LAPORAN PROYEK AKHIR

“Perancangan dan Implementasi Security Service Berbasis Kriptografi untuk Pertukaran Pesan Aman Antar Pengguna”

MATA KULIAH KEAMANAN DAN INTEGRITAS DATA

Kelompok (6) - Sains Data 2024B

Dosen Pengampu Mata Kuliah:

Hasanuddin Al-Habib, S.Si., M.Si.

Penyusun:

1.	Jeika Antama Syalom Tarigan	(24031554011)
2.	Alifiyanti Putri Nur Azizah	(24031554032)
3.	Astrid Septya Regita Pramesty	(24031554171)

FAKULTAS MATEMATIKA DAN ILMU PENGETAHUAN ALAM

UNIVERSITAS NEGERI SURABAYA

2025

BAB I
PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi informasi mendorong meningkatnya penggunaan Application Programming Interface (API) sebagai sarana pertukaran data antar sistem secara cepat dan terdistribusi. Meskipun API memberikan kemudahan integrasi dan fleksibilitas dalam komunikasi data, keterbukaannya juga menimbulkan berbagai risiko keamanan, seperti pemalsuan identitas, manipulasi data, penyadapan pesan, serta akses tidak sah terhadap layanan sistem.

Untuk mengatasi permasalahan tersebut, diperlukan mekanisme keamanan yang mampu menjamin autentikasi pengguna, integritas data, dan keaslian pesan yang dipertukarkan. Penerapan kriptografi asimetris seperti Ed25519 untuk tanda tangan digital, fungsi hash SHA-256 untuk pemeriksaan integritas, kriptografi simetris untuk menjaga kerahasiaan pesan, serta autentikasi berbasis JSON Web Token (JWT) menjadi solusi yang banyak digunakan dalam sistem keamanan modern. Oleh karena itu, proyek ini berfokus pada perancangan dan implementasi sebuah security service berbasis kriptografi sebagai pihak ketiga terpercaya (trusted authority) guna mendukung pertukaran pesan aman antar pengguna.

1.2 Tujuan

Tujuan dari pelaksanaan proyek ini adalah sebagai berikut:

1.2.1 Merancang dan mengimplementasikan layanan keamanan berbasis API untuk 1.2.2 mendukung pertukaran pesan aman antar pengguna.

1.2.2 Menerapkan algoritma kriptografi asimetris Ed25519 untuk mekanisme tanda tangan digital dan verifikasi keaslian pesan.

1.2.3 Mengimplementasikan fungsi hash SHA-256 untuk memastikan integritas data pesan dan dokumen PDF.

1.2.4 Menerapkan mekanisme autentikasi dan otorisasi menggunakan JSON Web Token (JWT) pada layanan API.

1.2.4 Mengintegrasikan kriptografi simetris (Fernet/AES) untuk menjaga kerahasiaan pesan selama proses komunikasi.

1.2.5 Melakukan pengujian sistem guna memastikan seluruh fitur keamanan berjalan sesuai dengan kebutuhan fungsional.

1.3 Manfaat

Adapun manfaat yang diharapkan dari proyek ini adalah:

1.3.1 Memberikan pemahaman praktis mengenai penerapan konsep keamanan dan integritas data dalam sistem berbasis API.

1.3.2 Menjadi contoh implementasi sederhana namun komprehensif terkait penggunaan kriptografi dalam pertukaran data digital.

1.3.3 Meningkatkan kesadaran akan pentingnya aspek keamanan seperti autentikasi, integritas, dan non-repudiation dalam sistem informasi.

1.3.4 Menjadi dasar pengembangan sistem keamanan yang lebih kompleks pada aplikasi terdistribusi di masa mendatang.

BAB II
DASAR TEORI

2.1 Kriptografi Asimetris (Ed25519)

Kriptografi asimetris merupakan metode kriptografi yang menggunakan sepasang kunci, yaitu private key dan public key. Private key bersifat rahasia dan digunakan untuk melakukan proses penandatanganan atau dekripsi, sedangkan public key bersifat terbuka dan digunakan untuk verifikasi atau enkripsi. Salah satu algoritma kriptografi asimetris yang banyak digunakan saat ini adalah Ed25519.

