STUDI LITERATUR: ANALISIS PERBANDINGAN ALGORITMA HASH (MD5, SHA-2, SHA-3, DAN SHA-512)

Menemukan "Ide" Implementasi Terbaik untuk Keamanan Otentikasi

Mata Kuliah: Kriptografi

Dosen Pengampu: Jefry Sunupurwa Asri, S.Kom., M.Kom.

Disusun oleh:

Dini Febryana Sari 20230801168

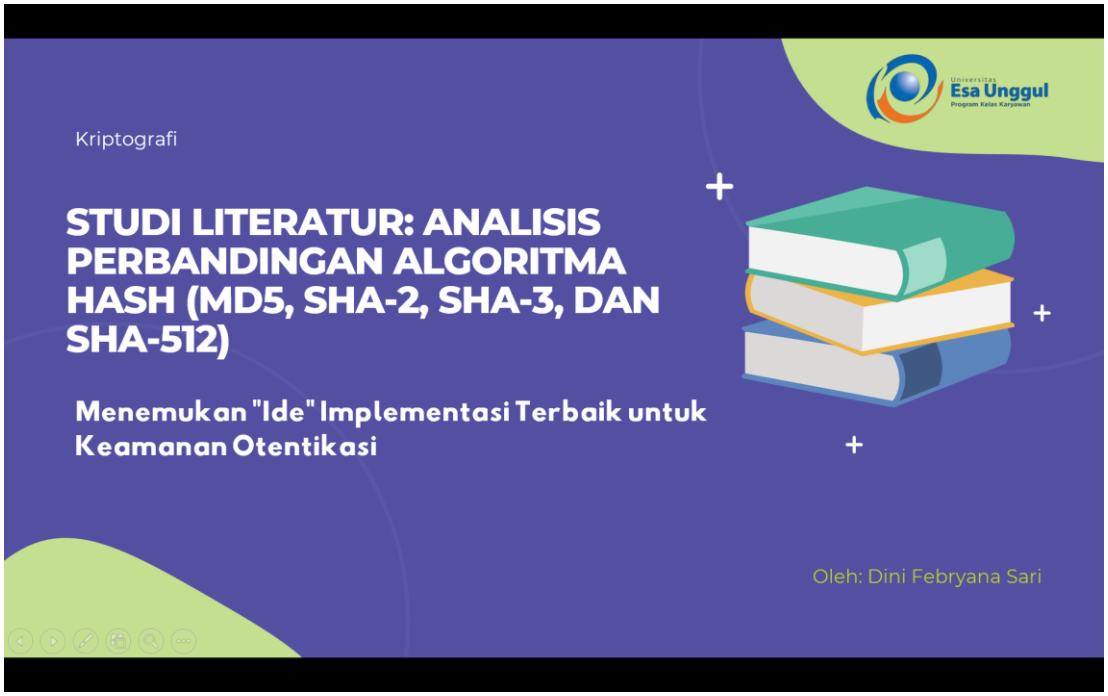
PROGRAM STUDI TEKNIK INFORMATIKA

FAKULTAS ILMU KOMPUTER

UNIVERSITAS ESA UNGGUL TANGERANG

2025

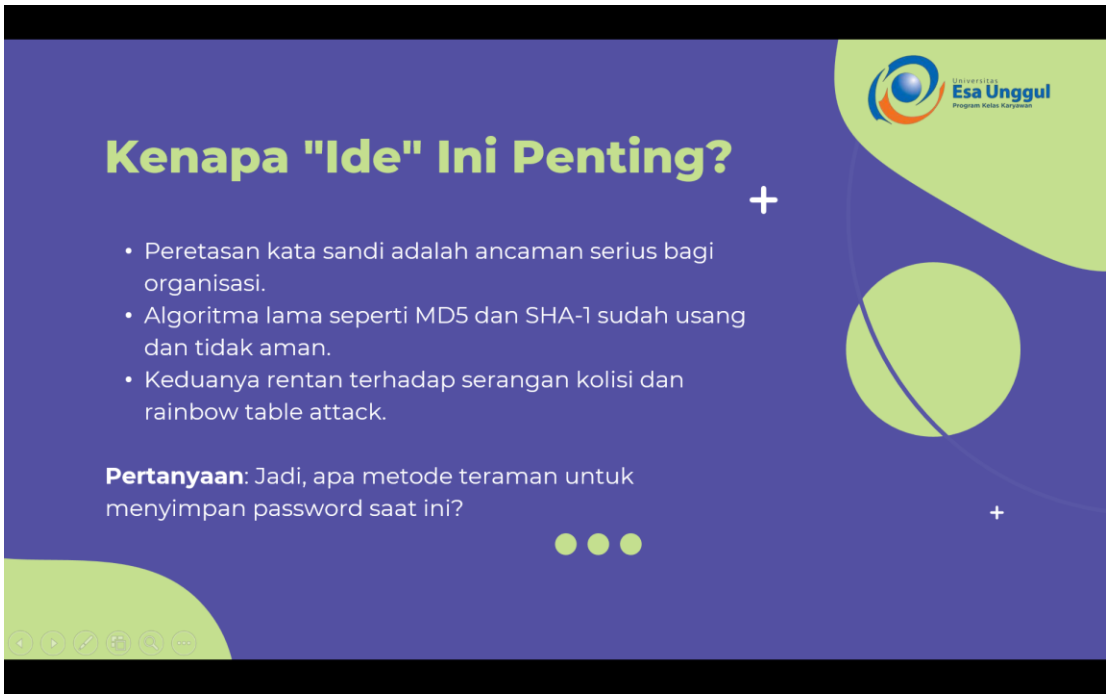
1. **Slide 1: Judul Presentasi**



Naskah Penjelasan: Selamat pagi/siang, Bapak Jefry Sunupurwa Asri, S.Kom., M.Kom. Saya Dini Febryana Sari dengan NIM 20230801168. Pada kesempatan ini, saya akan mempresentasikan hasil studi literatur saya mengenai perbandingan algoritma hash, khususnya MD5, SHA-2, SHA-3, dan SHA-512.

Tujuan dari presentasi ini adalah untuk menemukan "ide" atau gagasan implementasi terbaik untuk keamanan otentikasi.

