**Kriptografi dan Enkripsi-Deskripsi**

Kriptografi adalah ilmu yang mempelajari teknik untuk mengamankan informasi, seperti menjaga kerahasiaan, integritas, dan keaslian data. Dalam materi ini, kita fokus pada hashing dan enkripsi (simetris dan asimetris).

**1. Hashing**

Hashing adalah proses mengubah data (teks, file, dll.) menjadi string dengan panjang tetap (hash) menggunakan algoritma khusus. Hash ini seperti sidik jari digital: unik untuk setiap input, tetapi tidak bisa diubah kembali ke data asli (sifat satu arah).

**SHA-256**

* **Apa itu?** SHA-256 (Secure Hash Algorithm 256-bit) adalah bagian dari keluarga SHA-2, yang dianggap aman untuk saat ini. Digunakan untuk memverifikasi integritas data, misalnya memastikan file yang diunduh tidak diubah.
* **Cara Kerja**:
  + Input: Data apa pun (teks, file, dll.).
  + Output: String 64 karakter (256-bit) dalam format heksadesimal.
  + Jika data sedikit saja berubah, hash-nya akan sangat berbeda.
* **Keamanan**: Sangat aman, tahan terhadap serangan kolisi (dua input berbeda menghasilkan hash sama).

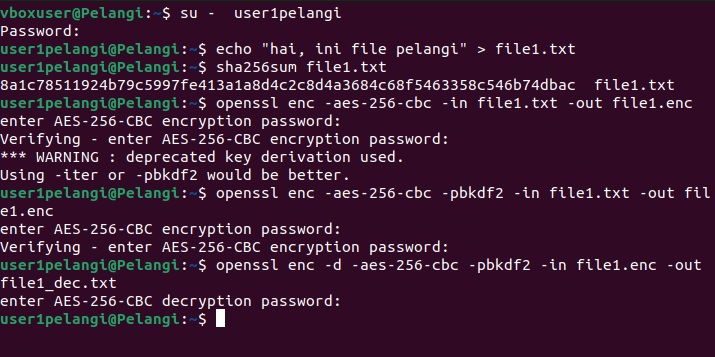
**MD5**

* **Apa itu?** MD5 (Message Digest 5) adalah algoritma hash yang menghasilkan hash 128-bit (32 karakter heksadesimal).
* **Mengapa Tidak Aman?** MD5 rentan terhadap serangan kolisi, di mana penyerang bisa membuat dua file berbeda dengan hash yang sama. Karena itu, **jangan gunakan MD5 untuk keamanan** seperti menyimpan kata sandi.
* **Penggunaan**: Hanya untuk verifikasi integritas sederhana (misalnya, checksum file) di lingkungan yang tidak kritis.
* **Catatan**: Gantikan MD5 dengan SHA-256 atau SHA-3 untuk keamanan.

**Uji Coba**

sha256sum: Perintah di Linux untuk menghitung hash SHA-256.

File1.txt: File yang akan di-hash.



**2. Enkripsi**

Enkripsi mengubah data menjadi bentuk yang tidak dapat dibaca (ciphertext) tanpa kunci yang tepat. Ada dua jenis utama: simetris dan asimetris.

**Symmetric Encryption: AES**

* **Apa itu?** AES (Advanced Encryption Standard) adalah algoritma enkripsi simetris yang menggunakan kunci yang sama untuk enkripsi dan dekripsi. AES-256 (kunci 256-bit) adalah varian yang sangat aman.

**Cara Kerja**:

* Input: Data (plaintext) dan kunci.
* Output: Ciphertext (data terenkripsi).
* Mode: Dalam latihan, kita menggunakan **CBC (Cipher Block Chaining)**, yang menambahkan lapisan keamanan dengan mengaitkan setiap blok data.