Ed25519 merupakan algoritma tanda tangan digital berbasis Elliptic Curve Cryptography (ECC) yang menggunakan kurva Edwards. Algoritma ini dirancang untuk memberikan tingkat keamanan yang tinggi dengan performa yang efisien serta implementasi yang relatif sederhana. Ed25519 memiliki keunggulan dalam hal kecepatan proses penandatanganan dan verifikasi, serta ketahanan terhadap berbagai serangan kriptografi dibandingkan algoritma tanda tangan digital konvensional.

Dalam sistem ini, Ed25519 digunakan untuk menghasilkan dan memverifikasi tanda tangan digital pada pesan dan dokumen PDF. Penggunaan algoritma ini memungkinkan sistem untuk menjamin keaslian pengirim dan mencegah pemalsuan data.

2.2 Hash Function (SHA-256)

Fungsi hash kriptografis adalah algoritma yang digunakan untuk mengubah data dengan ukuran arbitrer menjadi nilai hash dengan panjang tetap. Fungsi hash yang baik memiliki sifat one-way, collision resistant, dan avalanche effect, sehingga perubahan kecil pada data akan menghasilkan nilai hash yang sangat berbeda.

SHA-256 merupakan bagian dari keluarga Secure Hash Algorithm (SHA-2) yang menghasilkan output sepanjang 256 bit. Algoritma ini banyak digunakan dalam berbagai aplikasi keamanan seperti tanda tangan digital, integritas data, dan sistem blockchain. Dalam proyek ini, SHA-256 digunakan untuk melakukan pemeriksaan integritas terhadap public key yang diunggah serta untuk menghitung hash dokumen PDF sebelum dilakukan proses penandatanganan digital. Dengan menggunakan SHA-256, sistem dapat memastikan bahwa data yang diverifikasi benar-benar identik dengan data asli yang ditandatangani sebelumnya.

2.3 JSON Web Token (JWT)

JSON Web Token (JWT) merupakan standar terbuka (RFC 7519) yang digunakan untuk mengamankan pertukaran informasi antara dua pihak dalam bentuk token berbasis JSON. JWT terdiri dari tiga bagian utama, yaitu header, payload, dan signature. Signature digunakan untuk memastikan bahwa token tidak dimodifikasi oleh pihak yang tidak berwenang.

JWT banyak digunakan dalam sistem autentikasi berbasis API karena sifatnya yang stateless dan efisien. Setelah pengguna berhasil melakukan login, server akan menghasilkan

token JWT yang kemudian digunakan oleh pengguna untuk mengakses endpoint yang memerlukan autentikasi.

Dalam sistem ini, JWT digunakan sebagai mekanisme secure session, di mana setiap permintaan ke endpoint yang dilindungi harus menyertakan token yang valid. Hal ini bertujuan untuk mencegah akses tidak sah dan memastikan bahwa hanya pengguna terautentikasi yang dapat menggunakan layanan sistem.

2.4 Kriptografi Simetris (Fernet/AES)

Kriptografi simetris merupakan metode kriptografi yang menggunakan satu kunci yang sama untuk proses enkripsi dan dekripsi data. Advanced Encryption Standard (AES) adalah salah satu algoritma kriptografi simetris yang paling banyak digunakan dan telah menjadi standar internasional untuk pengamanan data.

Fernet merupakan sebuah skema enkripsi simetris tingkat tinggi yang berbasis AES-128 dalam mode CBC serta dilengkapi dengan HMAC untuk menjamin integritas data. Skema ini dirancang untuk memudahkan implementasi enkripsi tanpa harus mengelola detail teknis tingkat rendah dari algoritma kriptografi.

