting untuk melindungi data dari ancaman yang ada. Salah satu solusi yang paling efektif dan banyak digunakan dalam mengatasi masalah keamanan data adalah kriptografi. Kriptografi merupakan teknik yang digunakan untuk mengamankan informasi melalui proses enkripsi, di mana data asli diubah menjadi bentuk yang tidak dapat dibaca oleh pihak yang tidak memiliki otorisasi. Dengan adanya enkripsi, meskipun data diakses oleh pihak yang tidak sah atau tidak diizinkan, informasi di dalamnya tetap tidak dapat dibaca atau dimanfaatkan.

Penerapan kriptografi dalam layanan cloud computing menjadi solusi utama dalam menjawab kebutuhan akan keamanan data. Kriptografi memungkinkan pengguna untuk melindungi data mereka dari ancaman internal maupun eksternal. Berbagai algoritma kriptografi seperti Advanced Encryption Standard (AES), Rivest-Shamir-Adleman (RSA), dan Elliptic Curve Cryptography (ECC) telah digunakan untuk mengamankan data di layanan cloud. Meskipun demikian, setiap algoritma memiliki kelebihan dan kelemahan masing-masing, sehingga penelitian mengenai penerapan kriptografi dalam keamanan data pada cloud computing menjadi sangat relevan untuk menjawab tantangan ini.

Penelitian yang dilakukan oleh D. Sari dan R. Wijaya dengan judul "Penggunaan Kriptografi Asimetris untuk Keamanan Data dalam Layanan Cloud: Studi Kasus pada Implementasi RSA dan ECC" pada tahun 2022 mengeksplorasi penggunaan kriptografi asimetris dalam melindungi data di cloud computing, dengan fokus pada implementasi algoritma RSA (Rivest-Shamir-Adleman) dan ECC (Elliptic Curve Cryptography). Masalah yang dihadapi adalah bagaimana memilih dan menerapkan algoritma kriptografi asimetris yang memberikan keseimbangan antara keamanan dan efisiensi dalam konteks cloud. Metode yang digunakan melibatkan evaluasi kedua algoritma dalam skenario nyata dengan mempertimbangkan aspek seperti kecepatan, kekuatan enkripsi, dan penggunaan sumber daya. Tujuan penelitian ini adalah untuk menentukan algoritma asimetris yang lebih cocok untuk aplikasi cloud computing. Hasil penelitian menunjukkan bahwa ECC menawarkan tingkat keamanan yang setara dengan RSA namun dengan ukuran kunci yang lebih kecil, membuatnya lebih efisien dalam penggunaan sumber daya. RSA, meskipun lebih mapan, membutuhkan ukuran kunci yang lebih besar untuk mencapai tingkat keamanan yang sama dengan ECC.

2. METODOLOGI PENELITIAN

2.1 Pendekatan

Dalam Penelitian ini menggunakan pendekatan kuantitatif deskriptif, yang bertujuan untuk menggambarkan dan menganalisis sejauh mana algoritma kriptografi dapat diterapkan dalam meningkatkan keamanan data pada layanan cloud computing. Penelitian ini dilaksanakan di SMKN 8 Kabupaten Tangerang sebagai studi kasus nyata, mengingat sekolah ini mulai menerapkan layanan cloud untuk menyimpan dokumen penting seperti data nilai siswa, surat menyurat, dan arsip administrasi. Penelitian ini bertujuan untuk menguji efektivitas dan efisiensi dari tiga algoritma kriptografi, yakni AES (Advanced Encryption Standard), RSA (Rivest-Shamir-Adleman), dan ECC (Elliptic Curve Cryptography).

Biner : Jurnal Ilmu Komputer , Teknik dan Multimedia
Volume 3, No. 3 Agustus 2025
ISSN 2828-2442 (media online)
Hal 275-287

Jenis penelitian ini tergolong sebagai penelitian terapan (applied research) karena secara langsung mengimplementasikan dan menguji teknologi keamanan informasi di lingkungan nyata. Penelitian ini juga mengandung unsur eksperimen, karena terdapat proses pengujian algoritma kriptografi secara langsung terhadap data digital milik institusi. Dengan demikian, pendekatan yang digunakan bersifat kombinatif antara penerapan teknologi dan analisis kinerja, untuk menjawab permasalahan keamanan data yang berpotensi terjadi dalam penggunaan cloud computing.

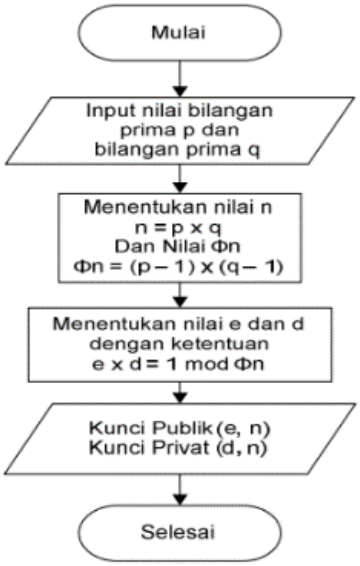
Dalam proses implementasi, algoritma AES menunjukkan kinerja yang sangat baik dalam hal kecepatan enkripsi dan dekripsi. AES bekerja secara simetris, artinya menggunakan satu kunci yang sama untuk proses enkripsi dan dekripsi, sehingga sangat efisien untuk pengamanan data dalam jumlah besar seperti dokumen nilai siswa atau file PDF. AES cocok digunakan dalam sistem cloud sekolah karena mampu menjaga integritas dan kerahasiaan data dengan kecepatan tinggi dan kompleksitas rendah dalam pengelolaan kunci.

