



YAYASAN MEMAJUKAN ILMU DAN KEBUDAYAAN
UNIVERSITAS SIBER ASIA

Kampus Menara, Jl. RM. Harsono, Ragunan - Jakarta Selatan, Daerah Khusus Ibukota Jakarta 12550.
Telp. (+6221) 27806189. pmb@unsia.ac.id <https://unsia.ac.id>

UJIAN TENGAH SEMESTER
SEMESTER GANJIL TAHUN AJARAN 2024/2025

Mata Kuliah : **Kriptografi dan Steganografi**
Kelas : IF501, IF504, IF505
Prodi : **Informatika PJJ S1**
Waktu : **1 s/d 14 Desember 2025**
Dosen : Abdul Azzam Ajhari, S.Kom., M.Kom.
Sifat Ujian : **Kelompok – Project Base Test**

Petunjuk Pengerjaan Soal:

- *Dilarang keras copy-paste atau plagiat hasil tugas rekannya. (jika copy-paste atau plagiat maka nilai 0 untuk nilai keduanya).*
- *Dilarang keras menggunakan tools AI dalam bentuk apapun untuk membuat laporan, jika ketahuan maka nilai 0.*

JAWABAN

"Invisible Guardian: Analisis Implementasi Kriptografi dalam Menghadapi Ancaman Siber Modern"

1. PENDAHULUAN

Di era di mana data adalah 'minyak baru', kebocoran data bukan lagi sekadar isu teknis, melainkan bencana nasional. Mengambil pelajaran dari kasus Ransomware PDN (Pusat Data Nasional) tahun 2024, kita melihat bagaimana kegagalan dalam manajemen kunci dan enkripsi bisa melumpuhkan negara. Laporan ini merangkum hasil eksplorasi modul TryHackMe mengenai bagaimana Kriptografi menjadi garis pertahanan terakhir.

2. PEMBAHASAN MODUL (The Core Findings)

1. **Integritas Data & Hashing: "Sidik Jari Digital yang Tak Bisa Berbohong"**
(Relate to Module: Hashing / Integrity)

1. Pemahaman Standar: Hashing (MD5, SHA-256) mengubah data menjadi string acak tetap. Analisis Out-of-the-Box: Bayangkan kasus Deepfake Video Pejabat saat pemilu. Bagaimana cara membuktikan video itu asli atau palsu? Mata manusia bisa ditipu, tapi Hash Value tidak.

1. Studi Kasus: Digital Forensics. Jika satu bit pixel pada video bukti diubah, hash SHA-256 akan berubah total (Avalanche Effect).
2. Implementasi di Laporan: Tunjukkan screenshot dari TryHackMe saat Anda melakukan cracking hash atau verifikasi file, lalu hubungkan: "Hash bukan enkripsi, hash adalah segel garansi digital."

2. Kriptografi Simetris & Asimetris: "Dilema Kunci Rumah vs. Kunci Brankas Bank"



YAYASAN MEMAJUKAN ILMU DAN KEBUDAYAAN

UNIVERSITAS SIBER ASIA

Kampus Menara, Jl. RM. Harsono, Ragunan - Jakarta Selatan, Daerah Khusus Ibukota Jakarta 12550.
Telp. (+6221) 27806189. pmb@unsia.ac.id <https://unsia.ac.id>





1. Pemahaman Standar: Simetris (1 kunci), Asimetris (2 kunci: publik & privat).
2. Analisis Out-of-the-Box (Analogi Kreatif):
 1. Simetris (AES): Seperti kunci pintu hotel. Cepat dan efisien, tetapi jika resepsionis memberi kunci duplikat ke orang jahat, kamar Anda tidak aman. Ini yang terjadi pada kebocoran data internal.
 2. Asimetris (RSA/PGP): Seperti kotak pos. Siapapun (publik) bisa memasukkan surat ke kotak pos Anda, tapi hanya Anda (privat) yang punya kunci untuk membukanya.
3. Studi Kasus Aktual: End-to-End Encryption (E2EE) WhatsApp. Mengapa polisi sulit menyadap chat WA kriminal? Karena WA menggunakan protokol Signal (gabungan kurva eliptik/asimetris untuk pertukaran kunci di awal, lalu simetris untuk kecepatan chat).
4. Poin Kritis: Bahas bahwa keamanan bukan pada algoritamanya (RSA sudah kuat), tetapi pada Manajemen Kunci (di mana kunci disimpan? Di post-it note atau di HSM?).

3. Encoding vs Encryption: "Jangan Tertipu Topeng"

1. Analisis Kreatif: Banyak orang awam (dan developer ceroboh) mengira Base64 adalah pengamanan.
 2. Contoh Kasus: Seringkali password di database developer pemula hanya di-encode ke Base64. Ini sama seperti menyembunyikan uang di balik kaca transparan. Siapapun bisa melakukan decode.
 3. Kesimpulan: Encoding untuk usability (agar data biner bisa dikirim lewat teks), Enkripsi untuk confidentiality.
3. KESIMPULAN & REFLEKSI Kesimpulan: Kriptografi di TryHackMe mengajarkan bahwa tidak ada sistem yang 100% aman. Algoritma matematika mungkin sempurna, tetapi implementasi manusia sering cacat. Keamanan siber masa depan (Post-Quantum Cryptography) akan menjadi tantangan baru ketika komputer kuantum bisa memecahkan RSA dalam hitungan detik.

4.

-----*Selamat Mengerjakan, Jangan Lupa Berdoa*-----

| Diverifikasi Oleh: | | | Disusun Oleh: |
|---|--|---|---|
| Penjaminan Mutu | Ketua Program Studi | Koordinator Mata Kuliah | Dosen Pengampu |
|  (Abdu Rahman, S.E., M.Ak.) |  (Syahid Abdullah, S.Si., M.Kom) |  (Ambros Magnus Rudolf Mekeng, S.T., M.T.) |  (Abdul Azzam Ajhari, S.Kom., M.Kom.) |
| Disahkan Tanggal: 28-11-2025 | | | Dibuat Tanggal: 26-11-2025 |



YAYASAN MEMAJUKAN ILMU DAN KEBUDAYAAN

UNIVERSITAS SIBER ASIA

Kampus Menara, Jl. RM. Harsono, Ragunan - Jakarta Selatan, Daerah Khusus Ibukota Jakarta 12550.

Telp. (+6221) 27806189. pmb@unsia.ac.id <https://unsia.ac.id>
