UNIVERSITAS KEBANGSAAN REPUBLIK INDONESIA
UJIAN AKHIR SEMESTER
Tahun Akademik 2025-2026

Nama Mata Kuliah	: **KRIPTOGRAFI**
Program Studi	: Teknik Informatika
Dosen	: Deni Suprihadi, S.T, M.KOM, MCE
Waktu	: 4 Hari
Sifat Ujian	: **TAKE-HOME TEST (PROJEK)**

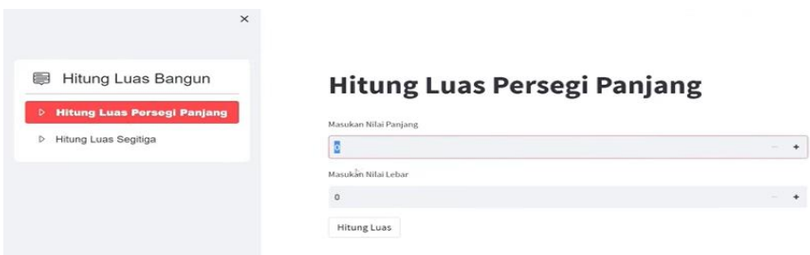
Ketentuan Ujian :

- Kerjakan soal-soal di bawah ini dengan rapih, baik dan benar
- Sifat ujian adalah **TAKE-HOME (Laptop / Netbook)**
- **TIDAK BOLEH** saling meminjamkan NOTE saat pelaksanaan UAS.

BACA dan PAHAMI dahulu Soal-soal dibawah ini sebelum memberikan Jawaban !

Seiring dengan meningkatnya kebutuhan akan keamanan dan keaslian data dalam sistem digital, **digital signature dan QRIS** menjadi salah satu mekanisme penting untuk menjamin **integritas, autentikasi, dan non-repudiation** suatu pesan. Salah satu algoritma kriptografi kunci publik yang umum digunakan untuk digital signature adalah **RSA (Rivest–Shamir–Adleman)**.
Sebuah institusi ingin membuat **verifikasi dokumen digital** yang dapat digunakan untuk menandatangani dan memverifikasi pesan secara digital menggunakan **Python** dan **dideploy menggunakan framework Streamlit** agar mudah diakses dan menghasilkan tampilan yang menarik. Dengan ketentuan sebagai berikut :

1. Buatlah **pasangan kunci RSA (public key dan private key)** untuk pengirim pesan, kemudian pesan asli di-*hash* terlebih dahulu menggunakan algoritma hash (misalnya SHA-256).
2. Lakukan Enkripsi pada Nilai hash tersebut menggunakan **private key RSA** untuk menghasilkan **digital signature** dalam bentuk QRIS.
3. Lakukan verifikasi dengan cara mendekripsi signature menggunakan **public key RSA** dan membandingkannya dengan hash pesan yang diterima pada penerima pesan.
4. Lakukan Deploy agar **tampilan menarik** terhadap Algoritma yang sudah dibuat pada No.1 sampai dengan No.3 menggunakan Streamlit dengan skenario menampilkan **antarmuka pengiriman pesan** yang menghasilkan **digital signature dan QRIS,** kemudian menampilkan **antarmuka penerima pesan** digital signature dalam bentuk QRIS, sehingga (**menampilkan isi pesan dan signature**)



Contoh Antar Muka berbasis Streamlit

Note :

- ✓ Semua Fungsi yang dibuat diawali dengan NPM, sebagai contoh : 2021232_save_enkrip, 20211232_tampilkan, dan seterusnya.
- ✓ Submit dokumentasi kode dan Antarmuka dalam bentuk PDF dengan Nama File : Jawab_UAS_KRIPTO_NPM.pdf, serta File Kode Streamlit.

***** Jangan Lupa Berdoa sebelum mengerjakan soal- !! *****