Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung

Tugas 4 II4021 Kriptografi – Semester II tahun 2024/2025

Sistem Keamanan Data Terintegrasi Berbasis Multi-Kriptografi dan *Group-based Decryption*

Batas pengumpulan	**:** Sabtu, 14 Juni 2025, Pukul 23.59 WIB
Tempat pengumpulan	**:** Form Pengumpulan
Anggota kelompok	**:** 2-3 orang
QnA	**:** QnA Tugas II4021 Kriptografi

Berkas pengumpulan :

a. Laporan (soft copy) dengan format PDF
b. Kode program yang bisa dijalankan, disertai README
c. Video demo

Studi Kasus

Keamanan Terdistribusi untuk Akses Data Akademik Mahasiswa

Dalam era digitalisasi sistem akademik, data transkrip nilai mahasiswa menjadi salah satu aset sensitif yang harus dijaga kerahasiaan dan keasliannya. Transkrip akademik tidak hanya memuat informasi nilai mata kuliah, tetapi juga berperan sebagai dokumen resmi yang sering digunakan dalam berbagai kebutuhan administratif, seperti beasiswa, rekrutmen, hingga akreditasi. Oleh karena itu, dibutuhkan sistem yang dapat menjamin keamanan data tersebut, baik dari segi **kerahasiaan (*confidentiality*), integritas (*integrity*), maupun autentikasi (*authentication*)**.

Gambar 1. Ilustrasi keamanan data sebagai aspek yang penting untuk dijaga.
Sumber: https://pdpsi.unisnu.ac.id/cybersecurity-di-lingkungan-akademik-untuk-melindungi-data-mahasiswa

Pada Tugas 4 ini, Anda diminta untuk mengembangkan sebuah aplikasi yang dapat melakukan enkripsi dan penandatanganan digital terhadap data transkrip akademik dengan pendekatan multi-kripto. Sistem akan mengenkripsi data menggunakan algoritma AES (kriptografi simetris), disertai tanda tangan digital berbasis RSA dan SHA-3 untuk memastikan integritas dan autentikasi. Selain itu, sebagai bentuk pengendalian akses, kunci enkripsi AES akan dibagi menggunakan **Shamir's Secret Sharing Scheme**, memungkinkan skema ***group-based decryption***. Dengan pendekatan ini, hanya pihak-pihak tertentu, seperti Dosen Wali dan Ketua Program Studi, yang dapat bersama-sama merekonstruksi kunci untuk mengakses data sensitif, sementara mahasiswa hanya bisa melihat versi data yang sudah dibatasi. Pendekatan ini mendemonstrasikan bagaimana teknik-teknik kriptografi modern dapat diterapkan untuk meningkatkan keamanan dan keadilan dalam sistem akademik.

Penjelasan Implementasi

Pada tugas ini, Anda diminta untuk mengimplementasikan aplikasi berbasis web atau desktop yang mengamankan data transkrip akademik mahasiswa dengan menggabungkan berbagai konsep kriptografi: **kriptografi simetris (AES, RC4)**, **kriptografi asimetris (RSA)**, ***hash* (SHA-3)**, dan ***secret sharing* (Shamir's Secret Sharing Scheme)**. Sistem ini menekankan keamanan, integritas, dan kontrol akses berbasis peran (*role-based access control*) dengan pendekatan *Group-Based Decryption*.

Secara garis besar, sistem ini terdiri dari beberapa tahap utama, yaitu: pembuatan kunci, input dan enkripsi data transkrip, penandatanganan digital, penyimpanan dan pembagian kunci, laporan transkrip akademik, serta proses dekripsi terkontrol berdasarkan peran. Berikut adalah beberapa *use case* yang wajib dimiliki oleh aplikasi.

1. Autentikasi Pengguna

Dalam melakukan autentikasi, pengguna perlu melakukan aksi login terlebih dahulu. Setelah sukses melakukan login, identitas pengguna akan disimpan dalam browser. Bentuk penyimpanan identitas pengguna dibebaskan.

- Untuk mengetahui pengguna mana yang sedang login, identitas ini dapat dicek di basis data.
- Jika identitas ini tidak ada, pengguna dianggap belum login dan diarahkan kembali ke halaman login dari halaman yang sedang dibukanya.
- Masa berlaku identitas pengguna dibebaskan.

