Simulasi Kriptanalisis terhadap Skema Enkripsi Simetris dengan Kunci Statis pada Skenario Known-Plaintext Attack

Nicholas Francis Aditjandra - 18221005[1,2]
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia
[1]18221005@std.stei.itb.ac.id, [2]francisaditjandra@gmail.com

Abstrak*—Penggunaan kunci statis berulang merupakan salah satu skema enkripsi yang tidak seharusnya digunakan dalam sistem teknologi modern. Makalah ini akan melakukan simulasi skema enkripsi tersebut dan menganalisis masalah keamanan yang mungkin dihadapi ketika menggunakan skema tersebut terutama dalam kasus serangan Known Plaintext Attack (KPA). Serangan tersebut dilakukan ketika penyerang sudah memiliki akses terhadap pasangan plaintext dan ciphertext mulai dari satu pasangan yang tidak sempurna sampai beberapa pasangan lengkap. Hasil eksperimen menunjukkan bahwa meskipun penggunaan kunci statis dapat mempercepat proses sistem teknologi, enkripsi yang dihasilkan justru lemah dan dapat dipecahkan dalam waktu cepat juga dengan tingkat akurasi tinggi.

***Kata Kunci*—kriptanalisis, known plaintext attack, enkripsi simetris, kunci statis, manajemen kunci**

I. Pendahuluan

Selama beberapa dekade yang lalu, kriptografi simetris telah menjadi tulang punggung sistem keamanan informasi, dengan menyediakan kerahasiaan serta integritas informasi menggunakan algoritma yang efisien dan terpercaya. Namun, kelayakan keamanan informasi tidak bisa hanya ditentukan menggunakan algoritma yang efisien dan kuat tetapi juga melalui penerapan dan pengelolaan yang benar. Salah satu kesalahan umum yang masih sering diterapkan meskipun sudah dianggap berbahaya adalah penggunaan kunci statis yang tidak diganti secara rutin dalam waktu yang lama. Praktik ini seringkali digunakan karena efisiensinya dalam menghemat biaya operasional dan waktu komputasi. Situasi ini mengakibatkan adanya kerentanan yang dapat dieksploitasi menggunakan berbagai teknik kriptanalisis.

Dalam konteks keamanan modern, skema enkripsi ini seringkali berhasil dipecahkan menggunakan teknik known plaintext attack (KPA). KPA adalah sebuah teknik pemecahan enkripsi atau kriptanalisis yang dilakukan oleh penyerang yang memiliki setidaknya memiliki satu pasangan plaintext dan ciphertext yang sah. Dengan menggunakan informasi minimal tersebut, penyerang tidak hanya mampu mendapatkan kunci statis sistem tetapi juga dapat menggunakan kunci tersebut untuk membuka enkripsi semua data yang ada di dalam sistem. Serangan ini biasanya dilakukan dengan memanfaatkan beberapa vektor untuk mendapatkan pasangan plaintext ciphertext baik melalui sniffing jaringan, injeksi konten, kebocoran data parsial atau bahkan analisis pola data terprediksi seperti header pada protokol. Dalam sistem yang menggunakan kunci statis, setiap pasangan plaintext dan ciphertext yang diketahui akan semakin mengurangi entropi kunci yang pada kasus ekstrim seperti pada enkripsi berbasis XOR kemungkinan besar kunci akan dapat diungkapkan dengan mudah.

Salah satu insiden yang menunjukkan kerentanan dari kunci statis dapat terlihat pada implementasi awal wired equivalent privacy (WEP) untuk wifi. Protokol keamanan WEP dianggap rentan karena tidak hanya menggunakan kunci statis tetapi juga menggunakan initialization vector (IV) yang lemah. Kerentanan tersebut mengakibatkan berbagai serangan dimana penyerang membobol kunci hanya dengan menyadap lalu lintas data dan menganalisis packet yang telah diambil tersebut. Kunci statis juga umum digunakan di berbagai situs web dimana kunci sesi statis mengakibatkan pencurian sesi pengguna dan memberikan hak akses ilegal kepada penyerang. Kasus-kasus ini memberikan pembelajaran bagi para developer dimana masalah tidak hanya bisa muncul dari kecanggihan rumus dan kunci enkripsi tetapi juga dari bagaimana kunci enkripsi tersebut digunakan.