Sebaliknya, algoritma RSA yang merupakan kriptografi asimetris membutuhkan dua kunci berbeda (publik dan privat), dan proses enkripsinya cenderung lebih lambat dibanding AES. RSA lebih cocok digunakan untuk pengamanan pertukaran kunci atau transmisi data penting berukuran kecil, seperti login sistem atau komunikasi antar server. Dalam penelitian ini, RSA membutuhkan waktu lebih lama dalam proses enkripsi file besar, namun memberikan keunggulan dalam aspek pertukaran kunci yang lebih aman dibanding AES.

Sementara itu, ECC (Elliptic Curve Cryptography) menawarkan alternatif kriptografi asimetris yang lebih efisien dari RSA dalam hal panjang kunci dan kecepatan. Dalam pengujian, ECC mampu memberikan tingkat keamanan yang sama dengan RSA namun dengan ukuran kunci yang jauh lebih kecil. Hal ini berdampak positif terhadap penggunaan bandwidth dan efisiensi penyimpanan di cloud. Di SMKN 8 Kabupaten Tangerang, penggunaan ECC menunjukkan potensi besar untuk diadopsi karena mampu menjaga performa sistem sambil tetap menjamin keamanan data. Hasil perbandingan menunjukkan bahwa untuk pengamanan file besar secara cepat, AES lebih unggul, sementara untuk keamanan transfer data dan efisiensi kunci, ECC menjadi pilihan terbaik.

2.2 Algoritma Rivest-Shamir-Adleman (RSA)

2.1.1 Proses Pembangkitan Kunci



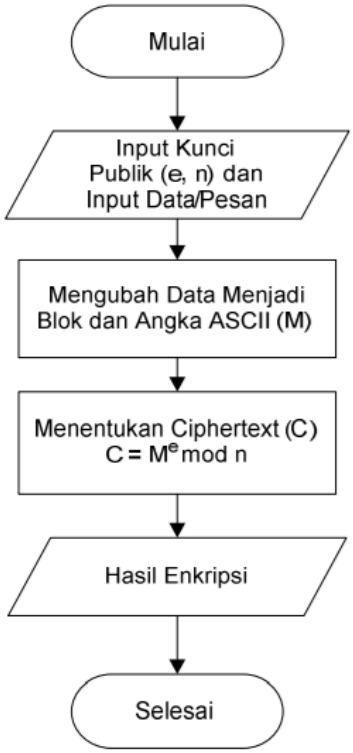
Biner : Jurnal Ilmu Komputer , Teknik dan Multimedia
Volume 3, No. 3 Agustus 2025
ISSN 2828-2442 (media online)
Hal 275-287

Gambar 2.1. Flowchart Algoritma RSA

2.1.2 Proses Enkripsi

Proses enkripsi dengan algoritma RSA dilakukan dengan menghitung exponen plaintext dalam operasi modulo n (modulo = sisa pembagian) untuk setiap blok pesan atau data sehingga dapat menghasilkan ciphertext. Eksponen yang digunakan adalah public exponent e. Operasi ini bisa dituliskan dengan persamaan berikut :

$C=M^e \bmod n$
C = ciphertext
M = pesan (plaintext)
e = public exponent
n = modulus



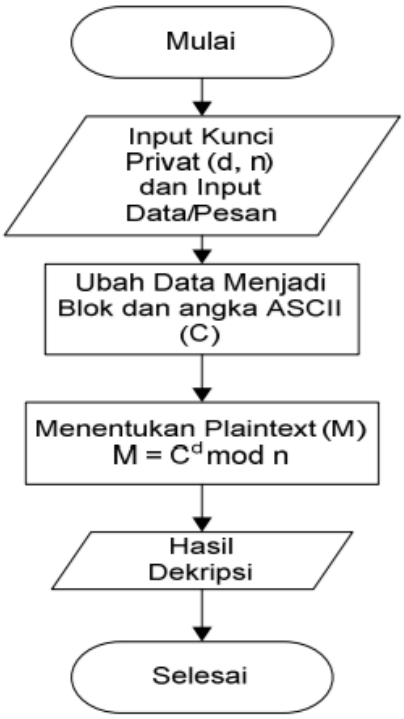
Gambar 2.2. Flowcart proses enkripsi

2.1.3 Proses Deskripsi

Sedangkan pada proses deskripsi, yang dilakukan hampir sama dengan enkripsi tapi eksponen yang digunakan adalah private exponent d untuk mengembalikan pesan seperti semula. Operasi ini bisa dituliskan dengan persamaan berikut :