2. *Role-based Access Control* (RBAC)

Dalam mengimplementasikan aplikasi diharapkan terdapat **tiga** buah *role*, yaitu **Ketua Program Studi**, **Dosen Wali**, dan **Mahasiswa**.

- Untuk membuat batasan lebih masuk akal, hanya boleh terdapat dua orang Ketua Program Studi yaitu untuk **Prodi Teknik Informatika** dan **Prodi Sistem dan Teknologi Informasi**.
- Mekanisme implementasi RBAC dibebaskan.

Berikut adalah daftar akses untuk masing-masing *role*.

Role	Bisa lihat transkrip sendiri?	Bisa lihat transkrip mahasiswa lain?	Bisa membuka enkripsi transkrip penuh?
Mahasiswa	✅	❌	❌
Dosen Wali	-	✅ (jika merupakan mahasiswa bimbingannya)	✅ (jika bergabung dengan sesama Dosen Wali)
Ketua Program Studi	-	✅	✅

3. *Input* Data Akademik

Aplikasi diharapkan menyediakan halaman dimana **Dosen Wali** bisa memasukkan data akademik mahasiswanya. Data yang perlu dimasukkan untuk setiap mahasiswa adalah sebagai berikut.

a. NIM
b. Nama Lengkap
c. 10 mata kuliah yang diambil mahasiswa terkait dengan informasi meliputi:
   - Kode mata kuliah
   - Nama mata kuliah
   - Jumlah SKS
   - Indeks

Tambahkan pula satu kolom IPK yang dihitung secara otomatis dari nilai-nilai mata kuliah.

4. Enkripsi Kolom Data

Setelah mendapatkan data akademik yang berada pada poin 3, dilakukan enkripsi terhadap kolom-kolom basis data (boleh semua *field*, atau setiap *field* kecuali NIM) menggunakan **algoritma AES.** Kunci enkripsi ditanyakan saat melakukan enkripsi.

5. Shamir's Secret Sharing

Seperti yang disampaikan pada daftar akses pada poin 2, Dosen Wali hanya bisa membuka enkripsi penuh jika bergabung dengan sesama Dosen Wali. Disinilah peran *secret sharing* diperlukan. Pada saat kunci enkripsi dibuat pada poin 4, dilakukan **Shamir's Secret Sharing Scheme (SSSS)** untuk membagi kunci AES (AES *key*) kepada setiap Dosen Wali yang terdaftar dalam aplikasi, implementasi detail penerimaan hasil *sharing* dibebaskan (dapat menggunakan "notifikasi" atau menambahkan *field* baru pada penyimpanan data Dosen Wali atau cara lainnya). Mekanisme SSSS **harus diimplementasikan sendiri** tanpa *library*.

6. Tanda Tangan Digital

Aplikasi juga diharapkan menyediakan tanda tangan digital yang diimplementasikan dengan **algoritma RSA** dan ***hash* SHA-3**.

- Pembangkitan tanda-tangan untuk setiap *record* dilakukan menggunakan kunci privat yang sama, yaitu **kunci privat Ketua Program Studi**.
- Verifikasi tanda-tangan digital untuk setiap *record* dilakukan menggunakan kunci publik yang sama, yaitu **kunci publik Ketua Program Studi**.
- Boleh menambahkan satu kolom pada dalam basis data untuk menyimpan kunci publik dari setiap *record* (mungkin saja kunci publik yang digunakan berbeda untuk setiap *record*).
- Nilai *hash* dibangkitkan dari nilai semua *field* pada setiap rekaman
  Contoh: SHA3('II301' + 'Aljabar' + '3' + 'AB' + … + 'II403' + 'Tugas Akhir' + '4' + 'AB').
- Algoritma RSA **harus diimplementasikan sendiri** tanpa *library*.

7. Dekripsi dan *Group-based Access*

Setelah proses pada poin 5 dan 6, khusus ketika **Dosen Wali** ingin mengakses data selain mahasiswa bimbingannya.