Penelitian ini bertujuan untuk menyelidiki seberapa rentankah sistem enkripsi simetris menggunakan kunci statis apabila diserang menggunakan metode known plaintext attack hanya dengan pasangan plaintext dan ciphertext. Eksperimen akan mengukur seberapa efektif serangan ini dan faktor apa yang menentukan keberhasilannya. Dalam mendapatkan data dan informasi tersebut, akan dibangun sebuah simulasi yang menerapkan enkripsi berbasis XOR yang menggunakan kunci statis dan menguji enkripsi tersebut dalam berbagai skenario serangan untuk mengamati hasilnya.

II. Landasan Teori

Bagian ini membahas berbagai konsep kriptografi yang menjadi dasar dalam penelitian ini. Penjelasan diberikan untuk memberikan konteks teori yang memadai mengenai eksperimen yang dilakukan bagi pembaca makalah ini.

A. Kriptografi Simetris

Kriptografi simetris atau juga disebut kriptografi kunci privat adalah sebuah sistem kriptografi dimana seluruh entitas yang berkomunikasi akan menggunakan dan berbagi kunci rahasia yang sama untuk proses enkripsi dan dekripsi mereka. Fungsi dari kriptografi simetris dapat dilambangkan menggunakan formula berikut:

$$C = Ek(P) \tag{1}$$

$$P = Dk(C) \tag{2}$$

Dimana ciphertext C didapatkan dari diterapkannya kunci enkripsi E_k terhadap plaintext P dan sebaliknya plaintext P didapatkan dari diterapkannya kunci dekripsi D_k terhadap ciphertext C. Formula tersebut hanya berlaku apabila

$$Dk(Ek(P)) = P \tag{3}$$

Kriptografi memiliki beberapa keunggulan spesifik jika dibandingkan kriptografi asimetris, yaitu kecepatan komputasi yang lebih tinggi dan efisiensi dalam menangani data dengan volume besar. Namun, untuk keamanan dari sistem ini bergantung pada dua aspek utama yaitu kekuatan algoritma kriptografis yang digunakan dan keamanan distribusi dan pengelolaan kunci. Algoritma simetris modern seperti Advanced Encryption Standard (AES) telah terbukti mampu bertahan terhadap serangan kriptanalisis ketika diimplementasikan dengan baik, tetapi dengan pengelolaan kunci yang buruk, keamanan yang didapatkan menjadi tidak berguna kembali.

Gambar 2.1 Diagram Kriptografi Kunci Simetris
Sumber :
https://doubleoctopus.com/security-wiki/encryption-and-cryptography/symmetric-key-cryptography/

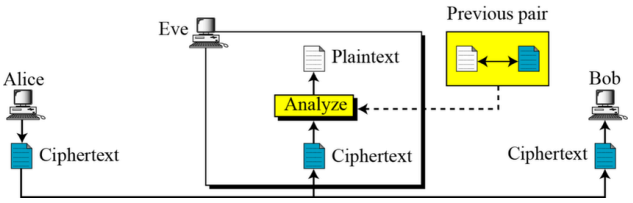
B. Kriptanalisis

Kriptanalisis adalah sebuah cabang ilmu kriptografi yang mempelajari metode untuk memecahkan sistem kriptografi yang ada. Berdasarkan informasi yang ada, serangan kriptanalisis dapat dibagi menjadi :

1. Ciphertext Only Attack (COA): Dimana penyerang hanya memiliki akses ke ciphertext.
2. Known Plaintext Attack (KPA): Dimana penyerang memiliki satu atau beberapa pasangan plaintext dan ciphertext.
3. Chosen Plaintext Attack (CPA): Dimana penyerang dapat memperoleh ciphertext untuk plaintext buatannya.
4. Chosen Ciphertext Attack (CCA): Dimana penyerang dapat memperoleh dekripsi untuk ciphertext buatannya.