$C=M^d \bmod n$
C = ciphertext
d = private exponent
n = modulus
M = pesan (plaintext)

Biner : Jurnal Ilmu Komputer , Teknik dan Multimedia
Volume 3, No. 3 Agustus 2025
ISSN 2828-2442 (media online)
Hal 275-287



Gambar 2.3. Proses deskripsi

2.2 Algoritma AES (Advance Encryption Standard)

2.2.1 Proses Pembangkitan Kunci

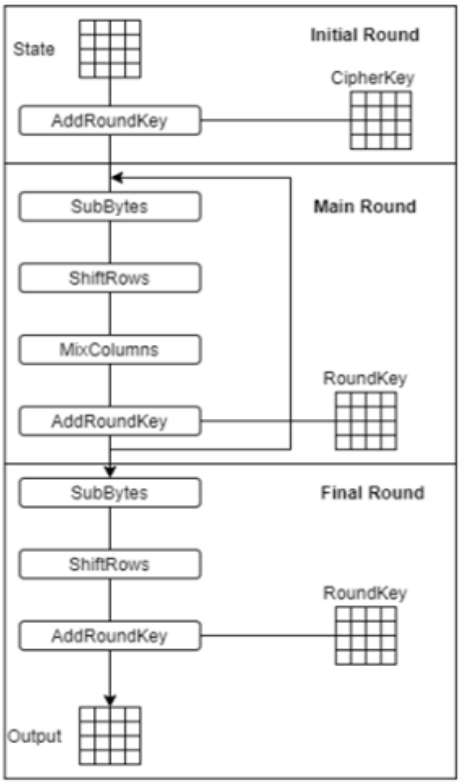
Sebelum proses enkripsi dimulai, AES melakukan pembangkitan kunci turunan yang disebut sebagai round keys. Round key ini berasal dari kunci utama (master key) yang dimasukkan oleh pengguna, dan dihasilkan melalui proses yang disebut key expansion. Jumlah round key yang dihasilkan tergantung pada panjang kunci yang digunakan. Sebagai contoh, AES-128 menghasilkan 11 round key (1 round key awal + 10 round key untuk setiap putaran enkripsi).

Proses key expansion dilakukan dengan cara mengambil blok kunci utama dan mengaplikasikan sejumlah operasi transformasi pada blok tersebut, termasuk rotasi byte (rotword), substitusi byte menggunakan S-box (subword), dan penambahan konstanta (Rcon). Hasil dari proses ini adalah kunci turunan yang memiliki ukuran lebih besar daripada kunci utama, dan akan digunakan pada setiap tahap (round) enkripsi untuk memberikan variasi transformasi yang unik pada data.

2.2.2 Proses Enkripsi

Proses enkripsi AES terdiri dari serangkaian transformasi terhadap blok data 128-bit yang disebut sebagai state. Proses ini diawali dengan tahap AddRoundKey, di mana blok data di-XOR-kan dengan round key awal. Transformasi ini menyatukan kunci ke dalam data dan menjadi fondasi keamanan dari seluruh proses.

Biner : Jurnal Ilmu Komputer , Teknik dan Multimedia
Volume 3, No. 3 Agustus 2025
ISSN 2828-2442 (media online)
Hal 275-287



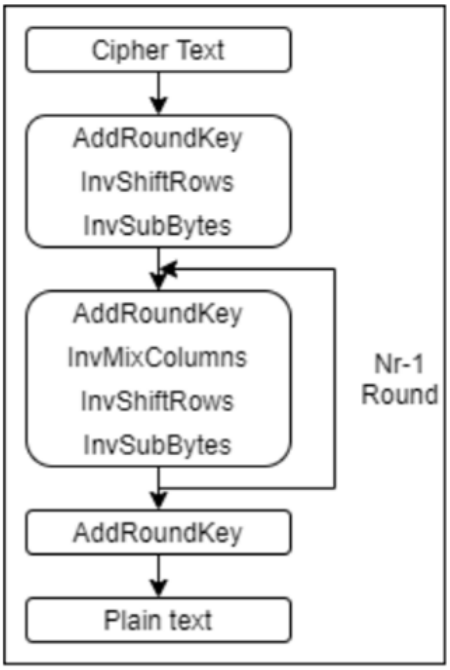
Gambar 2.4. Proses Enkripsi

2.2.3 Proses Deskripsi

Proses dekripsi dalam AES merupakan kebalikan dari proses enkripsi. Tujuannya adalah untuk mengembalikan ciphertext menjadi plaintext asli menggunakan kunci yang sama (karena AES adalah algoritma simetris). Dekripsi juga dilakukan dalam blok 128-bit dan menggunakan round key yang sama namun dalam urutan terbalik.

Langkah pertama dalam dekripsi adalah menerapkan AddRoundKey pada ciphertext menggunakan round key terakhir. Setelah itu, proses memasuki tahapan inverse dari setiap transformasi yang dilakukan saat enkripsi. Tahapan ini mencakup InverseShiftRows, InverseSubBytes, InverseMixColumns, dan AddRoundKey.