- Sistem akan meminta partisipasi dari **minimal 3 Dosen Wali**, yang salah satunya adalah dosen yang menjadi wali dari mahasiswa yang dimaksud, untuk menggabungkan kembali AES *key* menggunakan *Shamir's Secret Reconstruction*.
- Setelah kunci berhasil direkonstruksi, sistem dapat melakukan dekripsi nilai dan IPK untuk ditampilkan.
- Sebelum data ditampilkan, sistem akan melakukan verifikasi tanda tangan digital menggunakan kunci publik RSA seperti yang ada pada poin 6.
  a. Jika *signature* valid, data ditampilkan dengan label ✅ **Verified**.
  b. Jika invalid, data ditampilkan sebagai ❌ **Unverified** dan dianggap telah diubah.

Mekanisme dekripsi ini **tidak berlaku** untuk **Mahasiswa** yang ingin melihat nilainya sendiri dan **Ketua Program Studi** yang ingin melihat semua nilai mahasiswa.

8. Laporan Transkrip Akademik

Dalam rangka keperluan eksternal seperti pendaftaran beasiswa, aplikasi juga mampu membuat laporan transkrip akademik yang dapat disimpan dalam format PDF.

- Aplikasi menyediakan tampilan untuk melakukan cetak laporan transkrip akademik mahasiswa tertentu.
- Laporan transkrip akademik harus memuat semua informasi dari mahasiswa terkait (Nama, NIM, Mata kuliah dan nilainya, Total SKS dan IPK, serta tanda tangan digital Ketua Program Studi beserta namanya), tampilan PDF dibebaskan dan dapat diunduh ke lokal.

- Pengguna juga dapat memilih apakah akan melakukan enkripsi terhadap PDF laporan transkrip akademik atau tidak. Implementasi enkripsi dilakukan dengan **algoritma RC4**.
- Jika pengguna memilih untuk mengenkripsi, aplikasi akan menanyakan kunci enkripsi, kemudian pengguna dapat mengunduh hasil enkripsi secara lokal. Aplikasi juga menyediakan antarmuka untuk membuka PDF yang telah terenkripsi di dalam aplikasi dengan menanyakan kunci dekripsinya terlebih dahulu.
- Algoritma RC4 **harus diimplementasikan sendiri** tanpa *library*.

9. Lain-lain

Berikut adalah beberapa hal yang perlu menjadi perhatian dan dapat menjadi konsiderasi.

- Implementasi penyimpan data akademik **wajib** dilakukan menggunakan basis data SQL (sebagai contoh, MySQL, PostgreSQL, SQLite), desain skema basis data relasional (DDL) dibebaskan, tetapi wajib dijelaskan di laporan.
- Data yang disimpan pada basis data adalah data transkrip yang kolomnya sudah terenkripsi dan tanda tangan digital untuk setiap *record* data mahasiswa beserta nilainya.
- Data yang disimpan dapat ditampilkan di layar aplikasi sesuai dengan daftar akses yang didefinisikan pada poin 2, antarmuka dibebaskan. Khusus untuk Dosen Wali, perhatikan kembali skema *group-based access* pada poin 7.
- Implementasi aplikasi dilakukan berbasis web atau desktop, kakas yang boleh digunakan **dibebaskan**.
- Tanda-tangan digital direpresentasikan sebagai karakter-karakter heksadesimal atau karakter base64. Cipherteks disimpan dalam bentuk string atau base64.

Bonus

1. **Implementasi SHA-3 (Keccak)**
   - Fungsi *hash* menggunakan algoritma Keccak diimplementasikan sendiri tanpa menggunakan *library*.
   - Fungsi *hash* ini akan digunakan pada proses tanda tangan digital.
2. **Cryptographically Secure Pseudorandom Generator (CSPRNG)**
   - Untuk melakukan pembangkitan bilangan acak, gunakan algoritma Blum Blum Shub (BBS).
   - Algoritma Blum Blum Shub wajib diimplementasikan sendiri tanpa menggunakan *library*.
   - Pembangkit ini dapat digunakan saat ingin membentuk *random key*, seperti kunci untuk AES atau RC4. Buatlah algoritmanya sehingga memenuhi berbagai macam kasus, misalkan ketika bilangan acak yang dibuat diharapkan merupakan bilangan prima.
3. **Melakukan *deployment* terhadap aplikasi**

Prosedur Pengerjaan

Berikut adalah prosedur pengerjaan dari tugas ini.