Diantara berbagai tipe serangan tersebut, KPA adalah metode yang paling sering digunakan dalam skenario penyerangan di dunia nyata. Hal itu terjadi karena penyerang secara umum dapat memperoleh plaintext menggunakan berbagai metode serangan seperti analisis pola data, injeksi konten atau eksploitasi kerentanan sistem.

Pada KPA, dari pasangan plaintext dan ciphertext yang ada, penyerang berusaha menggunakan algoritma linier kepada pasangan yang ada untuk membentuk sebuah sistem persamaan yang dapat diselesaikan. Dari persamaan yang didapatkan penyerang kemudian dapat memulihkan kunci atau melakukan dekripsi ciphertext lain tanpa menemukan kunci. Tujuan akhir serangan adalah untuk mengumpulkan keseluruhan plaintext dari ciphertext yang ada pada sistem.



Gambar 2.2 Diagram Umum Know Plaintext Attack
Sumber :
https://www.researchgate.net/figure/Shows-how-Known-Plaintext-Attack-works_fig6_371119558

C. Enkripsi XOR

Operasi XOR (eXclusive OR) memiliki sifat matematis yang unik yang membuatnya berguna untuk diterapkan dalam fungsi kriptografi. Operasi XOR $\oplus$ berfungsi pada byte a dan b berdasarkan kedua aturan dasar untuk berikut:

$$a \oplus b = 1, a \neq b \tag{4}$$

$$a \oplus b = 0, a = b \tag{5}$$

Selain itu sifat-sifat penting dari XOR yang bisa dimanfaatkan adalah:

1. Komutatif : $a \oplus b = b \oplus a$
2. Asosiatif : $(a \oplus b) \oplus c = a \oplus (b \oplus c)$
3. Involutif : $(a \oplus b) \oplus b = a$
4. Identitas : $a \oplus 0 = a$
5. Self-inverse : $a \oplus a = 0$

Dalam penerapannya pada enkripsi, untuk plaintext biner P dan ciphertext biner C akan ada kunci biner dengan panjang yang sama K dengan formula:

$$C = P \oplus K \tag{6}$$

$$P = C \oplus K \tag{7}$$

Dalam penerapannya, apabila kunci K benar-benar acak dan hanya dapat digunakan sekali maka sistem akan benar-benar aman. Namun ketika kunci K digunakan berulang sebagai kunci statis, keamanan akan hilang sepenuhnya.

Pada KPA terhadap enkripsi XOR, hubungan plaintext pasangan P_i dan ciphertext C_i serta kunci K akan bersifat deterministik untuk setiap pasangan dengan formula berikut:

$$K = Pi \oplus Ci \tag{8}$$

III. Implementasi

A. Desain Sistem Simulasi

Implementasi eksperimen dirancang untuk menguji kerentanan enkripsi berbasis XOR dengan kunci statis terhadap known plaintext attack. Eksperimen ini akan terdiri dari dua modul utama yaitu :

1. *Modul Sistem Enkripsi*
   Enkripsi akan dilakukan dengan enkripsi XOR menggunakan kunci statis yang dapat diubah panjangnya dari 64 byte, 128 byte hingga 256 byte. Kunci dibuat menggunakan pembangkit nilai acak kriptografis dari library secrets.

2. *Modul Penyerang*
   Known plaintext attack akan dilakukan pada empat skenario umum yaitu, serangan dengan satu pasangan lengkap, serangan dengan informasi parsial, serangan analisis efek domino serta serangan dengan informasi dunia nyata yang terprediksi.

B. Skenario Pengujian

Empat skenario utama akan disimulasikan untuk menguji aspek berbeda dari kerentanan sistem ini. Setiap skenario akan diulang sebanyak 100 kali untuk mendapatkan data statistik yang signifikan.