Biner : Jurnal Ilmu Komputer , Teknik dan Multimedia
Volume 3, No. 3 Agustus 2025
ISSN 2828-2442 (media online)
Hal 275-287



Gambar 2.9. Proses Deskripsi AES

2.3 Algoritma ECC (Elliptic Curve Cryptography)

2.3.1 Perhitungan Operasi Matematika ECC

Persamaan matematika dari kurva eliptik pada bidang prima Fp yang digunakan pada Elliptic Curve Cryptography adalah sebagai berikut:

$x^3 + ax + b \bmod p$, dimana $4a^3 + 27b^2 \bmod p \neq 0$

Pada elemen bidang berhingga menggunakan bilangan bulat antara 0 dan p – 1. Aritmatika modular pada semua operasi seperti penambahan, pengurangan, pembagian, dan perkalian melibatkan bilangan bulat antara 0 dan p – 1. Bilangan prima p ditentukan dengan nilai tertentu, sehingga ada sebagian besar titik pada kurva eliptik memberikan sistem kriptografi yang aman. Elliptic Curve Cryptography memiliki tiga operasi utama yaitu penjumlahan titik, penggandaan titik, dan perkalian titik (Ridhoi, 2023)

2.3.2 Proses Enkripsi dan Deskripsi ECC

Pada logaritma diskrit dari kurva eliptik (ECC), diberikan P dan Q yang merupakan dua buah titik di kurva eliptik, carilah integer k sedemikian sehingga Q = kP. Secara komputasi sulit untuk menemukan k, jika k adalah bilangan yang besar. Bilangan k merupakan logaritma diskrit dari Q dengan basis P. Pada ECC, Q adalah kunci publik, k adalah kunci privat, dan P adalah sembarang titik pada kurva eliptik. Dalam kriptografi kunci asimetris, harus ditentukan terlebih dahulu nilai parameter yang akan digunakan dan telah disepakati oleh pihak yang akan berkomunikasi. Parameter yang digunakan dalam ECC yaitu nilai a dan b, bilangan prima p dalam persamaan kurva eliptik bidang terbatas serta titik generator G yang dipilih dari kurva eliptik. Pendekatan enkripsi dan dekripsi dengan ECC ini dapat dijelaskan dalam contoh kasus misalnya A ingin mengirimkan pesan ke B:

1. Pembangkitan Kunci Privat dan Kunci Publik

B membangkitkan kunci privat nB dengan cara memilih bilangan acak yang nilainya diantara $[1, p - 1]$. Dengan kunci privat tersebut, B membangkitkan kunci publik $PB = nB \,.\, G$.

Biner : Jurnal Ilmu Komputer , Teknik dan Multimedia
Volume 3, No. 3 Agustus 2025
ISSN 2828-2442 (media online)
Hal 275-287

2. Enkripsi

Misalnya pesan yang akan dikirim adalah pesan m. A mengencode pesan m menjadi integer nilai ASCII. Lalu memilih bilangan acak k yang nilai diantara [1, $p - 1$], kemudian dinyatakan x = (m.k) + 1, lalu sulihkan x kedalam persamaan kurva eliptik hingga mendapatkan nilai y, sehingga didapatkan pesan (Pm) telah menjadi titik (x,y). Terakhir, A menghasilkan cipherteks (Cm), yang terdiri dari pasangan titik Cm = $\{(kG), (Pm + kPB)\}$ dimana G adalah titik generator dan PB adalah kunci publik B.

3. Dekripsi

Untuk melakukan dekripsi cipherteks Cm, B awalnya mengalikan titik pertama dari cipherteks dengan kunci privatnya nB dan kemudian mengurangkan titik kedua dari cipherteks dengan hasil perkalian tersebut. $Pm + kPB\ nB(kG) = Pm + k(nBG)\ nB(kG) = Pm$ Terakhir decode Pm (m = (x-1/n)) menjadi pesan m semula.

3. HASIL DAN PEMBAHASAN

3.1 Hasil

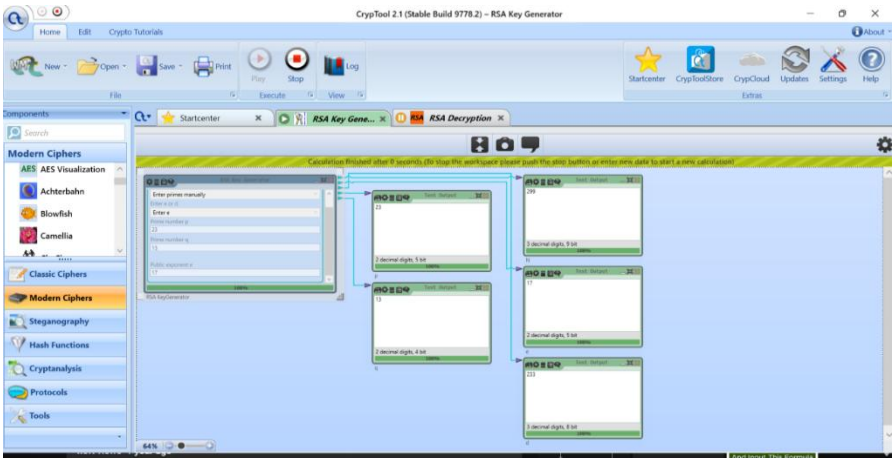
Hasil Penelitian ini dilakukan di SMKN 8 Kabupaten Tangerang sebagai bagian dari upaya meningkatkan keamanan data pada layanan berbasis cloud yang digunakan sekolah, seperti penyimpanan nilai siswa, dokumen guru, dan data administrasi lainnya. Penelitian dilakukan dengan pendekatan simulasi langsung menggunakan aplikasi CrypTool 2, yang memungkinkan analisis visual terhadap proses enkripsi dan dekripsi menggunakan tiga algoritma: AES, RSA, dan ECC.

