Digital Signature

Oleh :

Harry Witriyono, M.Kom
NIDN. 0210126903

Fakultas Teknik UM Bengkulu

Apa itu Digital Signature

- Digital Signature adalah proses penandaan dan pemenuhan aspek keamanan data secara digital dengan menggunakan algoritma tertentu.
- Aspek yang harus dipenuhi dalam suatu tanda tangan digital :
  - Confidentiality
  - Data Integrity
  - Authentication
  - Non Repudiation

Cara Digital Signature

- Digital signature / tanda tangan digital dilakukan dengan dua cara :
  - Enkripsi – Dekripsi Pesan / Dokumen Digital
  - Penggunaan Fungsi Hash.
- Pesan yang telah terenkripsi menandakan bahwa pesan tersebut telah ditandatangani dan otentik karena kedua pihak mengetahui kuncinya.
- Tanda tangan digital dengan fungsi hash bisa jadi tidak membutuhkan kerahasiaan tetapi hanya otentikasi pesan bagi ke dua pihak.

Konsep Tanda Tangan Digital / Digital Signature

- Tanda tangan adalah bukti yang otentik
- Tanda tangan tidak dapat dilupakan
- Tanda tangan tidak dapat dipindah untuk digunakan ulang
- Dokumen yang telah ditanda tangan tidak dapat diubah.
- Tanda tangan tidak dapat disangkal.

Tanda Tangan Digital Dengan Enkripsi Kunci Simetri

- Konsep enkripsi kunci simetri sudah merupakan bentuk dari tanda tangan digital karena ada otentikasi dari kunci yang dimiliki oleh kedua pihak pengirim dan penerima pesan, permasalahannya adalah pada aspek non repudiation / penyangkalan.
- Untuk mengatasi masalah nor repudation pada digital signature maka diperlukan arbitrase / penengah yang dipercaya oleh kedua pihak dan memvalidasi kebenaran data yang berasal atau diterima kedua pihak.
- Konsepnya pesan chipertext divalidasi oleh arbitrase dengan menambah pernyataan keabsahan berdasarkan kunci simetri yang disepakai pengirim pesan dengan arbitrase lalu dienkripsi kembali pesan dan pernyataan keaslian tadi dengan kunci simetri yang disepakati oleh arbitrase dengan penerima pesan.

Digital Signature dengan Kunci Publik

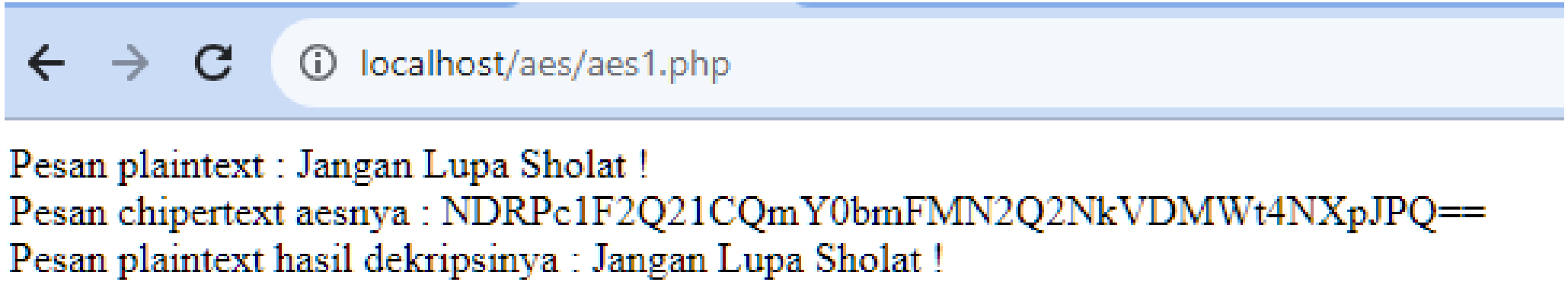
- Diffle dan Hellman menyatakan bahwa digital signature dengan kunci publik hanya dapat dilakukan bila enkripsi pesan dengan kunci private pengirim dan dekripsi menggunakan kunci publik pengirim.
- Bila menggunakan kunci publik, maka aspek otentikasi tidak bisa diterapkan karena semua orang mempunyai kunci publiknya.

Sesi Praktikum Otentikasi Pesan Dengan Enkripsi AES pada PHP

Untuk melaksanakan praktikum ini anda butuh server apache dan server basisdata MySQL.

Latihan 1. AES1.php

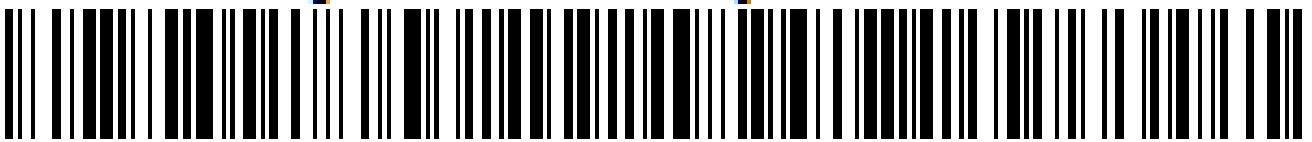
- File ini mencontohkan secara sederhana proses enkripsi dan dekripsi AES dengan algoritma AES-128-CTR
- Source codenya dapat dilihat di : https://github.com/HarryWitriyono/simpelaes/blob/main/aes1.php
- Hasilnya :



Tugas Latihan 2. Terapkan pada barcode

- Silahkan anda coba buat sehingga hasilnya seperti tampilan berikut ini:

Pesan pada barcode :Harry W.1311094102
Hasil enkrip dan barcodenya :



4YOwV+joc3W83vLqFP/fVgh3

Number:4YOwV+joc3W83vLqFP/fVgh3
Harry W.1311094102

Sumber Rujukan

- PHP OpenSSL : https://www.php.net/manual/en/function.openssl-encrypt.php
- PHP Algoritma lihat di : https://www.php.net/manual/en/function.openssl-get-cipher-methods.php