Implementasi AES-256 sebagai Alternatif Solusi *End-to-End Encryption* pada Discord *Private Message*

Natasya Vercelly Harijadi 18221119
Program Studi Sistem dan Teknologi Informasi
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jalan Ganesha 10 Bandung
18221119@std.stei.itb.ac.id

***Abstract*—Discord merupakan salah satu *platform* komunikasi terkemuka di seluruh belahan dunia dengan basis pengguna mencapai 614 juta pengguna terdaftar per Januari 2024. Discord menawarkan berbagai macam fitur interaksi seperti percakapan pribadi, grup, obrolan suara dan video. Dengan fitur dan basis pengguna sebesar itu, Discord harus mengimplementasi kriptografi untuk menjaga keamanan percakapan dan privasi penggunanya. AES-256 dipilih sebagai solusi alternatif untuk menunjang keamanan dan privasi pengguna pada fitur percakapan pribadi. Algoritma kriptografi AES-256 dan aplikasi percakapan pribadi akan diimplementasi menggunakan Flet, sebuah *framework* Python berbasis Flutter yang dapat digunakan untuk membangun aplikasi *mobile, desktop,* maupun *website*.**

Kata kunci—Discord; AES-256; percakapan pribadi; Flet

I. PENDAHULUAN

Pada zaman digital ini, komunikasi yang aman menjadi hal yang paling penting, terutama untuk *platform* dengan basis pengguna yang luas. Discord, *platform* komunikasi terkemuka, tercatat memiliki lebih dari 614 juta pengguna terdaftar per Januari 2024. Dilansir dari helplama.com, peladen Discord melayani 4 miliar menit percakapan setiap harinya [1]. Dengan basis pengguna sebanyak ini, semakin menguatkan posisi Discord sebagai *platform* percakapan populer di dunia. Meskipun Discord menawarkan berbagai fitur interaksi, sperti obrolan suara, video, dan teks, keamanan pesan pribadi tetap menjadi perhatian penting. Seiring dengan berkembangnya ancaman dunia maya dan menigkatknya ekspektasi privasi pengguna, terdapat peningkatan kebutuhan akan metode enkripsi yang kuat untuk melindungi data sensitive pengguna.

Studi ini mengeksplorasi peneraman Advanced Encryption Standard (AES) dengan panjang kunci 256-bit sebagai solusi alternatif untuk E2EE pada sistem pesan pribadi Discord. AES-256, yang dikenal karena keamanan dan efisiensinya yang tangguh, menghadirkan pendekatan yang mumpuni untuk meningkatkan privasi pengguna dan perlindungan data. Standar enkripsi ini telah diadopsi secara luas di berbagai industry karena ketahanannya terhadap serangan kriptografi yang diketahui.

Studi ini mencoba mengimplementasikan AES-256 pada percakapan pribadi menggunakan kerangka kerja Flet yang berbasis bahasa pemrograman Python. Flet dipilih karena Flet mampu membuat aplikasi *multi-platform*, seperti *web*, *mobile application*, dan *desktop application* dengan Python. Hal ini sesuai dengan Discord yang dapat dijalankan di *website* atau sebagai aplikasi yang terinstal di *smartphone* dan *desktop*.

II. LANDASAN TEORI

A. Kriptografi

Kriptografi merupakan proses menutupi atau *encoding* data untuk memastikan bahwa hanya penerima yang diinginkan yang bisa membaca atau men-decipher pesan yang dikirim. Kriptografi telah ada selama beribu-ribu tahun untuk meng-encode pesan dan komunikasi. Kriptografi sampai saat ini digunakan untuk berbagai macam keperluan, seperti kartu kredit, kata kunci digital, hingga transaksi daring. [2]

Konsep dari kriptografi fokus pada *encoding* informasi dengan tujuan membatasi akses hanya kepada penerima yang diinginkan. Kriptografi juga disebut sebagai kriptologi, mengintegrasikan berbagai ilmu seperti ilmu komputer, rekayasa, dan matematika untuk menghasilkan kode yang mengacaukan konten asli dari sebuah pesan. [2]

B. Algoritma Kunci Simetri

Algoritma kunci simetri merupakan algoritma kriptografi yang memanfaatkan kunci yang sama untuk melakukan enkripsi dan dekripsi pada *plaintext*. Algoritma ini juga disebut dengan nama lain *single-key algorithm*.

C. Aplikasi Discord

Discord merupakan aplikasi untuk berinteraksi melalui suara, video, dan teks. Discord digunakan oleh jutaan individu berusia 13 tahun ke atas untuk berinteraksi dan bersosialisasi dengan komunitas dan teman-temannya.

Setiap harinya, aplikasi Discord digunakan untuk mendiskusikan berbagai macam topik, termasuk seni, liburan keluarga, hingga tugas sekolah. Discord berfungsi sebagai penghubung antar komunitas dari berbagai ukuran.