Data yang digunakan untuk simulasi berupa file teks dan gambar yang merepresentasikan file laporan nilai, data pribadi siswa, dan dokumen penting lainnya. Tujuan utamanya adalah menguji efektivitas, efisiensi, dan tingkat keamanan dari ketiga algoritma tersebut dalam penggunaan di lingkungan sekolah.

Berikut adalah hasil simulasi dari ketiga algoritma yang diujikan.

a. Algoritma RSA

Di bawah ini adalah tampilan awal ketika kita akan melakukan proses simulasi dengan RSA. Proses awal yaitu dengan membangkinkan kunci dengan memasukan angka atau nilai yang akan dijadikan kunci atau key.



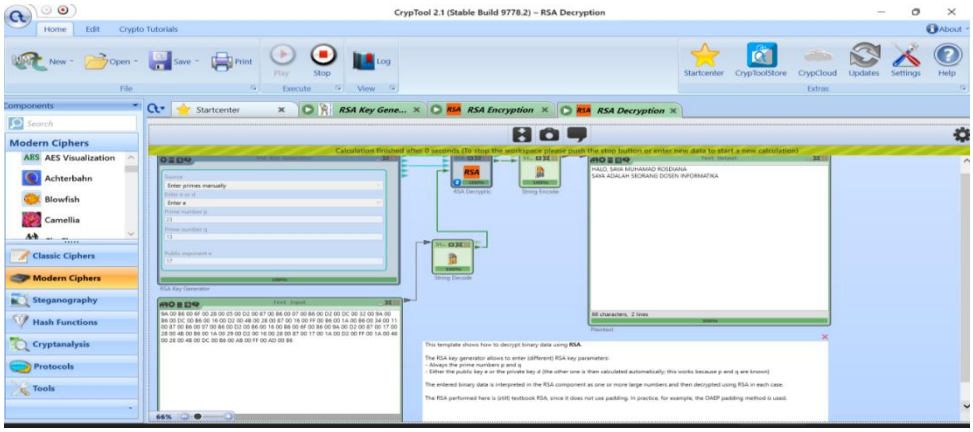
Gambar 3.1. RSA key

Pada gambar 3.2 adalah proses deskripsi yang mana dari data pembangkit kunci kita masukan plain text atau data aslinya yang diujikan adalah berupa kalimat “HALO, SAYA MUHAMAD ROSDIANA

Biner : Jurnal Ilmu Komputer , Teknik dan Multimedia
Volume 3, No. 3 Agustus 2025
ISSN 2828-2442 (media online)
Hal 275-287

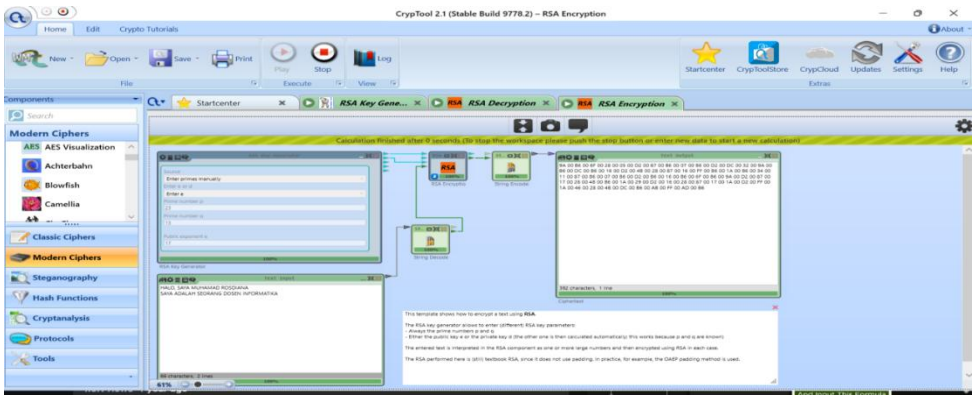
SAYA ADALAH SEORANG DOSEN INFORMATIKA”

Kalimat tersebut kemudian diproses dengan mengklik tombol play yang ada dibagian atas, kemudian menghasilkan kode-kode bilangan heksa seperti erlihat di gambar.



Gambar 3.2. RSA Deskripsi

Pada gambar 3.3 yaitu adalah proses enkripsi yang mana kita memasukan kode-kdoe hasil deskripsi yang sudah dilakukan di awal kemudian dengan menekan tombol play makan akan diproses dan menghasilkan kalimat awal yang dimasukan sebelumnya.