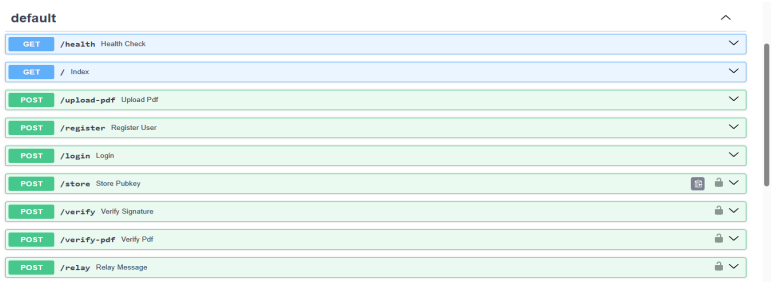
Pada proyek ini, Fernet digunakan di sisi client untuk mengenkripsi pesan sebelum dikirimkan ke server. Dengan demikian, server hanya berperan sebagai perantara (relay) tanpa mengetahui isi pesan, sehingga kerahasiaan komunikasi antar pengguna tetap terjaga.

BAB III
IMPLEMENTASI DAN PENGUJIAN SISTEM

3.1 Implementasi Server (API)

Server menyediakan beberapa endpoint utama untuk mendukung proses registrasi, autentikasi, serta pertukaran dan verifikasi data secara aman. Endpoint /register digunakan untuk melakukan registrasi pengguna baru sekaligus proses autentikasi awal, sedangkan /login berfungsi untuk memverifikasi kredensial pengguna dan menghasilkan token akses. Endpoint /store digunakan untuk menyimpan public key milik pengguna ke dalam sistem serta melakukan pemeriksaan integritas data yang dikirimkan.

Selanjutnya, endpoint /verify berfungsi untuk melakukan verifikasi tanda tangan (signature) pada pesan, sementara /verify-pdf digunakan untuk memverifikasi tanda tangan digital pada dokumen PDF guna menjamin keaslian dan keutuhan dokumen. Endpoint /relay berperan dalam meneruskan pesan terenkripsi dari satu pengguna ke pengguna lain tanpa membuka isi pesan tersebut. Keamanan sesi komunikasi dijaga menggunakan mekanisme JWT Bearer Token, di mana token ini akan diverifikasi pada setiap endpoint yang memerlukan autentikasi untuk memastikan bahwa hanya pengguna yang sah yang dapat mengakses layanan sistem.



Gambar 3.1. Endpoint utama server API

3.2 Implementasi Client

Client bertanggung jawab dalam pengelolaan proses kriptografi di sisi pengguna. Client membuat dan menyimpan pasangan private key dan public key menggunakan algoritma Ed25519 sebagai dasar mekanisme tanda tangan digital. Selain itu, client melakukan proses enkripsi dan dekripsi pesan menggunakan skema Fernet untuk menjaga kerahasiaan data selama komunikasi. Client juga berperan dalam pembuatan signature pada pesan serta melakukan proses hashing dokumen PDF sebelum ditandatangani. Selanjutnya, client menghasilkan tanda tangan digital pada dokumen PDF yang kemudian dikirimkan ke server untuk dilakukan proses verifikasi, sehingga keaslian dan integritas dokumen dapat dipastikan.

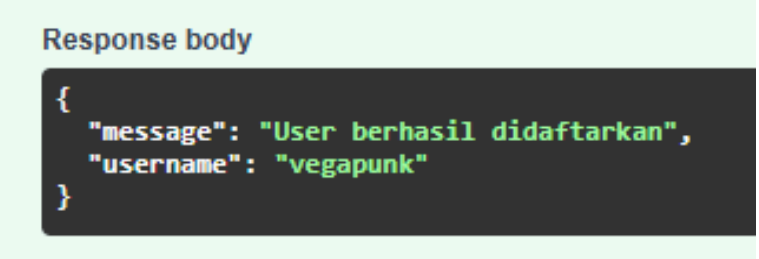
3.3 Pengujian Sistem

Pengujian sistem dilakukan untuk memastikan bahwa seluruh fitur utama pada aplikasi dapat berjalan sesuai dengan kebutuhan fungsional yang telah dirancang. Proses pengujian dilakukan menggunakan Swagger UI untuk pengujian endpoint server serta client Python untuk mensimulasikan interaksi pengguna. Hasil pengujian menunjukkan bahwa seluruh fitur dapat berjalan dengan baik dan menghasilkan output yang sesuai.