Orang-orang menyukasi Discord karena aplikasi Discord menyediakan wadah untuk komunitas dan grup pertemanan mereka. Discord menyediakan lingkungan di mana mereka dapat mengekspresikan diri dengan bebas dan menghabiskan waktu dengan orang-orang yang mempunyai ketertarikan yang

sama. Diskusi pada Discord terbentuk dari orang-orang dan topik yang dipilih penggunanya. [3]

D. *AES-256*

Standar global *block cipher* AES, juga diketahui sebagai Advanced Encryption Standard, merupakan salah satu metode kriptografi yang paling banyak digunakan dan populer di dunia. Dibuat pada 1997, AES telah sukses bertahan dari beberapa percobaan kriptanalis. [4]

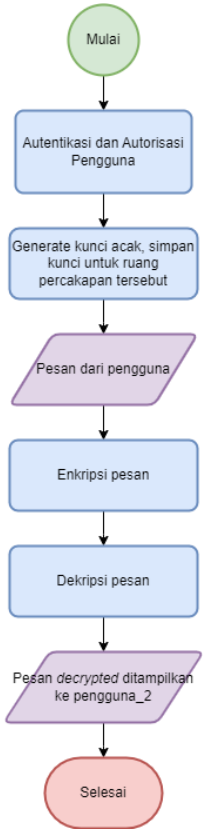
Dari seluruh versi AES, angka percobaan kriptanalis masih belum meningkat, 7 untuk AES-128, dan 8 untuk AES-192 dan AES-256; hanya ada penurunan pada kompleksitas komputasi untuk mengembalikan kunci. Dibanding AES, standar sebelumnya, DES, tidak terlihat ada peningkatan signifikas sejak studi yang dilakukan oleh Matsui pada 1993.

III. Rancangan Aplikasi dan Implementasi

Mock-up aplikasi Discord dan implementasi AES-256 direalisasikan menggunakan kerangka kerja Flet dengan bahasa pemrograman Python.

A. *Rancangan Aplikasi*

Aplikasi ini hanya akan mengimplementasi fitur percakapan pribadi pada Discord, dari berbagai fitur Discord yang tersedia. Pengguna dapat masuk dan mengobrol dengan teman-temannya melalui percakapan pribadi. Proses percakapan akan dienkripsi dan didekripsi menggunakan AES-256. Seluruh pesan yang dikirimkan pada percakapan akan disimpan dalam bentuk *encrypted*.



Gambar 1. Diagram alur aplikasi percakapan pribadi

B. *Implementasi*

Implementasi enkripsi dan dekripsi menggunakan AES-256.

```
from Crypto.Cipher import AES
from Crypto.Util.Padding import pad, unpad
from Crypto.Random import get_random_bytes

def encrypt(plaintext, key):
    cipher = AES.new(key, AES.MODE_ECB)
    ciphertext = cipher.encrypt(pad(plaintext, AES.block_size))
    return ciphertext

def decrypt(ciphertext, key):
    cipher = AES.new(key, AES.MODE_ECB)
    plaintext = unpad(cipher.decrypt(ciphertext),
AES.block_size)
    return plaintext

print("AES-256 Implementation")

# generate random key
key = get_random_bytes(32)
print("Key:", key)

plaintext = input("Plaintext: ").encode()

print("Encrypting...")
ciphertext = encrypt(plaintext, key)
print("Ciphertext:", ciphertext)

print("Decrypting...")
decrypted_text = decrypt(ciphertext, key)
print("Decrypted text:", decrypted_text)
```

C. *Simulasi*

Saat program dimulai, program akan membangkitkan kunci acak sepanjang 256 bit.

```
[redacted] py main.py
AES-256 Implementation
Key: b'B(\x13:\xec\x8a5\xf8\x83t\x1f\xbc\x03\xd3\xff\x1e\x84\\\xae\xf0$\xd6\xc1\xa1M\xe86\xbd`Z
\x85d'
```

Selanjutnya, masukkan pesan sebagai *plaintext*. Lalu program akan mengenkripsi dan mendekripsinya.

```
Plaintext: test
Encrypting...
Ciphertext: b'\n`o\x05\x8abB\x10\xbfJa\x00\xda]\xd0Q'
Decrypting...
Decrypted text: b'test'
```

REFERENCES

[1] "Discord Revenue and usage Statistics 2024". Retrieved from https://helplama.com/discord-statistics/ June 23rd, 2024.

[2] "What is Cryptography?" . Retrieved from https://www.fortinet.com/resources/cyberglossary/what-is-cryptography June 24th, 2024.

[3] Discord, "What is Discord?". Retrieved from https://discord.com/safety/360044149331-what-is-discord June 24th, 2024.

[4] A. Bogdanov, D. Khovratovich, and C. Rechberger, "Biclique cryptanalysis of the full AES", archived 2016.

PERNYATAAN

Dengan ini saya menyatakan bahwa makalah yang saya tulis ini adalah tulisan saya sendiri, bukan saduran, atau terjemahan dari makalah orang lain, dan bukan plagiasi.

Bandung, 24 Juni 2024

Natasya Vercelly Harijadi