2. **Slide 2: Latar Belakang**



Naskah Penjelasan: Peretasan kata sandi adalah ancaman serius bagi organisasi. Algoritma lama seperti MD5 dan SHA-1 sudah usang dan tidak aman. Keduanya rentan terhadap serangan kolisi dan *rainbow table attack*.

Hal ini membawa kita pada pertanyaan penelitian utama: Jadi, apa metode teraman untuk menyimpan *password* saat ini?

3. **Slide 3: Analisis Berdasarkan Konteks**

Naskah Penjelasan: Algoritma yang "terbaik" sangat bergantung pada konteks penggunaannya.

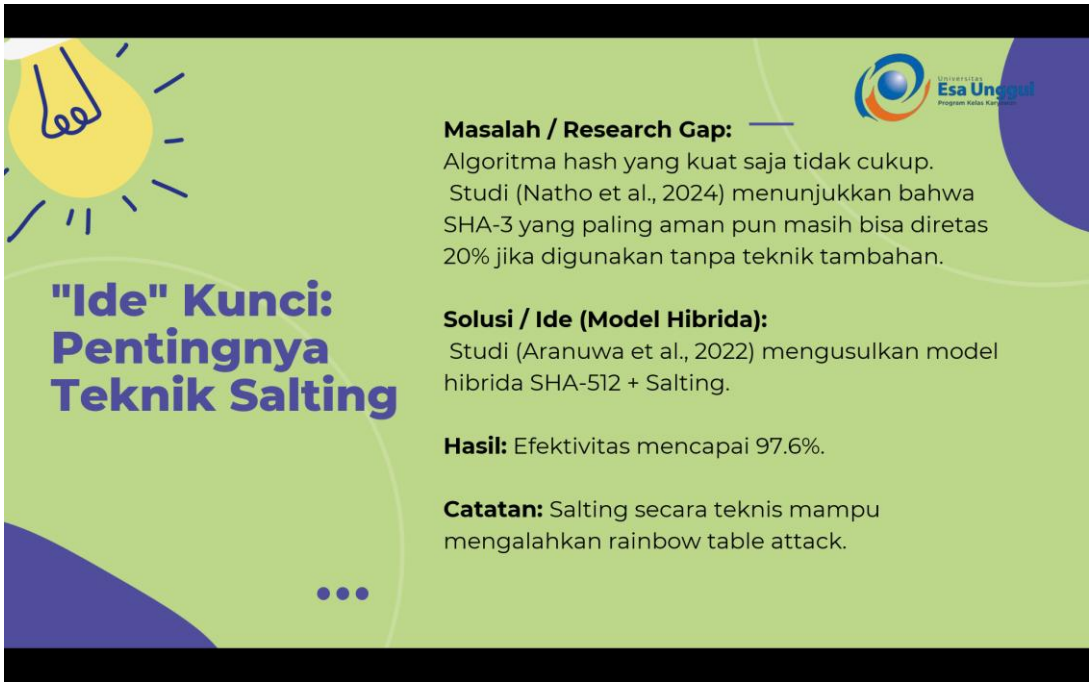
Konteks 1: Penyimpanan Password

Sebuah studi (Natho et al., 2024) membandingkan MD5, SHA1, SHA2, dan SHA3. Hasilnya, SHA-3 ditemukan paling aman (hanya 20% tembus) meskipun ia juga yang paling lambat. Perlu dicatat, lambat itu justru baik untuk *password* karena membuat serangan *brute force* menjadi mahal.