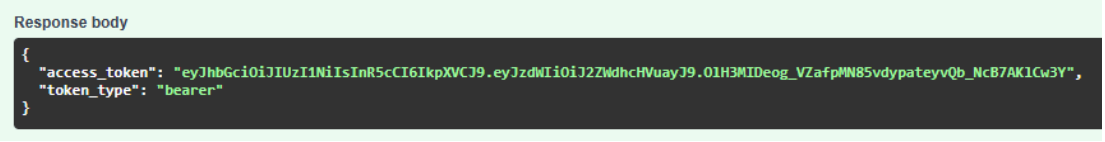
3.3.1 Pengujian Registrasi dan Login

Pengujian registrasi dan login dilakukan melalui endpoint /register dan /login menggunakan Swagger UI. Pada proses registrasi, pengguna memasukkan data yang diperlukan untuk pembuatan akun baru. Sistem kemudian memproses data tersebut dan menyimpan informasi registrasi ke dalam basis data sebagai histori registrasi pengguna. Penyimpanan histori ini bertujuan untuk mencatat aktivitas pendaftaran yang dilakukan, sehingga data pengguna dapat dikelola dan ditelusuri dengan lebih baik.

Setelah proses registrasi berhasil, pengguna dapat melakukan login menggunakan kredensial yang telah terdaftar. Sistem melakukan verifikasi data login dan menghasilkan respons yang sesuai. Berdasarkan hasil pengujian, proses registrasi dan login berjalan dengan baik, serta data registrasi berhasil tersimpan dan dapat digunakan kembali pada proses autentikasi berikutnya.



Gambar 3.3.1 Endpoint Register



Gambar 3.3.1.2 Endpoint Login

Gambar 3.3.1.3 File Histori Register User

3.3.2 Pengujian JWT Authorization

Pengujian JWT Authorization dilakukan untuk memastikan bahwa mekanisme autentikasi berbasis token berjalan dengan benar. Setelah pengguna berhasil login, server akan menghasilkan JWT Bearer Token yang digunakan untuk mengakses endpoint yang memerlukan autentikasi. Pengujian menunjukkan bahwa endpoint hanya dapat diakses apabila token yang diberikan valid, sehingga keamanan akses sistem dapat terjaga.

Gambar 3.3.2.1 Authorize Barier Token

3.3.3 Pengujian Penyimpanan Public Key

Pengujian penyimpanan public key dilakukan melalui endpoint /store. Public key yang digunakan dihasilkan oleh masing-masing pengguna melalui proses eksekusi client.py, di mana client secara otomatis membangkitkan pasangan private key dan public key menggunakan algoritma Ed25519. Public key yang dihasilkan kemudian dikirimkan ke server melalui mekanisme unggah file.

Server menerima public key dari client dan melakukan proses pemeriksaan integritas data sebelum menyimpannya. Setelah proses validasi berhasil, public key tersebut disimpan ke dalam media penyimpanan (storage) server dan dikaitkan dengan identitas pengguna yang bersangkutan. Berdasarkan hasil pengujian, public key dari setiap pengguna berhasil diterima dan tersimpan dengan baik, sehingga dapat digunakan kembali pada proses verifikasi signature dan tanda tangan digital selanjutnya.

Gambar 3.3.3.1 Penyimpanan Public Key sesuai User

3.3.4 Pengujian Verifikasi Signature Pesan

Pengujian verifikasi signature pesan dilakukan melalui endpoint /verify. Client mengirimkan pesan beserta signature yang telah dihasilkan menggunakan algoritma Ed25519. Server kemudian melakukan proses verifikasi menggunakan public key yang tersimpan. Hasil pengujian menunjukkan bahwa signature yang valid dapat diverifikasi dengan benar oleh sistem.

Response body


```
{
  "username": "vegapunk",
  "signature_status": "VALID",
  "message_checked": "Ini pesan rahasia dari client!"
}
```


Gambar 3.3.4.1 Validasi Pesan

3.3.5 Pengujian Verifikasi Tanda Tangan Digital PDF

Pengujian verifikasi dokumen PDF dilakukan melalui endpoint /verify-pdf dengan mengunggah file PDF beserta tanda tangan digitalnya. Server memverifikasi keaslian dan integritas dokumen berdasarkan hash dan signature yang diterima. Hasil pengujian menunjukkan bahwa dokumen PDF dengan tanda tangan yang sah berhasil diverifikasi oleh sistem.