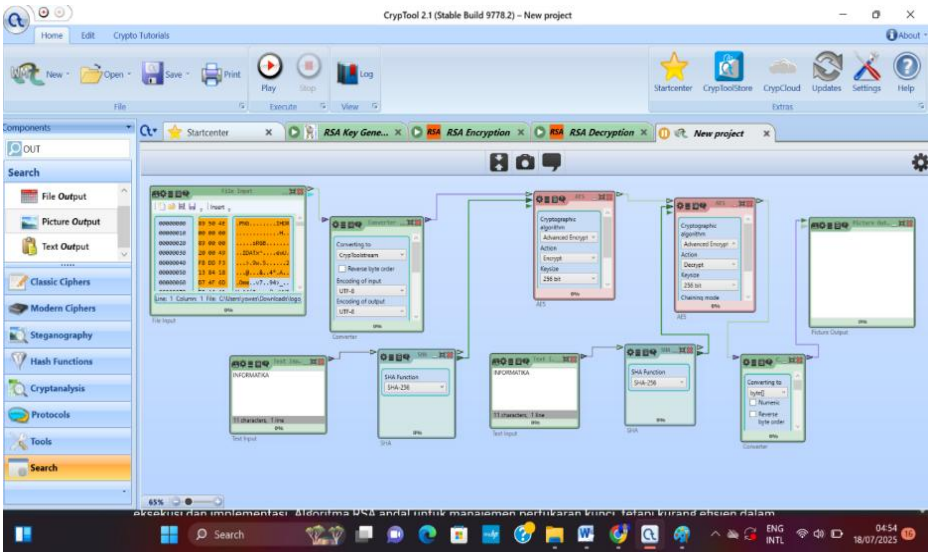


Gambar 3.3. RSA Enkripsi

b. Algoritma AES

Pada simulasi algoritma AES yaitu yang menjadi sampel adalah gambar berupa logo unpam. Pada prosesnya terlebih dahulu kita membuat key yang mana pada proses ini key nya adalah INFORMATIKA seperti yang terlihat pada gambar 3.4.

Biner : Jurnal Ilmu Komputer , Teknik dan Multimedia
Volume 3, No. 3 Agustus 2025
ISSN 2828-2442 (media online)
Hal 275-287



Gambar 3.4. Proses pembuatan Key

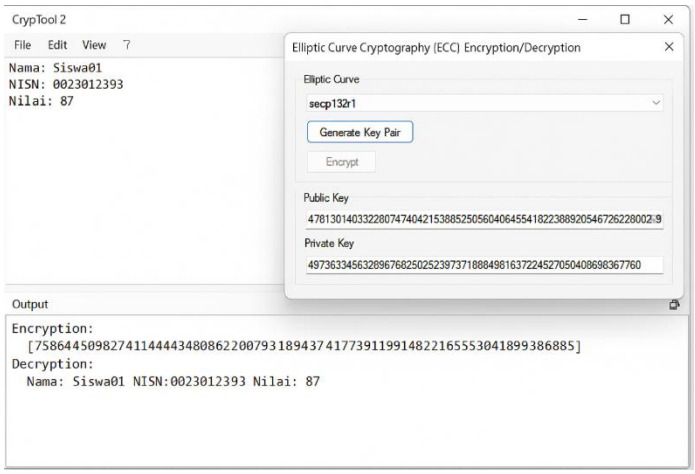
Pada gambar 3.5 terlebih dahulu kita memasukan inputannya yaitu berupa image kemudian dilakukan proses seperti yang terlihat adalah hasil dari AES yang mana setelah dibuatkan key maka kita mengklik tombol play maka pada output terlihat hasilnya adalah logo unpam.

Gambar 3.5 Algoritma AES

1. Algoritma ECC

Pada gambar 3.6 terlihat proses enkripsi dan deskripsi dari algoritma ECC yang mana data inputan ditulis terlebih dahulu kemudian diberikan private key dan public key yang dilanjutkan dengan prosesnya.

Biner : Jurnal Ilmu Komputer , Teknik dan Multimedia
Volume 3, No. 3 Agustus 2025
ISSN 2828-2442 (media online)
Hal 275-287



Gambar 3.6. Proses Algoritma ECC

3.2 Pembahasan

Penelitian ini dilakukan untuk menjawab tantangan keamanan data di lingkungan sekolah, khususnya di SMKN 8 Kabupaten Tangerang, yang saat ini mulai mengadopsi sistem digital berbasis cloud dalam pengelolaan dokumen dan informasi penting. Data-data seperti nilai siswa, data pribadi, surat keputusan, laporan keuangan, dan dokumen akademik disimpan dalam bentuk file digital dan disimpan pada sistem cloud (baik internal sekolah maupun layanan eksternal seperti Google Drive atau Microsoft OneDrive). Oleh karena itu, keamanan data menjadi isu yang sangat krusial.

