KEMENTERIAN PENDIDIKAN TINGGI, SAINS, DAN TEKNOLOGI
UNIVERSITAS NEGERI SURABAYA
FAKULTAS MATEMATIKA DAN ILMU PENGETAHUAN ALAM
PROGRAM STUDI S1 SAINS DATA

Kampus Unesa 1 Ketintang, Gedung E2, Surabaya 60231
Laman: https://datascience.fmipa.unesa.ac.id, Email: datascience@unesa.ac.id

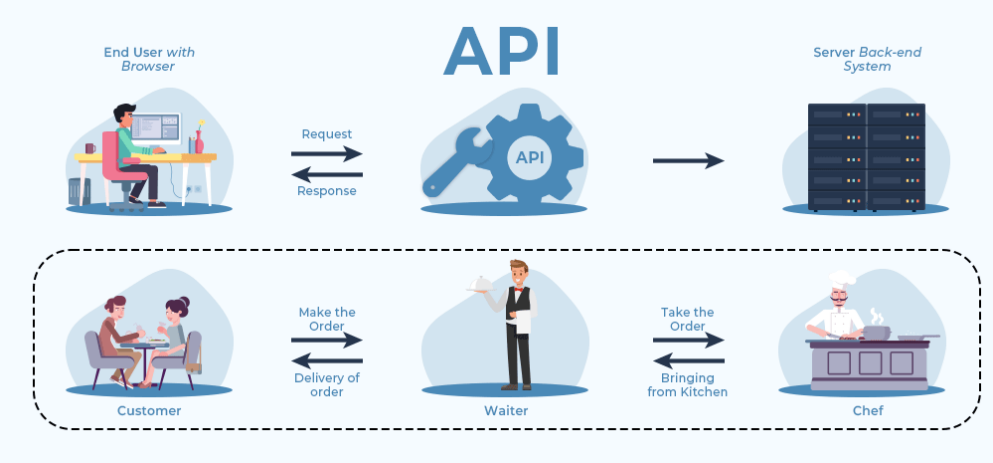
NASKAH UJIAN AKHIR
SEMESTER GASAL TAHUN AKADEMIK 2025/2026

Matakuliah	:	Keamanan dan Integritas Data
Prodi	:	S1 Sains Data
Kelas	:	2024
Tanggal	:	**7-18 Desember 2025 23:59**
Dosen	:	TIM
Materi	:	Layanan Kriptografi API
Sifat	:	Terbuka, Kelompok, Presentasi
Versi dokumen	:	6/12/2025

1. Petunjuk dan Ketentuan

1. Aktivitas ini dilakukan berkelompok beranggotakan **3-4** orang.
2. Perwakilan kelompok **wajib** mengunggah pekerjaan di LMS SINDIG Minggu ke-16
3. Setiap mahasiswa wajib mengisi penilaian rekan sejawat pada formulir berikut.

2. Latar Belakang



Gambar 1: Ilustrasi API (Sumber: Geek-For-Geek)

Menurut Kamus Oxford, API is a set of functions and procedures allowing the creation of applications that access the features or data of an operating system, application, or other service. API merupakan sekumpulan fungsi dan prosedur yang memfasilitasi pembuatan aplikasi yang memberikan akses ke fitur-fitur atau data dari sebuah sistem operasi, aplikasi, ataupun layanan lain. Menurut AWS[1], API merupakan mekanisme yang memungkinkan komponen-komponen dari dua perangkat lunak berkomunikasi satu dengan lainnya menggunakan sebuah himpunan definisi dan protokol. Sebagai contoh, sistem perangkat lunak agen cuaca berisi data cuaca harian. Aplikasi cuaca pada ponsel kita akan "berbicara" pada sistem ini melalui API dan menunjukkan update cuaca harian.

Pada evaluasi kali ini, Tim Anda diminta untuk mendemonstrasikan kemampuan implementasi pustaka pemrograman dalam menjamin keamanan dan keutuhan data melalui layanan API sederhana. Layanan API sederhana tersebut mensimulasikan proses-proses bisnis sederhana melalui pihak ketiga. Tim Anda akan melengkapi fungsi-fungsi skeleton yang disediakan. Fungsi-fungsi skeleton yang lengkap ini diibaratkan sebuah miniatur "trusted authority server". Keberadaan pihak ketiga ini bisa menjadi "asylum" dalam hal keamanan, karena memberikan dukungan ekstra atas pemeriksaan konten keamanan.