1. Tugas dikerjakan berkelompok dengan anggota minimal 2 orang dan maksimal 3 orang, dilarang *gabut*. Cantumkan pembagian tugas dengan jelas antara anggota kelompok.
2. Waktu pengumpulan tugas **paling lambat Sabtu, 14 Juni 2025 sebelum pukul 23.59**. Pengumpulan tugas yang terlambat **tidak akan memperoleh nilai** dan nilai Tugas 4 menjadi 0.
3. Program harus mengandung komentar yang jelas serta mudah dibaca.
4. Anda dilarang menggunakan kode program yang didapatkan dari internet (alasan menggunakan kakas seperti GitHub Copilot tidak diterima). Anda harus membuat program sendiri, diperbolehkan untuk belajar dari program yang sudah ada maupun menggunakan kakas AI (tetapi Anda harus tetap memahami apa yang dikerjakan, bila menggunakan kakas AI maka lampirkan tangkapan layar penggunaannya di laporan).
5. Program memiliki antarmuka yang *user-friendly*. Anda juga dapat menambahkan fitur lain untuk menunjang program yang Anda buat (unsur kreativitas).

Isi Laporan

Berikut adalah prosedur pengerjaan dari tugas ini.

1. *Cover* laporan ada foto anggota kelompok (foto berdua atau bertiga). Foto ini menggantikan logo "gajah" ganesha.
2. Teori singkat dari setiap aspek kriptografi yang digunakan.
3. Perancangan dan implementasi (termasuk di dalamnya, pemilihan kakas, desain basis data relasional, dan lain lain).
4. Pengujian program dan hasil analisis dengan berbagai kasus.
5. Tautan kode sumber program dalam sebuah repositori Github dengan README yang berisi minimal tata cara menjalankan program dan identitas pembuat.
6. Tautan *Google Drive* yang berisi demo aplikasi dalam berbagai kasus dan fitur.
7. Lampiran yang berisi antarmuka program.
8. Daftar Pustaka.

"Selamat Mengerjakan!"

eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJzdWIiOiJNaWNoYWVsIExlb24iLCJtc2ciOiJTZWxhbWF0IG1lbmdlcmpha2FuIFR1Z2FzIHBlbmdnYW50aSBVQVMhIHNlbW9nYSBoYXNpbG55YSBtZW11YXNrYW4uIFNhbGFtLCBBc2lzdGVuIElJNDAyMSAyMDI0LzIwMjUiLCJpYXQiOjE1MTYyMzkwMjJ9.ICo98rSM1u0U8KIQSRNJchQ4mgJ9lR_F8GEwpA4hE0

Lampiran

Contoh basis data akademik yang ditandatangani dan dienkripsi.

NIM	Nama	Kode MK 1	Nama MK	Nilai	SKS	...	Kode MK 10	Nama MK	Nilai	SKS	IPK	DS
76g5	rea76V	nbg%j l	C7bga7 x	c%4	3#vc		kitt	bvxZ	Bv58	Bc%	*kb	Asnbct6 a5g#
x^5f	br5@1	ewb6%	Ng&6c	tyc4	L&%		bvcxc	Vc^5	L6xr	tsc)8	Nz43	9jbxsU H67ehs
hyhbt	9*nvon c	Bc4ht	765cx	ht^51	!3#		E4vc%	)987o	l6%	Bvc	9*zg	mnavca y
jnccz	Vctreh 75	Czx6^	yzn43x	90bcz	pouc		I(8cxz	Bv)z	Nvz	Cx4	c8@	Nbcv6a 5f75

Contoh template PDF transkrip akademik.

Program Studi Sistem dan Teknologi Informasi
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung

Transkip Akademik

Nama: Alice Noorin
NIM: 18121013

No	Kode mata kuliah	Nama mata kuliah	SKS	Nilai
1	II301	Matematika STI	3	A
2	II391	Manajemen Proyek	2	AB
..				
10	II401	Tugas Akhir	4	A

Total Jumlah SKS = 36
IPK = 3.41

Ketua Program Studi

--Begin signature—
BFc65FFeCD2108CE340B
--End signature

(Dr. I Gusti Bagus Baskara)