Response body


```
{
  "status": "VALID",
  "message": "PDF ASLI dan signature cocok",
  "filename": "pdf kid.pdf"
}
```


Gambar 3.3.5.1 Validasi File PDF

3.3.6 Pengujian Relay Message

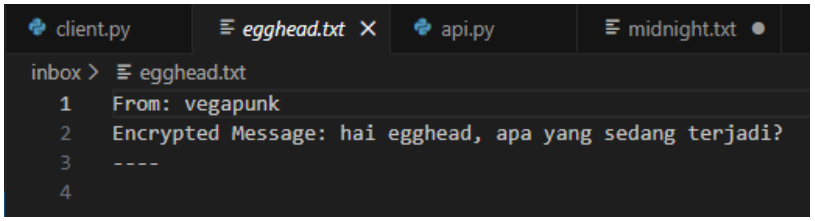
Pengujian relay message dilakukan untuk memastikan bahwa server dapat meneruskan pesan terenkripsi antar pengguna dengan benar. Pesan dikirim oleh pengirim menggunakan JWT user yang valid, kemudian diteruskan oleh server kepada pengguna tujuan tanpa membuka atau mengubah isi pesan.

Setelah pesan berhasil diteruskan, server menyimpan pesan tersebut ke dalam folder inbox milik masing-masing penerima. Pesan disimpan dalam bentuk file teks (.txt) yang berisi hasil pesan terenkripsi dari pengirim. Mekanisme ini memungkinkan setiap pengguna memiliki arsip pesan yang terpisah sesuai dengan identitas penerima, sehingga pesan dapat dikelola dan diakses kembali oleh pengguna yang bersangkutan. Berdasarkan hasil pengujian, pesan berhasil diteruskan ke penerima yang dituju dan tersimpan dengan baik di dalam inbox penerima dalam bentuk file .txt, tanpa mengganggu kerahasiaan isi pesan.

Response body


```
{
  "status": "success",
  "from": "vegapunk",
  "to": "egghead",
  "message": "Pesan terenkripsi berhasil dikirim ke egghead"
}
```


Gambar 3.3.6.1 Relay Pesan ke Receiver



Gambar 3.3.6.2 Inbox Pesan Receiver

BAB IV
HASIL DAN ANALISIS KEAMANAN

4.1 Hasil Pengujian

Berdasarkan seluruh pengujian yang telah dilakukan menggunakan Swagger UI dan client Python, dapat disimpulkan bahwa sistem keamanan data yang dibangun berjalan sesuai dengan kebutuhan fungsional yang dirancang. Seluruh endpoint utama dapat diakses dan menghasilkan keluaran yang sesuai dengan skenario pengujian. Proses registrasi dan login berhasil dilakukan, serta data pengguna dan histori registrasi dapat tersimpan dengan baik di dalam sistem. Mekanisme JWT Authorization berjalan dengan benar, di mana hanya pengguna dengan token yang valid yang dapat mengakses endpoint yang memerlukan autentikasi.

Pengujian penyimpanan public key menunjukkan bahwa public key yang dihasilkan dari eksekusi client.py pada masing-masing pengguna berhasil diterima oleh server dan tersimpan ke dalam storage, sehingga dapat digunakan kembali pada proses verifikasi signature. Selanjutnya, pengujian verifikasi signature pesan dan verifikasi tanda tangan digital PDF menunjukkan hasil VALID, yang menandakan bahwa sistem mampu menjamin keaslian dan integritas pesan maupun dokumen. Pada pengujian relay message, pesan terenkripsi berhasil diteruskan ke pengguna tujuan dan tersimpan dengan baik pada inbox masing-masing penerima dalam bentuk file teks (.txt), tanpa membuka atau mengubah isi pesan. Hal ini menunjukkan bahwa sistem mampu menjaga kerahasiaan komunikasi antar pengguna. Secara keseluruhan, hasil pengujian membuktikan bahwa sistem telah berfungsi dengan baik dan memenuhi aspek keamanan data, khususnya dalam hal autentikasi, kerahasiaan, dan integritas informasi.