1. *Pemulihan Kunci dengan Satu Pasangan*

Skenario ini dilakukan untuk menguji kemampuan pemulihan kunci ketika penyerang memiliki sepasang plaintext dan ciphertext lengkap. Pertama-tama kunci akan dibangkitkan dengan tiga konfigurasi yaitu 64, 128 dan 256 byte. Kemudian sebuah plaintext acak akan dibuat dan diproses sehingga didapatkan ciphertextnya. Pasangan tersebut akan kemudian dimasukkan ke dalam fungsi KPA untuk mendapatkan kunci asli. Kunci ini kemudian akan dibandingkan dengan kunci asli untuk membuktikan bahwa satu pasangan kunci cukup untuk mengkompromi sistem enkripsi XOR sederhana.

2. *Analisis Efek Domino Kunci Simetris*

Skenario ini akan menganalisis lebih lanjut efek domino yang dialami dari penggunaan kunci statis di dalam sistem. Eksperimen berusaha mencari tahu seberapa cepat sekumpulan ciphertext pesan didekripsi sebagai akibat langsung KPA pada pasangan pesan yang bocor. Penyerang pada tahap ini juga hanya akan diberikan satu pasangan plaintext dan ciphertext yang akan digunakan untuk memulihkan kunci. Kunci ini kemudian akan digunakan untuk mendekripsi pesan-pesan lainnya. Skenario ini akan dilakukan dengan pengaturan kunci 128 byte dan jumlah pesan 5, 10 dan 20 pesan. Skenario ini bertujuan untuk menunjukkan bahwa kompromi satu pesan akan dengan cepat merambat ke seluruh pesan terenkripsi di dalam sistem dengan kunci statis.

3. *Serangan dengan Partial Known Plaintext*

Skenario ini mensimulasikan kondisi yang lebih realistis dimana penyerang hanya memiliki pengetahuan parsial mengenai plaintext. Pada skenario ini, KPA akan dilakukan pada sebagian plaintext yang memiliki lokasi random dengan tingkat pengetahuan 25%, 50% dan 75% dari plaintext. Skenario ini dilakukan untuk mengetahui seberapa besar ancaman yang mungkin dialami sistem meski hanya dengan sebagian dari plaintext.

4. *Serangan dengan Pola Data Dunia Nyata*

Skenario ini dirancang untuk mencari tahu seberapa valid eksperimen yang dilakukan dengan menerapkannya pada pola data yang umum ditemukan di dunia nyata. Lima pola data yang akan diuji adalah:

- Header HTTP dengan contoh format "GET / HTTP/1.1\r\nHost: "
- Header email dengan contoh format "From: user@example.com\r\nTo: "
- Magic number PNG dengan contoh format "\x89PNG\r\n\x1a\n"
- Struktur JSON dengan contoh format "{"username":""
- Query SQL dengan contoh format "SELECT * FROM users WHERE "

Semua pola tersebut mewakili pola data yang seringkali dapat ditebak penyerang dalam skenario dunia nyata. Eksperimen dilakukan dengan membuat plaintext yang terdiri dari pola yang diketahui tersebut ditambah dengan data acak sebagai filler yang kemudian dienkripsi dengan kunci. Penyerang kemudian diberikan hanya plaintext bagian pola dunia nyata tersebut dan ciphertext lengkap. Skenario ini bertujuan untuk mencari tahu bagaimana

performa aplikasi praktis dari KPA terhadap sistem di dalam konteks nyata.

C. Metrik Pengukuran

Metrik yang digunakan untuk mengukur hasil dari skenario tersebut adalah:

1. Tingkat Keberhasilan (Success Rate)
   Tingkat keberhasilan diukur sebagai persentase pemulihan kunci dibandingkan total upaya pemulihan kunci. Formula tingkat keberhasilan adalah

$$SR = (Jumlah\ iterasi\ K' = K) / (Total\ iterasi) * 100\% \quad (9)$$

2. Rata-rata Waktu Serangan (Average Execution Time)
   Metrik ini akan mengukur rata-rata waktu serangan untuk 100 iterasi untuk masing-masing skenario dengan variasi masing-masing. Pengukuran waktu diukur mencakup waktu komputasi XOR, analisis data dan verifikasi akhir. Pengukuran waktu akan menggunakan library time. Formula rata-rata waktu serangan adalah

$$AET = \Sigma(Waktu\ serangan\ berhasil) / (Total\ iterasi\ berhasil) \quad (10)$$