[1] https://aws.amazon.com/what-is/api/

KEMENTERIAN PENDIDIKAN TINGGI, SAINS, DAN TEKNOLOGI
UNIVERSITAS NEGERI SURABAYA
FAKULTAS MATEMATIKA DAN ILMU PENGETAHUAN ALAM
PROGRAM STUDI S1 SAINS DATA

Kampus Unesa 1 Ketintang, Gedung E2, Surabaya 60231
Laman: https://datascience.fmipa.unesa.ac.id, Email: datascience@unesa.ac.id

3. Deskripsi Pekerjaan: `Punk Records-v1`

Tim Anda bekerja untuk Vegapunk, seorang ilmuwan jenius yang memiliki fasilitas laboratorium canggih di pulau Egghead. Operasional lab bergantung pada keamanan dan integritas data pada database utama Vegapunk, yaitu Punk Records. Punk Records dapat menerima dan mengirim data antar peneliti laboratorium. Vegapunk ingin meningkatkan keamanan fasiltas tersebut dengan mengimplementasikan teknik-teknik kriptografi sederhana melalui API.

Secara umum, layanan yang dibutuhkan `Punk Records-v1` adalah sebagai berikut:

1. Menyimpan public key dari para peneliti Egghead.
2. Melakukan verifikasi signature dari suatu pesan yang dipertukarkan oleh peneliti.
3. Melakukan proses relay pesan aman antar 2 peneliti.

Tugas Tim Anda adalah merealisasikan permintaan Vegapunk tersebut menggunakan suatu aplikasi, khususnya dengan library FastAPI. Kerangka project tersebut dapat diunduh pada URL berikut: https://bit.ly/proj-kid-25. Adapun deskripsi konten file `kid-uas.zip` adalah sebagai berikut:

1. `pyproject.toml` dan `uv.lock`: File konfigurasi project dengan `uv` project manager[2] (lihat di sini).
2. `Readme.md`: Deskripsi, instalasi, dan cara penggunaan FastAPI dengan `uv` project manager ⇐ WAJIB BACA.
3. Folder `punkhazard-keys`: Berisi private dan public keys server. Anda boleh menggantikan ini dengan key Anda.
   - `priv.pem` dan `pub.pem`: Algoritma EC, Curve: SECP256K1.
   - `priv19.pem` dan `pub19.pem`: Algoritma ED25519.

Dengan `uv`, Anda cukup menggunakan perintah berikut untuk menjalankan file python:

```
uv run <nama-file-python.py>
```

tanpa perlu mengaktifkan virtual environment dan mengetikkan `python` di depan nama file.

4. The Challenge and Score

Bagian ini berisi daftar pekerjaan yang wajib dan opsional tim Anda selesaikan. Pekerjaan wajib (*mandatory tasks*) menjadi baseline penilaian akhir; sedangkan opsional (*optional tasks*) menjadi nilai tambah pekerjaan.

Table 1: Aspek Pekerjaan dan Grade Penilaian (Bobot: 80% nilai akhir)

York (Skor: E)		**Edison (B-)**		**Pythagoras (B+)**		**Stella (A)**
Aspek pekerjaan	Jalan	Static entry	Integrity check	Variasi cipher	Multiuser	Secure session
Simpan public key	☐	☐	☐	☐	☐	☐
Verifikasi signature	☐	☐	☐		☐	☐
Relay message	☐	☐	☐			☐
Tandatangan pdf	☐			☐	☐	☐

Petunjuk:
Static entry: Hanya terbatas pada entri user yang di-hardcode.
Integrity check: Ada pemeriksaan integritas data pokok pekerjaan yang dimaksud.
Variasi cipher: Penggunaan cipher (algoritma enkripsi) selain template, juga asymmetric ⇔ symmetric.
Multiuser: Menyimpan entri dari beberapa user dan menggunakan sesuai dengan kebutuhan.
Secure session: Menggunakan token atau field Bearer pada tiap sesi komunikasi (lihat: JWT atau token lainnya).

Penilaian Rekan Sejawat (20%)

[2] https://docs.astral.sh/uv/