Konteks 2: Otentikasi API (JWT)

Sebuah studi (Rasyada, 2022) membandingkan SHA-512 vs SHA-256. Hasilnya menunjukkan bahwa SHA-512 sangat baik, bahkan sedikit lebih cepat (512.8 ms) dari SHA-256 (515.55 ms) dalam pengujian tersebut.

4. **Slide 4: Ide Kunci dan Solusi**



Naskah Penjelasan: Dari analisis tadi, kita sampai pada "Ide" kunci yaitu pentingnya Teknik Salting.

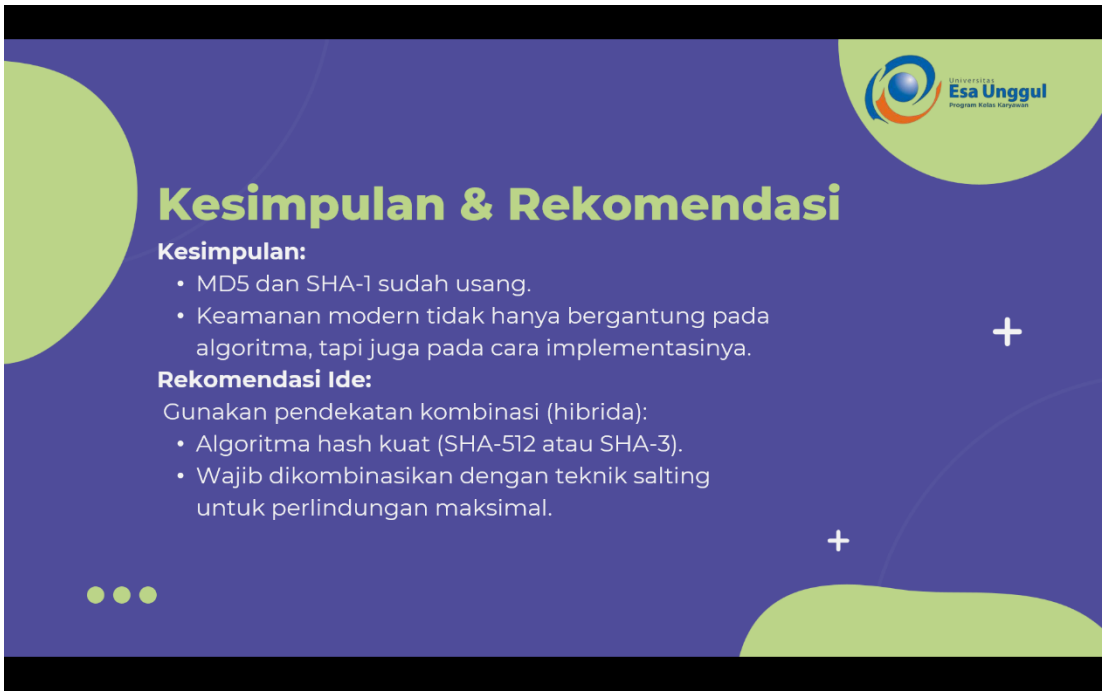
Masalah / Research Gap

Algoritma hash yang kuat saja ternyata tidak cukup. Studi Natho et al. (2024) menunjukkan bahwa SHA-3 yang paling aman pun masih bisa diretas 20% jika digunakan tanpa teknik tambahan.

Solusi / Ide (Model Hibrida)

Sebuah studi (Aranuwa et al., 2022) mengusulkan model hibrida SHA-512 yang dikombinasikan dengan *Salting*. Hasil model hibrida ini menunjukkan efektivitas keamanan mencapai 97.6%. *Salting* secara teknis mampu mengalahkan *rainbow table attack*.

5. **Slide 5 & 6: Kesimpulan & Rekomendasi**



Naskah Penjelasan: Sebagai kesimpulan dari studi literatur ini:

1. MD5 dan SHA-1 sudah usang.
2. Keamanan modern tidak hanya bergantung pada algoritma, tetapi juga pada cara implementasinya.

Rekomendasi Ide Implementasi: Gunakan pendekatan kombinasi atau hibrida. Pilih algoritma hash yang kuat (seperti SHA-512 atau SHA-3), dan wajib dikombinasikan dengan teknik *salting* untuk perlindungan maksimal.

Demikian presentasi studi literatur yang dapat saya sampaikan. Terima kasih atas perhatian Bapak Jefry