3. Akurasi Pemulihan Pesan (Message Recovery Accuracy)
   Untuk skenario efek domino, akurasi pemulihan pesan akan dihitung dengan membandingkan banyaknya pesan yang didekripsi dengan benar setelah kunci didapatkan. Formula akurasi pemulihan pesan adalah

$$MRA = (Jumlah\ pesan\ didekripsi) / (Total\ pesan\ diuji) \times 100\% \quad (11)$$

IV. Hasil Eksperimen

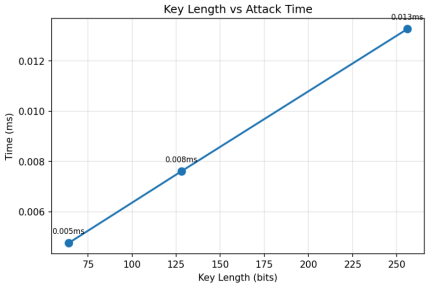
A. Hasil Eksperimen Pemulihan Kunci dengan Satu Pasangan

Berikut adalah hasil data pengujian KPA pemulihan kunci dengan satu pasangan.

Panjang Kunci (Byte)	Tingkat Keberhasilan (%)	Total Waktu (s)
64	100	0.004747001221403 48
128	100	0.007607999868923 798
256	100	0.013270999770611 525

Tabel 4.1 Tabel Hasil Eksperimen Pemulihan Kunci dengan Satu Pasangan

Dari hasil tersebut dapat terlihat bahwa waktu pembuatan meskipun mengalami peningkatan untuk masing-masing panjang kunci, KPA masih secara konsisten mengindikasikan performa yang tinggi dalam memecahkan sistem XOR. Berikut adalah hasil diagram perbandingan panjang kunci dan waktu serangan eksperimen ini



Gambar 4.1 Diagram Perbandingan Panjang Kunci dan Waktu Serangan

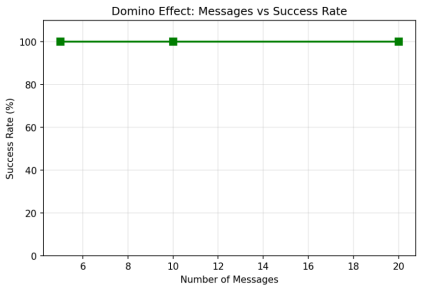
B. Hasil Eksperimen Efek Domino Kunci Simetris

Berikut adalah hasil data eksperimen efek domino kunci simetris dengan panjang kunci 128 byte dan panjang pesan 16 byte.

Jumlah Pesan	Tingkat Keberhasilan (%)	Total Waktu (s)
5	100	0.031837999995332 21
10	100	0.059698000550270 08
20	100	0.115906999999424 44

Tabel 4.2 Tabel Hasil Eksperimen Efek Domino Kunci Simetris

Berdasarkan hasil eksperimen tersebut, dapat dilihat bahwa meskipun jumlah pesan mempengaruhi total waktu pemecahan enkripsi semua pesan, tingkat keberhasilan tidak dipengaruhi sama sekali dari hal tersebut. Hasil ini menunjukan bahwa penggunaan kunci status memberikan sebuah titik kelemahan dimana kompromi di satu bagian sistem akan meruntuhkan keseluruhan sistem. Berikut adalah diagram akurasi pemulihan pesan eksperimen ini.



Gambar 4.2 Diagram Akurasi Pemulihan Pesan Efek Domino

C. Hasil Eksperimen Serangan dengan Partial Known Plaintext

Berikut adalah hasil data eksperimen serangan dengan partial known plaintext dengan panjang kunci 128 byte dan posisi known plaintext acak.

Known Plaintext (%)	Tingkat Keberhasilan (%)	Total Waktu (s)
25	100	0.004077000339748338
50	100	0.005240998434601352
75	100	0.006510999810416251

Tabel 4.3 Tabel Hasil Eksperimen Serangan dengan Partial Known Plaintext

Dari data tersebut dapat terlihat pada eksperimen bahwa persentase known plaintext tidak terlalu mempengaruhi waktu dan bahkan tidak mengurangi tingkat keberhasilan. Hal tersebut menunjukkan bahwa setiap byte plaintext yang diketahui secara langsung mengungkapkan byte kunci yang sesuai tanpa memerlukan analisis tambahan mengenai konteks sistem.

