ENKRIPSI ASIMETRIS

SOLUSI AMAN UNTUK DUNIA DIGITAL

Enkripsi Asimetris adalah metode enkripsi yang menggunakan sepasang kunci:

- **Kunci Publik, yang dibagikan secara terbuka untuk enkripsi atau verifikasi tanda tangan**
- **Kunci Privat, yang dirahasiakan pemiliknya untuk dekripsi atau pembuatan tanda tangan**

Perbedaan utama dengan enkripsi simetris adalah tidak perlu membagikan kunci rahasia. Pengirimnya hanya butuh kunci publik penerima untuk mengirim pesan aman.

CARA KERJA:

Pembuatan Kunci
Pasangan kunci (publik dan privat) dibuat dengan algoritma kriptografi asimetris.

Enkripsi
Data yang dienkripsi menjadi ciphertext, yang tidak dapat dibaca tanpa kunci dekripsi yang sesuai.

Pengiriman Data
Ciphertext dikirimkan kepada penerima melalui saluran komunikasi yang tidak aman.

Dekripsi
Penerima menggunakan kunci privatnya untuk mendekripsi ciphertext.

CONTOH PENGGUNAAN ENKRIPSI ASIMETRIS

Website Aman (HTTPS)
Saat membuka situs https:// browser dan server saling bertukar kunci publik dan privat. Ini melindungi data saat mengetik password, transaksi, atau isi formulir.

Tanda Tangan Digital
Saat menandatangani dokumen secara elektronik, penandatangan menggunakan kunci privat, dan penerima/sistem bisa mengecek keasliannya dengan kunci publik.

Email Terenkripsi (PGP atau GPG)
Jika mengirim email penting dan rahasia, bisa melakukan mengenkripsi pesan menggunakan kunci publik penerima dan hanya penerima yang bisa membacanya, karena hanya dia yang punya kunci privat.

KELEBIHAN

- **Tidak Perlu Pertukaran Kunci Rahasia**
- **Keamanan yang Lebih Kuat**
- **Enkripsi asimetris tidak hanya digunakan untuk kerahasiaan, tetapi juga untuk otentikasi dan tanda tangan digital.**
- **Dengan otentikasi, pesan berhasil didekripsi menggunakan kunci publiknya.**
- **Enkripsi memungkinkan pengirim untuk menandatangani dokumen secara digital.**

KEKURANGAN

- **Algoritma enkripsi asimetris jauh lebih kompleks secara matematis dibandingkan algoritma simetris.**
- **Kunci asimetris biasanya berukuran lebih besar (misalnya, 2048 bit atau 4096 bit).**
- **Meskipun kuncinya berbeda, ada potensi serangan di mana penyerang dapat menyusup di antara dua pihak dan memanipulasi pertukaran kunci publik.**

DISKOMINFOS PROVINSI BALI
PROGRAM LITERASI KESADARAN KEAMANAN SIBER
Ingin mendapatkan informasi terbaru dan konten literasi keamanan siber ?
Ayo berlangganan KABAR LENTERA (GRATIS !) di https://balikom.info/kabarlentera

SECURITY IS INCOMPLETE WITHOUT U
#JagaRuangSiber
LENTERA SIBER
SAYA NETIZEN CERDAS

DISKOMINFOS.BALIPROV.GO.ID | diskominfosbali | diskominfos_bali | lenterasiber | balikom.info/link/lenterasiber
TLP: CLEAR

Balai Besar Sertifikasi Elektronik
Dokumen ini telah ditandatangani secara elektronik menggunakan sertifikat elektronik yang diterbitkan oleh BSrE

BANGGA BUATAN INDONESIA
BANGGA BERWISATA DI INDONESIA