	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-7”**

### STANDAR KOMPETENSI

CPMK1 - Mahasiswa mampu memahami konsep dasar keamanan data dan informasi, security risk (C2)

### KOMPETENSI DASAR

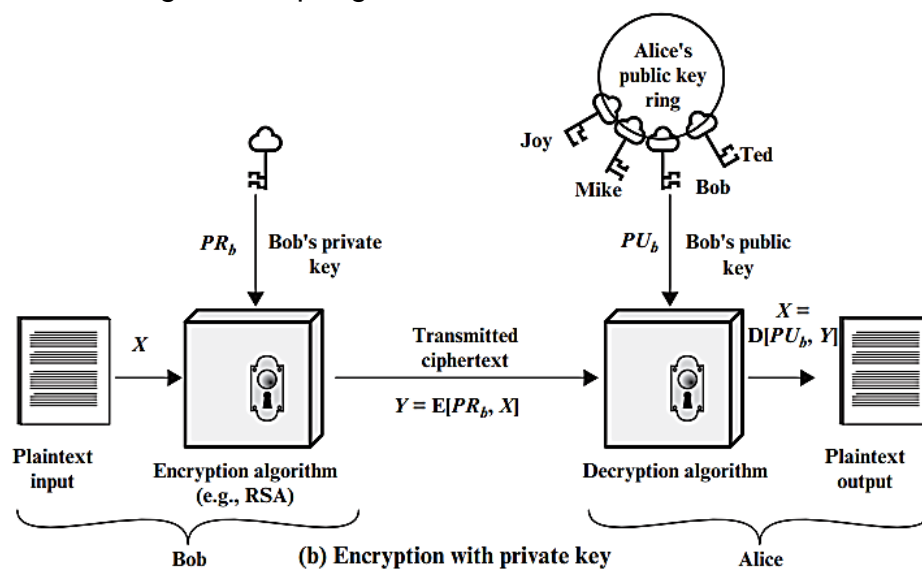
Sub-CPMK1 Mahasiswa mampu memahami konsep dasar keamanan data dan informasi, security risk (C2)

### INDIKATOR


- Ketepatan waktu penyelesaian tugas
- Ketepatan solusi atas tugas

### A. DASAR TEORI

Algoritma enkripsi asimetrik menggunakan sepasang kunci yang berbeda, yaitu kunci publik untuk melakukan enkripsi, dan kunci private untuk melakukan dekripsi. Salah satu algoritma enkripsi asimetrik adalah RSA (Rivest-Shamir-Adleman). Selain untuk mengenkripsi pesan rahasia, dapat digunakan juga untuk tandatangan digital. Pesan di enkripsi menggunakan private key pengirim, dan proses dekripsi dilakukan penerima menggunakan public key pengirim dengan tujuan untuk memastikan bahwa pesan atau dokumen benar telah ditandatangani secara digital oleh pengirim.



*Skema Kriptografi Kunci Publik (Stalling, 2017)*

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

### Langkah Enkripsi dan Dekripsi saat pengiriman pesan :

1. Sebelum Bob melakukan enkripsi, Bob membangkitkan sepasang kunci (kunci privat dan kunci publik) miliknya dengan memanggil fungsi **PembangkitKunci**. Bob mempublikasikan kunci publik  $K_{pub}$ , namun tetap menjaga kerahasiaan kunci privat  $K_{pv}$  :  $(K_{pub}, K_{pv}) \leftarrow \text{PembangkitKunci}$
2. Bob mengenkripsi sebuah teks asli ( $M$ ) dengan kunci publik Bob ( $K_{pv}$ ) menghasilkan sebuah teks sandi ( $C$ ) dengan digital signature Bob sesuai teks yang dikirimkan dengan memanggil fungsi **Enkripsi** :  $C \leftarrow \text{Enkripsi}(K_{pv}, M)$
3. Bob mengirim teks sandi  $C$  ke Alice melalui saluran tidak aman.
4. Alice mendekripsi teks sandi ( $C$ ) dengan kunci public Bob ( $K_{pub}$ ) untuk memeriksa keaslian teks dari Bob, serta mendapatkan teks asli  $M$  dengan fungsi **Dekripsi** :  $M \leftarrow \text{Dekripsi}(K_{pub}, C)$
5. Alice mendapatkan teks asli ( $M$ ) jika teks sandi ( $C$ ) dienkripsi dengan kunci publik Bob.

Pelajari lebih dalam dengan uji coba melalui link simulasi berikut :

<https://www.devglan.com/online-tools/rsa-encryption-decryption>

### B. TUJUAN PRAKTIKUM

1. Mahasiswa memahami konsep cryptography kunci publik (asimetri)
2. Mahasiswa memahami RSA Algorithm

### C. ALAT DAN BAHAN

1. Komputer
2. Website : <https://www.devglan.com/online-tools/rsa-encryption-decryption>

### D. LANGKAH KERJA PRAKTIKUM


- mempelajari RSA Algorithm untuk digital signature
- uji coba RSA Algorithm

### E. LATIHAN

- Tidak ada

### F. TUGAS

1. Beri penjelasan tentang RSA Algorithm untuk digital signature.
2. Silahkan lakukan simulasi saling berkirim pesan yang telah ditandatangani bersama teman sebelah Anda. Tuliskan dan capture layar tampilan uji coba RSA Algorithm (gunakan

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

simulator dari <https://www.devglan.com/online-tools/rsa-encryption-decryption>). Lakukan peran bergantian sebagai berikut dan tuliskan langkah-langkahnya jika :

- a. Anda sebagai pengirim pesan (lakukan enkripsi), teman Anda sebagai penerima pesan (lakukan dekripsi)
  - b. Teman Anda sebagai pengirim pesan (lakukan enkripsi), Anda sebagai penerima pesan (lakukan dekripsi)
3. Ketiklah jawaban dan simpan dalam bentuk file **NIM\_Nama\_Prak7.docx**

## PENGESAHAN

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