Kriptografi

Pertemuan - 01

Topics: Kontrak, Pengertian, Jenis, Aplikasi, Contoh

Peraturan Praktikum

- Praktikan wajib mengikuti praktikum sesuai jadwal kelas masing-masing yaitu:
  Kelas A: Hari Rabu, pukul 10.15 - 12.15 WIB
  Kelas B: Hari Senin, pukul 13.00 - 15.00 WIB
- Praktikan **wajib mengumpulkan tugas** di G-Classroom
- Praktikan diharap dapat mengikuti praktikum dengan baik dan tidak melakukan kegiatan yang mengganggu jalannya praktikum
- Praktikan yang berhalangan hadir wajib memberi kabar H-1 ke Asprak
- Tidak diperbolehkan melakukan kecurangan dengan cara apapun saat ujian
- Aturan tambahan akan ditentukan di kemudian hari

Bobot Penilaian

UAS	30%
UTS	25%
Tugas	30%
Kuis	15%

Classroom

Kelas A

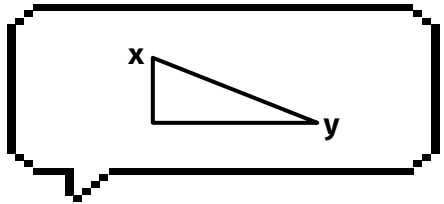
`n5sqo4i`

Kelas B

`57hnmak`

DISKORD

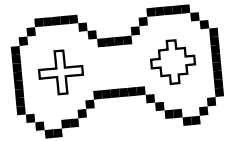
https://discord.gg/3pMkP7vA



01

Kriptografi??

Kriptografi??

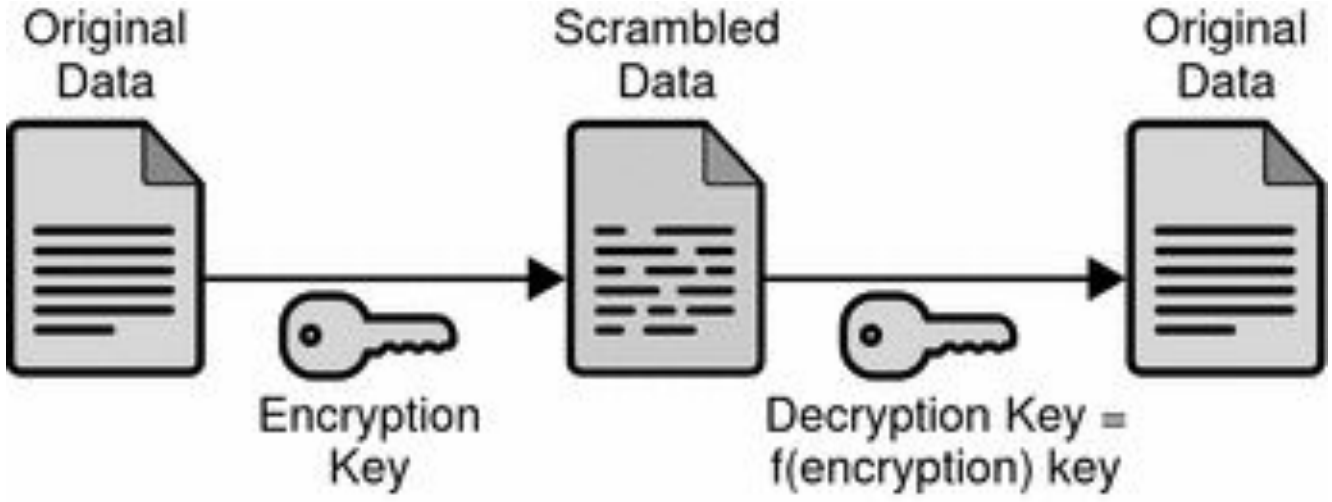


Kriptografi merupakan seni/ilmu/disiplin yang digunakan untuk menyembunyikan isi pesan dengan menggunakan teknik **enkripsi**.

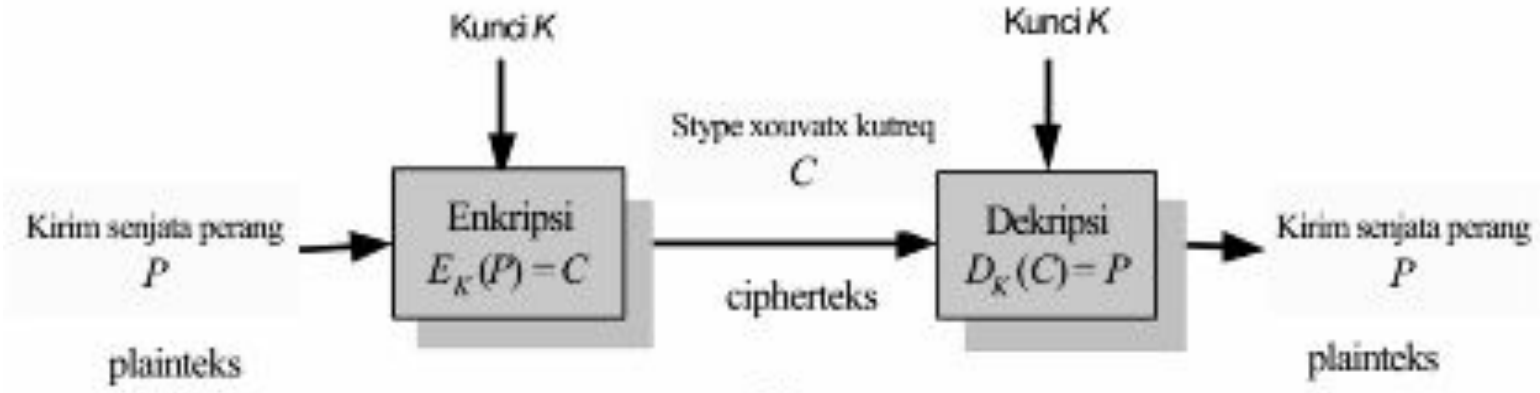
Biasanya berhubungan dengan “C” dan “I” pada konsep **CIA Triad (Confidentiality, Integrity, & Availability).**

Intinya, pada kriptografi, kita akan belajar cara **konstruksi dan analisis** sebuah **pesan/protokol** agar tidak bisa dibaca oleh **Unauthorized Party**.