D. Hasil Eksperimen Serangan dengan Pola Data Dunia Nyata

Berikut adalah hasil data eksperimen serangan dengan pola data dunia nyata.

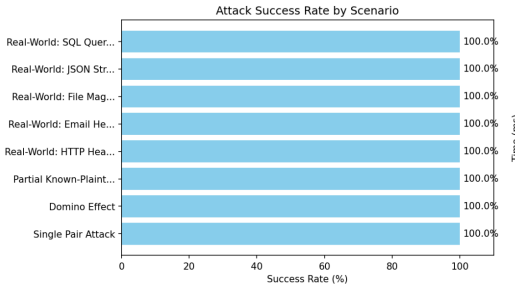
Pola Data	Panjang Pola (Byte)	Tingkat Keberhasilan (%)	Total Waktu (s)
Header HTTP	35	100	0.006315999780781567
Header email	47	100	0.004665999440476298
Magic number	8	100	0.002880000683944723
PNG			
Struktur JSON	35	100	0.004943999520037323
Query SQL	36	100	0.004883999063167721

Tabel 4.4 Tabel Hasil Eksperimen Serangan dengan Pola Data Dunia Nyata

Dari data tersebut dapat terlihat pada eksperimen bahwa waktu hanya dipengaruhi oleh panjang dari known plaintext masing-masing pola. Selain itu semakin prediktif pola header, semakin cepat juga komputasi KPA. Hal tersebut menunjukkan bahwa KPA dapat digunakan untuk mengkonfirmasi bagian data terprediksi dengan cepat, tetapi untuk memperluas pengetahuan mengenai kunci perlu diterapkan metode kriptanalisis lain.

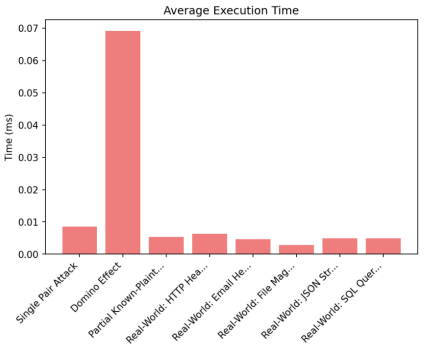
E. Analisis Statistik Komprehensif

Berikut adalah diagram perbandingan tingkat keberhasilan antara semua skenario yang telah dilakukan. Dimana secara keseluruhan tingkat keberhasilan KPA pada semua skenario adalah 100%.



Gambar 4.3 Diagram Perbandingan Tingkat Keberhasilan Antar Skenario

Berikut adalah diagram perbandingan rata-rata waktu serangan antara semua skenario yang telah dilakukan.



Gambar 4.2 Diagram Perbandingan Rata-rata Waktu Serangan

Rata-rata untuk semua skenario berkisar pada area yang sama di bawah 0.01 detik kecuali untuk skenario efek

domino. Perbedaan waktu skenario tersebut berkorelasi langsung dengan jumlah operasi XOR yang dilakukan pada setiap byte. Selain itu, perbedaan waktu besar pada skenario efek domino adalah akibat dari lebih banyaknya KPA dilakukan pada skenario tersebut.

V. Kesimpulan

Berdasarkan hasil eksperimen yang telah dilakukan, dapat disimpulkan bahwa penggunaan kunci statis dalam skema enkripsi simetris berbasis XOR menimbulkan kerentanan keamanan yang signifikan terhadap known plaintext attack. Mulai dari skenario pertama, tingkat keberhasilan serangan mencapai 100% untuk semua panjang kunci dengan waktu eksekusi yang sangat cepat. Hal ini membuktikan bahwa kerentanan enkripsi bersifat deterministik dan tidak bergantung pada panjang kunci.