Dalam hal ini, kriptografi menjadi solusi utama untuk menjaga kerahasiaan, integritas, dan autentikasi data. Penelitian ini membandingkan tiga algoritma kriptografi yang umum digunakan, yaitu AES (Advanced Encryption Standard), RSA (Rivest-Shamir-Adleman), dan ECC (Elliptic Curve Cryptography). Ketiganya diuji menggunakan simulasi melalui aplikasi CrypTool 2, untuk menilai efektivitasnya dalam melindungi file digital yang umum digunakan di sekolah.

a. AES: Cepat dan Efisien untuk Pengamanan Data Massal

Hasil simulasi menunjukkan bahwa AES merupakan algoritma yang paling cepat dan stabil ketika digunakan untuk mengenkripsi dan mendekripsi file berukuran kecil hingga besar. AES merupakan algoritma kriptografi simetris, artinya menggunakan satu kunci yang sama untuk proses enkripsi dan dekripsi.

Dalam simulasi terhadap file teks, PDF, dan gambar, AES mampu menyelesaikan proses enkripsi dan dekripsi dalam waktu yang sangat singkat, bahkan kurang dari 0.01 detik untuk file teks. Ukuran file setelah dienkripsi juga tidak mengalami perubahan signifikan, yang menunjukkan efisiensi dalam penggunaan ruang penyimpanan. Hal ini menjadikan AES sangat cocok diterapkan untuk pengamanan data masal, seperti data nilai seluruh siswa atau arsip surat-menyurat dalam jumlah besar.

Kelebihan AES juga terletak pada kesederhanaannya dalam implementasi. Sistem manajemen sekolah berbasis web/cloud dapat mengintegrasikan algoritma ini dengan mudah menggunakan berbagai pustaka kriptografi yang tersedia, seperti di PHP, Python, maupun JavaScript.

Namun demikian, AES memiliki satu kelemahan utama, yaitu karena bersifat simetris, maka kunci enkripsi harus dijaga secara ketat, sebab jika kunci diketahui pihak yang tidak berwenang, seluruh data dapat dengan mudah didekripsi.

Biner : Jurnal Ilmu Komputer , Teknik dan Multimedia
Volume 3, No. 3 Agustus 2025
ISSN 2828-2442 (media online)
Hal 275-287

b. RSA: Autentikasi dan Pengamanan Kunci

RSA adalah algoritma kriptografi asimetris, artinya menggunakan dua kunci yang berbeda: kunci publik untuk enkripsi dan kunci privat untuk dekripsi. Dalam simulasi yang dilakukan di SMKN 8 Kabupaten Tangerang, RSA menunjukkan hasil yang kurang efisien untuk mengenkripsi file berukuran sedang hingga besar. Sebagai contoh, ketika digunakan untuk mengenkripsi file PDF dan gambar JPEG, waktu proses RSA meningkat secara drastis dibandingkan AES, dan ukuran file hasil enkripsi membengkak hingga 4–5 kali lipat dari ukuran aslinya.

Meski demikian, RSA memiliki nilai lebih dalam fungsi autentikasi dan pengamanan pertukaran kunci. Dalam praktiknya, RSA tidak digunakan untuk mengenkripsi seluruh file, tetapi digunakan untuk mengenkripsi kunci AES sebelum dikirimkan melalui jaringan. Ini dikenal sebagai teknik hybrid cryptosystem, di mana RSA digunakan untuk komunikasi awal (negosiasi kunci), dan AES digunakan untuk enkripsi data selanjutnya.

Di lingkungan sekolah seperti SMKN 8, RSA dapat diimplementasikan untuk login guru dan siswa secara aman dengan sistem digital signature atau token berbasis RSA. Hal ini akan meningkatkan integritas dan keaslian komunikasi antar sistem, terutama untuk aplikasi yang memerlukan autentikasi tingkat lanjut seperti e-Raport atau e-SKP.

c. ECC: Kriptografi Modern untuk Era Mobile

ECC merupakan bentuk kriptografi asimetris yang lebih modern dan efisien dibandingkan RSA. Dalam simulasi yang dilakukan, ECC memberikan hasil yang jauh lebih cepat dari RSA, dan hampir mendekati kecepatan AES, namun tetap mempertahankan keunggulan asimetris-nya. ECC memiliki kekuatan kriptografi yang sangat tinggi, bahkan dengan ukuran kunci yang jauh lebih kecil dibanding RSA. Misalnya, kunci ECC 256-bit memiliki tingkat keamanan yang setara dengan RSA 3072-bit.

Di lingkungan sekolah, ECC sangat potensial untuk diimplementasikan dalam aplikasi mobile atau sistem dengan sumber daya terbatas, seperti perangkat tablet siswa, server lokal sekolah yang memiliki keterbatasan RAM/CPU, atau sistem IoT seperti fingerprint scanner atau access control. Selain itu, ECC juga sangat sesuai untuk penggunaan tanda tangan digital dalam dokumen PDF seperti SK, surat tugas, atau laporan.

Walau ECC memiliki kompleksitas implementasi yang lebih tinggi dibanding AES atau RSA, namun banyak pustaka modern yang telah mendukungnya, seperti OpenSSL, BouncyCastle, dan libsodium.