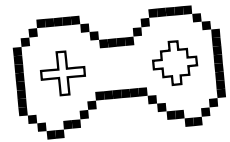
Proses


Original Data
Scrambled Data
Original Data
Encryption Key
Decryption Key = f(encryption) key

Proses


Kunci K
Kunci K
Stype xouvatx kutreq
C
Kirim senjata perang
P
Enkripsi
$E_K(P) = C$
cipherteks
Dekripsi
$D_K(C) = P$
Kirim senjata perang
P
plainteks
plainteks

Common Terms



Plain Text: Human-readable text, yang akan dienkripsi.

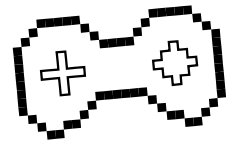
Cipher Text: Non-readable text, hasil dari enkripsi.

Encryption: Plain Text → Cipher Text.

Decryption: Cipher Text → Plain Text.

Key: Kunci yang digunakan untuk enkripsi atau dekripsi.

Tujuan Kriptografi



Security: Mengamankan komunikasi, data (in transit, at rest, in process).

Confidentiality: Menjaga kerahasiaan dari sebuah informasi.

Integrity: Menjaga integritas data (HMAC, Hashing, dsb.).

Autentikasi: Identifikasi dan pengecekan kebenaran identitas seseorang.

Non-Repudiasi: Mencegah penyangkalan dari data atau informasi yang ditukar oleh setiap pihak.

404 NOT FOUND

02

Jenis & Aplikasi Kriptografi

Ada apa aja sih jenis-jenisnya??

Klasik vs Modern

Klasik

Bermain langsung dengan **karakter**, **simple**, tidak memerlukan bantuan komputer, **metode dan sistem yang digunakan rahasia**, **tidak aman**.

Modern

Bermain dengan **bit (umumnya ASCII)**, **kompleks**, perlu bantuan komputer, **algoritma boleh publik**, tetapi **key harus rahasia**, **lebih aman** (tetapi **tidak selalu foolproof**).

Stream vs Block

Stream Cipher

One byte at a time (8 bits), Plain Text dibagi ke **beberapa byte** sebelum di encrypt, **lebih kompleks** dari block, Cipher Text **lebih mudah di reverse**.

Block Cipher

One block at a time (64 bits), Plain Text dibagi ke **beberapa block** sebelum di encrypt, **lebih simple** dari stream, Cipher Text **lebih sulit untuk di reverse**.

Symmetric vs Asymmetric

Symmetric

Enkripsi dan Dekripsi menggunakan **kunci yang sama**, biasanya dengan **Pre-Shared Key (PSK)**, disebut juga sebagai **Same Key Cryptography**.

Asymmetric

Enkripsi dan Dekripsi menggunakan **kunci yang berbeda**, salah satu kunci bersifat **Public**, dan satunya bersifat **Private**, disebut juga sebagai **Public Key Cryptography**.

Contoh Aplikasi??

Smart Card

Transaksi Bank / ATM

End-to-End Encryption WA

Login ke Website

Message Integrity Check

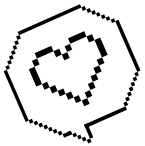
Dan Masih Banyak Lagi!!

Algoritma??

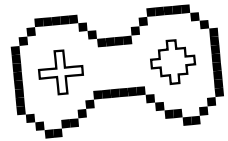
Caesar/Shift, Hill, Affine, ROT13, Vigenere, Autokey, Permutasi, Rail Fence, Elgamal, Rivest-Shamir-Adleman (RSA), Advanced Encryption Standard (AES), DES, S-DES, 3DES, Elliptic Curve Cryptography (ECC), Menezes-Vanstone, Diffie-Hellman, MD5, RIPEMD, SHA, CRC, HMAC, dan masih banyak lagi...

Kriptografi itu penting!!

Walau kalian ga bergerak di bidang keamanan, orang IT yang baik **harus tahu cara mengamankan data**, dan kriptografi adalah salah satu cara utamanya.



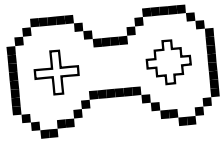
Tugas



1. Cari penjelasan dan perbedaan lebih lanjut terkait perbedaan kriptografi Klasik dan Modern, termasuk jenis/tipe dari masing-masing kriptografi!
2. Cari 3 (atau lebih) contoh lain dari aplikasi/penerapan kriptografi, dan jelaskan secara singkat peran dan logika kriptografi dalam penerapan tersebut! **(Selain yang sudah disebutkan di slide sebelumnya)**
3. Cari contoh algoritma kriptografi klasik dan 1 contoh algoritma modern, lalu berikan penjelasan singkatnya!
4. Pilih algoritma dari slide 16, coba eksplorasi terkait algoritma tersebut, lalu tuliskan penjelasan hasil eksplorasi kalian!

Format: Tugas1_NPM.pdf

Deadline: H-1 Praktikum Berikutnya



Thank You!!

Kalau misalkan ada pertanyaan,
yaudah tanya aja

Praktikum Kriptografi 2022