4.2 Analisis Keamanan

Sistem yang dibangun telah menerapkan beberapa aspek keamanan penting untuk melindungi data dan komunikasi antar pengguna. Mekanisme autentikasi berbasis JWT (JSON Web Token) digunakan untuk memastikan bahwa hanya pengguna yang telah terverifikasi yang dapat mengakses endpoint tertentu. Setiap permintaan ke endpoint yang memerlukan autentikasi akan divalidasi menggunakan token yang sah, sehingga akses tidak sah dapat dicegah.

Selain itu, sistem melakukan pemeriksaan integritas data menggunakan fungsi hash untuk memastikan bahwa pesan maupun dokumen yang dikirimkan tidak mengalami perubahan selama proses transmisi. Aspek non-repudiation juga diterapkan melalui penggunaan digital signature, yang memungkinkan sistem untuk memastikan keaslian pengirim serta mencegah pengguna menyangkal pengiriman pesan atau dokumen.

Sistem ini juga dirancang untuk mendukung multiuser, dimana setiap pengguna memiliki identitas dan data yang terpisah. Mekanisme pembatasan akses diterapkan agar pengguna tidak dapat mengakses data milik pengguna lain, baik pada proses penyimpanan public key, verifikasi data, maupun pengelolaan pesan. Dengan penerapan aspek-aspek tersebut, sistem mampu memberikan tingkat keamanan yang memadai dalam pengelolaan dan pertukaran data.

BAB V
PENUTUP

5.1 Kesimpulan

Berdasarkan hasil perancangan, implementasi, dan pengujian yang telah dilakukan, dapat disimpulkan bahwa proyek ini berhasil membangun sebuah security service berbasis kriptografi untuk mendukung pertukaran pesan aman antar pengguna. Sistem yang dikembangkan mampu menyediakan layanan autentikasi, penyimpanan public key, verifikasi tanda tangan digital, verifikasi integritas dokumen PDF, serta mekanisme relay pesan terenkripsi melalui API berbasis FastAPI. Seluruh fungsi utama sistem dapat berjalan dengan baik sesuai dengan kebutuhan fungsional yang telah dirancang.

Penerapan algoritma kriptografi asimetris Ed25519, fungsi hash SHA-256, kriptografi simetris menggunakan skema Fernet (AES), serta mekanisme autentikasi berbasis JSON Web Token (JWT) terbukti mampu menjamin aspek keamanan data, khususnya autentikasi pengguna, kerahasiaan pesan, integritas data, dan keaslian pesan maupun dokumen digital. Hasil pengujian menunjukkan bahwa sistem dapat mendeteksi perubahan data, memverifikasi keabsahan signature, serta membatasi akses layanan hanya kepada pengguna yang terautentikasi.

Secara keseluruhan, sistem yang dibangun telah memenuhi tujuan proyek dan kriteria keamanan yang ditetapkan pada mata kuliah Keamanan dan Integritas Data. Implementasi ini diharapkan dapat menjadi dasar pengembangan layanan keamanan yang lebih kompleks di masa mendatang, serta memberikan pemahaman praktis mengenai penerapan konsep kriptografi dan keamanan data dalam sistem berbasis API.

DAFTAR PUSTAKA

JWT.io, *Introduction to JSON Web Tokens (JWT)*. [Online]. Available: https://www.jwt.io/introduction

National Institute of Standards and Technology (NIST), *Advanced Encryption Standard (AES)*, FIPS Publication 197, Nov. 2001. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197.pdf

National Institute of Standards and Technology (NIST), *Secure Hash Standard (SHS)*, FIPS Publication 180-4, Aug. 2015. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.180-4.pdf

S. Nakov, *EdDSA and Ed25519 Digital Signatures*, Cryptography Book. [Online]. Available: https://cryptobook.nakov.com/digital-signatures/eddsa-and-ed25519