	PROGRAM STUDI LOGISTIK NIAGA EL	No Dok : FRM-AKD-002
		Tanggal Efektif : 5 Februari 2024
	MODUL PRAKTIKUM	No Rev : 00
		Halaman : Page of




**MODUL PRAKTIKUM
EL424 – KEAMANAN DATA & INFORMASI**

oleh

Januar Wahjudi

**Program Studi Logistik Niaga Elektronik
Politeknik Multimedia Nusantara
Tangerang, Banten
2024**

	PROGRAM STUDI LOGISTIK NIAGA EL	No Dok : FRM-AKD-002
		Tanggal Efektif : 5 Februari 2024
	MODUL PRAKTIKUM	No Rev : 00
		Halaman : Page of

**MODUL PRAKTIKUM
EL424 – KEAMANAN DATA & INFORMASI
“PERTEMUAN KE-9”**

STANDAR KOMPETENSI

CPMK3 - Mahasiswa mampu memahami konsep dan cara kerja keamanan jaringan, malware, social engineering (C2)

KOMPETENSI DASAR

Sub-CPMK Mahasiswa mampu memahami konsep dan cara kerja keamanan jaringan, malware, social engineering (C2)

INDIKATOR

- Ketepatan waktu penyelesaian tugas
- Ketepatan solusi atas tugas

A. DASAR TEORI

DSA (Digital Signature Algorithm) & RSA (Rivest-Shamir-Adleman)

Keduanya sama-sama algoritma kriptografi yang dapat digunakan untuk tanda tangan digital (digital signature) dan enkripsi. Berikut ini perbandingan kedua algoritma tersebut :

1. DSA adalah algoritma khusus tanda tangan dan butuh kunci privat untuk penandatanganan dan kunci publik untuk verifikasi.
2. RSA adalah dapat digunakan untuk tanda tangan digital dan enkripsi.
3. DSA lebih cepat dan lebih mudah diimplementasikan daripada RSA.
4. DSA lebih aman daripada RSA karena memberikan integritas dan non-repudiation pesan.
5. RSA rentan dan butuh lebih banyak daya komputasi.


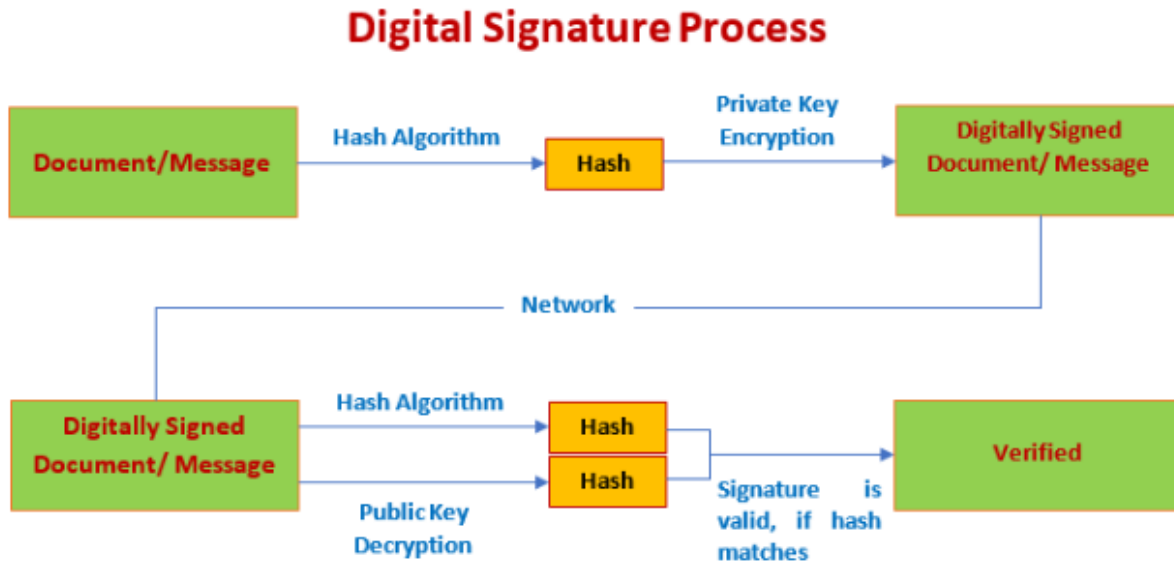
	PROGRAM STUDI LOGISTIK NIAGA EL	No Dok : FRM-AKD-002
		Tanggal Efektif : 5 Februari 2024
	MODUL PRAKTIKUM	No Rev : 00
		Halaman : Page of

Diagram alur proses DSA



Referensi :

<https://www.simplilearn.com/tutorials/cryptography-tutorial/digital-signature-algorithm>
<https://www.javatpoint.com/java-digital-signature>

B. TUJUAN PRAKTIKUM

1. Mahasiswa memahami konsep cryptography asimetri
2. Mahasiswa memahami DSA Algorithm

C. ALAT DAN BAHAN


1. Komputer
2. Website : <https://8gwifi.org/dsafunctions.jsp>

D. LANGKAH KERJA PRAKTIKUM

- mempelajari DSA untuk digital signature
- uji coba DSA

E. LATIHAN

- Tidak ada


	PROGRAM STUDI LOGISTIK NIAGA EL	No Dok : FRM-AKD-002
		Tanggal Efektif : 5 Februari 2024
	MODUL PRAKTIKUM	No Rev : 00
		Halaman : Page of

F. TUGAS

1. Beri penjelasan tentang DSA dan cara kerja DSA untuk digital signature.
2. Jelaskan perbedaan DSA dan RSA untuk digital signature !
3. Tuliskan dan capture layar tampilan uji coba DSA (<https://8gwifi.org/dsafunctions.jsp>)

Ketiklah jawaban dan simpan dalam bentuk file **NIM_Nama_Prak9.docx**

PENGESAHAN

PROSES	PENANGGUNG JAWAB		Tanda Tangan
	Nama	Jabatan	
Issued by	Dewi Hajar	Kaprodi Logistik Niaga El	
Reviewed by			
Approved by			
Controlled by			