Hindari bagian halaman yang kosong.

4. KESIMPULAN

Pemilihan algoritma kriptografi yang tepat harus mempertimbangkan aspek keamanan, efisiensi waktu pemrosesan, dan kesesuaian dengan kebutuhan sistem. Dari perbandingan antara algoritma RSA, AES, dan ECC, AES dinilai paling cocok digunakan untuk pengamanan data dalam layanan cloud computing karena memiliki proses enkripsi dan dekripsi yang cepat dengan konsumsi sumber daya yang lebih rendah dibanding RSA dan ECC. AES sangat ideal untuk data yang besar dan sering diakses, sementara RSA dan ECC lebih cocok untuk proses otentikasi dan pertukaran kunci. Selain itu, Kriptografi dapat memberikan perlindungan data secara efektif terhadap berbagai ancaman siber seperti pencurian data, data breach, dan manipulasi informasi, dengan catatan implementasinya dilakukan secara tepat. Penggunaan kombinasi algoritma simetris dan asimetris misalnya AES untuk enkripsi data dan RSA/ECC untuk pertukaran kunci mampu menjaga efisiensi dan performa sistem. Dengan strategi implementasi yang baik, sistem cloud tetap dapat berjalan optimal tanpa mengalami penurunan signifikan dalam performa akibat proses kriptografi. Adapun tantangan utama dalam penerapan kriptografi di lingkungan cloud meliputi manajemen kunci kriptografi, yang mencakup distribusi,

penyimpanan, dan rotasi kunci secara aman. Jika tidak ditangani dengan baik, kunci dapat menjadi celah keamanan.

DAFTAR PUSTAKA

Aprilio Ardianto, Alif Aulia Harun, Bagus Dwi Saputro, Dwi Susilo, Maria Putri Arisanti, Muhammad Jundi Fadhlurohman, Rifqi Rizhansyah, Suity, & Muhamad Rosdiana. (2024). PENGENALAN KONSEP CLOUD COMPUTING BAGI SISWA SMK NEGERI 8 KAB TANGERANG. APPA : Jurnal Pengabdian Kepada Masyarakat, 1(5), 367–37.

Ardiansyah, H., & Susanto, A. (2020). "Pengamanan Data pada Cloud Computing Menggunakan Algoritma AES." Jurnal Teknologi Informasi dan Komunikasi, 12(1), 45-52.

Fadhilah, A., & Anwar, K. (2020). "Penerapan Kriptografi Berbasis AES dan DES untuk Keamanan Data di Cloud." Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer, 4(4), 255-263.

Lestari, D. A., & Arief, M. (2020). "Pengamanan Data pada Layanan Cloud Menggunakan Algoritma Kriptografi ECC." Jurnal Teknologi dan Sistem Komputer, 9(1), 44-51.

Prasetyo, E., & Mulyadi, A. (2021). "Enkripsi Data Menggunakan Algoritma AES pada Cloud Computing untuk Meningkatkan Keamanan." Jurnal Informatika dan Komputasi, 8(2), 112-121.

Pratama, M. I., & Suryadi, T. (2021). "Implementasi Kriptografi Hybrid RSA-AES pada Keamanan Data Cloud Computing." Jurnal Ilmu Komputer dan Informasi, 15(3), 88-96.

Putra, H., & Wijayanti, F. (2019). "Implementasi Kriptografi ECC untuk Keamanan Data pada Layanan Cloud." Jurnal Pengembangan Teknologi Informasi dan Komunikasi, 5(2), 212-220.

Rachman, D., & Putra, A. (2019). "Kriptografi RSA dan AES dalam Pengamanan Data pada Cloud Computing." Jurnal Teknologi Informasi dan Komputer, 7(2), 67-75.

Rinaldi, A., & Yulianto, E. (2021). "Enkripsi Data Berbasis Kriptografi pada Cloud Computing Menggunakan Algoritma ElGamal." Jurnal Informatika dan Sistem Informasi, 13(2), 79-87.

Siregar, H., & Manurung, R. (2019). "Penerapan Algoritma Kriptografi RSA untuk Keamanan Data pada Layanan Cloud Computing." Jurnal Informatika, 13(2), 115-123.

Susanto, T., & Rizki, A. (2021). "Penerapan Algoritma Kriptografi Hybrid RSA-AES dalam Pengamanan Data pada Cloud Computing." Jurnal Sistem Informasi dan Komputer, 12(3), 98-106.

Wicaksono, H., & Darmawan, F. (2019). "Keamanan Data di Layanan Cloud Computing dengan Metode Kriptografi Vigenere." Jurnal Teknologi Informasi, 14(1), 45-53.

Wijaya, R., & Nurhayati, S. (2018). "Penggunaan Algoritma Blowfish untuk Meningkatkan Keamanan Data di Cloud Computing." Jurnal Sistem Informasi, 10(1), 34-42.

Yusra, A., & Kurniawan, T. (2020). "Penerapan Algoritma Kriptografi RSA untuk Keamanan Data di Cloud Computing." Jurnal Ilmu Komputer dan Sistem Informasi, 11(2), 75-82.