Dari skenario efek domino, didapatkan data tingkat keberhasilan serangan yang mencapai 100% untuk semua jumlah pesan. Waktu eksekusi yang dibutuhkan meningkat secara linier dengan jumlah pesan yang perlu didekripsi, tetapi tidak mengurangi efektivitas serangan. Hal ini menunjukkan bahwa kunci statis menciptakan *single point of failure* yang dapat meruntuhkan keamanan seluruh sistem.

Serangan partial known plaintext tetap efektif bahkan dengan pengetahuan terbatas dimana 25% byte plaintext dapat memulihkan 25% byte kunci dengan akurasi sempurna. Hubungan persentase plaintext dan pemulihan kunci yang 1:1 mengindikasikan bahwa setiap byte informasi bocor akan mengungkapkan byte kunci yang sesuai. Pola data dunia nyata yang dapat terprediksi berfungsi sebagai known plaintext yang efektif dalam KPA dimana tingkat keberhasilan mencapai 100% dengan waktu eksekusi yang cepat.

Secara keseluruhan, penelitian ini membuktikan bahwa masalah keamanan sistem enkripsi seringkali tidak terletak pada kekuatan algoritma kriptografis itu sendiri, tetapi juga pada implementasi dan pengelolaan kunci yang tepat. Meskipun penggunaan kunci statis dapat membantu mengurangi beban komputasi sistem teknologi, kerentanan sistemik yang diciptakan justru akan lebih merugikan sistem tersebut dalam jangka panjang kehidupan sistem tersebut. Oleh karena itu, direkomendasikan untuk menghindari penggunaan kunci statis di dalam sebuah sistem. Selain itu dapat diterapkan juga metode pengelolaan kunci yang lebih aman seperti rotasi kunci berkala, penggunaan nonce atau initialization vector yang unik. Penelitian lebih lanjut dapat menguji kerentanan serupa pada algoritma enkripsi yang lebih kompleks dan atau mencoba mengeksplorasi teknik mitigasi kerentanan yang lebih baik.

VI. Ucapan Terima Kasih

Penulis mengucapkan syukur kepada Tuhan Yang Maha Esa yang telah membantu dalam setiap langkah penulisan makalah ini. Ucapan terima kasih juga penulis sampaikan kepada Bapak Dr. Ir. Rinaldi Munir, M.T. selaku dosen pengampu mata kuliah IF4020 Kriptografi atas bimbingan, arahan serta wawasan yang telah diberikan selama perkuliahan sehingga makalah ini dapat disusun dengan baik. Penulis juga menyampaikan apresiasi kepada seluruh pihak yang telah memberikan dukungan dan masukan selama penyusunan makalah ini.

References

[1] W. Stallings, *Cryptography and Network Security: Principles and Practice*, 8th ed. Pearson, 2020. [*Online*]. Tersedia: https://dl1.technet24.ir/Downloads/EBooks/Cryptography-and-Network-Security-Principles-and-Practice-Global-Edition-Pearson_Technet24.pdf. Diakses: 24 Desember 2025.

[2] J. Katz and Y. Lindell, Introduction to Modern Cryptography, 3rd ed. CRC Press, 2020. [*Online*]. Tersedia: http://staff.ustc.edu.cn/~mfy/moderncrypto/reading%20materials/Introduction_to_Modern_Cryptography.pdf. Diakses: 24 Desember 2025.

[3] L. Ertaul and O. Catambay, "Today & Tomorrow: IEEE 802.11 WLAN Security," in Proc. Int. Conf. Security and Management (SAM), Las Vegas, NV, USA, 2009, pp. 73-77. [Online]. Tersedia: https://www.researchgate.net/publication/221199759_Today_Tomorrow_IEEE_80211_WLAN_Security. Diakses: 24 Desember 2025.

[4] Symmetric-Key Cryptography. Double Octopus. [Online]. Tersedia: https://doubleoctopus.com/security-wiki/encryption-and-cryptography/symmetric-key-cryptography/. Diakses: 24 Des. 2025.

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, 26 Desember 2025

Nicholas Francis Aditjandra
18221005