**Penggunaan**: Mengenkripsi file, disk, atau komunikasi (misalnya VPN, HTTPS).

**Keunggulan**: Cepat dan efisien untuk data besar.

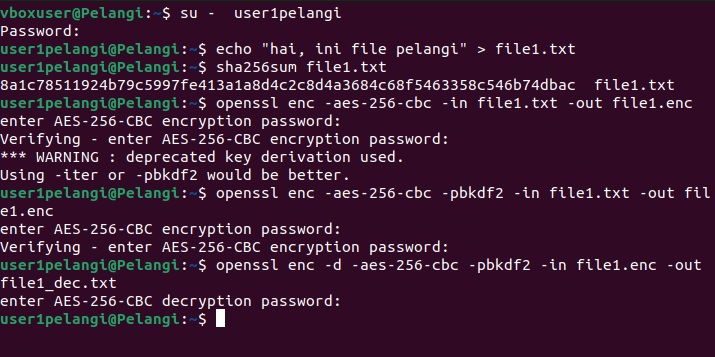
**Kekurangan**: Kunci harus dibagikan dengan aman kepada penerima.

**Asymmetric Encryption: RSA**

* **Apa itu?** RSA (Rivest-Shamir-Adleman) adalah algoritma enkripsi asimetris yang menggunakan dua kunci: kunci publik (untuk enkripsi) dan kunci privat (untuk dekripsi).
* **Cara Kerja**:
  + Kunci publik disebarkan secara bebas, kunci privat dirahasiakan.
  + Data yang dienkripsi dengan kunci publik hanya bisa didekripsi dengan kunci privat.
* **Penggunaan**: Pertukaran kunci, tanda tangan digital, atau enkripsi data kecil (karena RSA lebih lambat daripada AES).
* **Keunggulan**: Tidak perlu berbagi kunci rahasia.
* **Kekurangan**: Lambat untuk data besar, biasanya digunakan bersama AES.

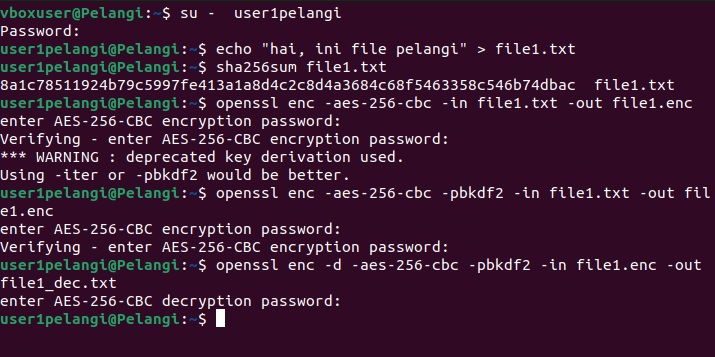
**Uji coba**

Enkripsi File dengan OpenSSL (AES-256-CBC)



* openssl enc: Perintah untuk enkripsi menggunakan OpenSSL.
* -aes-256-cbc: Menggunakan algoritma AES-256 dengan mode CBC.
* -in file1.txt: File input (plaintext).
* -out file1.enc: File output (ciphertext).
* Saat dijalankan, OpenSSL akan meminta kata sandi. Kata sandi ini digunakan untuk menghasilkan kunci enkripsi.
* **WARNING : deprecated key derivation used :** OpenSSL memberi peringatan bahwa metode derivasi kunci yang digunakan (default OpenSSL) sudah usang.
* **"Using -iter or -pbkdf2 would be better."**: Disarankan untuk menggunakan opsi -iter (untuk iterasi tambahan) atau -pbkdf2 (Password-Based Key Derivation Function 2) untuk meningkatkan keamanan kunci yang dihasilkan dari kata sandi.

Dekripsi:



* **Penjelasan**: Mendekripsi file1.enc kembali ke file1.txt menggunakan kata sandi yang sama. Opsi -d menandakan dekripsi.
* **Catatan**: Jika kata sandi salah, dekripsi akan gagal.