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

Tugas Program ke-4 II4031 Kriptografi dan Koding

Program Basisdata Terenkripsi dan Bertanda-tangan Digital dengan Menggunakan Algoritma RSA dan Fungsi *hash* SHA-3

Tanda-tangan digital dapat digunakan untuk otentikasi data digital, seperti pesan yang dikirim melalui saluran komunikasi dan dokumen elektronis yang disimpan dalam komputer.

Pada tugas ke-3 ini, anda diminta membuat aplikasi berbasis desktop atau berbasis web yang mengimplementasikan algoritma RSA + SHA-3 (Keccak) untuk:

1. Mengenkripsi field-field basisdata transkip akademik
2. Menandatangi transkip akademik
3. Menandatangani dan mengenkripsi transkip akademik

Studi kasus yang digunakan adalah basisdata akademik. Basisdata transkip akademik berisi rekaman nilai-nilai mata kuliah mahasiswa beserta IPK. Diasumsikan jumlah mata kuliah 10 buah saja, yaitu mata kuliah pada Program Studi Sistem dan Teknologi Informasi.Struktur file basisdata kira-kira sebagai berikut:

NIM	Nama	Kode MK 1	Nama matkul	Nilai	SKS	...	Kode MK 10	Nama matkul	Nilai	SKS	IPK	Tanda-tangan digital

Basisdata dapat dibuat menggunakan basisdata SQL seperti MySQL, PostgreSQL, SQLite, atau menggunakan struktur data tabel biasa.

Aplikasi memiliki *use case* sebagai berikut:

1. Membangkitkan kunci publik dan kunci privat RSA
2. Menerima input data akademik mahasiswa
3. Mengenkripsi field-field basisdata (boleh semua field, atau semua field kecuali field NIM)
4. Membangkitkan tanda-tangan digital untuk setiap rekaman data akademik setiap mahasiswa
5. Mengenkripsi rekaman data akademik yang sudah ditandatangani
6. Memverifikasi tanda-tangan digital pada setiap rekaman
7. Menampilkan basisdata (plainteks dan cipherteks)
8. Membuat file laporan transkip akademik dan dapat disimpan dalam bentuk file pdf

Tanda-tangan digital direpresentasikan sebagai karakter-karakter heksadesimal atau karakter base64. Cipherteks disimpan dalam bentuk string atau base64.

Contoh basisdata akademik mahasiswa:

NIM	Nama	Kode MK 1	Nama matkul	Nilai	SKS	...	Kode MK 10	Nama matkul	Nilai	SKS	IPK	Tanda-tangan digital
1201	Alice	II301	Aljabar	A	3		II302	Kripto	AB	2	3.51	67B65987F41
1201	Bob	II301	Aljabar	B	3		II401	ML	B	3	2.75	B4510DE3052
1203	Carol	II204	Basdat	BC	2		II231	S.Info	A	3	3.01	B765EEF3125
1204	David	II302	OOP	C	3		II321	TA	A	4	3.78	8FC35219067C

Contoh basisdata akademik terenkripsi:

NIM	Nama	Kode MK 1	Nama matkul	Nilai	SKS	...	Kode MK 10	Nama matkul	Nilai	SKS	IPK	Tanda-tangan digital
%g5	Ta76V	~g%j1	Nbga7x	V%5	Gvc		Nbvct	bvcxZ	Bv58	Bc%	*76%	67B65987F41
H^5f	0J5@1	Jsb6%	Ng&6c	Bc4	65%		vcxc	Vc^5	L6xr	Vc)8	Nz43	B4510DE3052
9*hbt	9*nvas	#2jht	9k#cx	X^51	Vc#		Bvc%	)987o	l-6%	Bvc	9*7zg	B765EEF3125
)*hcz	Ky54a	Ojsa^	Jn43x	&bcz	*vc		I(8cxz	Bv)z	Nvz3	Cx4$	98@	8FC35219067C

Contoh basisdata akademik yang ditandatangani dan dienkripsi:

NIM	Nama	Kode MK 1	Nama matkul	Nilai	SKS	...	Kode MK 10	Nama matkul	Nilai	SKS	IPK	Tanda-tangan digital
76g5	rea76V	nbg%j1	C7bga7x	c%4	3#vc		kitt	bvxZ	Bv58	Bc%	*kb	Asnbct6a5g#
x^5f	br5@1	ewb6%	Ng&6c	tyc4	L&%		bvcxc	Vc^5	L6xr	tsc)8	Nz43	9jbxsUH67ehs
hyhbt	9*nvonc	Bc4ht	765cx	ht^51	!3#		E4vc%	)987o	l6%	Bvc	9*zg	mnavcay
jnccz	Vctreh75	Czx6^	yzn43x	90bcz	pouc		I(8cxz	Bv)z	Nvz	Cx4	c8@	Nbcv6a5f75

Contoh transkip 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)

Spesifikasi program:

1. Yang anda buat adalah aplikasi web/desktop yang terdiri dari menu:
   a) pembangkitan kunci publik dan kunci privat RSA.
   b) pembangkitan tanda-tangan digital (*signing*)
   c) verifikasi tanda-tangan digital (*verivying*)
   d) input data akademik
   e) enkripsi field-field basisdata
   f) enkripsi field-field basisdata yang sudah ditandatangani
   g) menampilkan basidata ke layar (plainteks dan cipherteks), format tampilan bebas
   h) membuat laporan transkrip akademik setiap mahasiswa dan menyimpan dalam bentuk file pdf (terenkripsi)
   i) mendekripsi file laporan akademik

2. Program RSA harus dibuat sendiri, tidak boleh menggunakan libary bahasa pemrograman yang dipilih.
3. Fungsi hash SHA-3 disarankan dibuat sendiri programnya (bonus: 10), namun jika tidak, boleh menggunakan library atau fungsi yang tersedia di dalam bahasa pemrograman yang dipilih, tetapi untuk program RSA harus dibuat sendiri primitif operasinya.
4. Nilai hash dibangkitkan dari nilai semua field pada setiap rekaman
   Contoh: SHA3('II301'+'Aljabar'+'3'+'AB'+…+'II403'+'Tugas Akhir'+'4'+'AB')
5. Pembangkitan tanda-tangan untuk setiap rekaman menggunakan kunci privat yang sama, yaitu kunci privat Kaprodi
6. Verifikasi tanda-tangan digital untuk setiap rekaman menggunakan kunci publik yang sama, yaitu kunci publik Kaprodi
7. Enkripsi *field-field* basidata menggunakan algoritma *modified* RC4 yang telah dibuat pada Tugas 2. Kunci enkripsi/dekripsi ditanyakan saat melakukan enkripsi.
8. IPK dihitung secara otomatis dari nilai-nilai mata kuliah
9. Boleh menambahkan satu field di dalam basisdata untuk menyimpan kunci public untuk setiap rekaman (mungkin saja kunci public yang digunakan untuk setiap rekaman berbeda-beda)
10. Bahasa pemrograman dan kakas yang digunakan bebas (Java, C, C++, C#, Python, dll).
11. File PDF (laporan transkip akademik mahasiswa) disimpan dalam bentuk file cipherteks. Enkripsi file menggunakan algoritma AES (gunakan library AES yang disediakan oleh kakas Bahasa pemrograman). Kunci enkripsi file boleh sama dengan kunci modified RC4 (poin nomor 7) atau boleh berbeda.
12. Tugas dikerjakan berkelompok, min 2 orang max 3 orang.
13. Waktu pengumpulan adalah Sabtu 25 Mei 2024 (max pukul 23.59 WIB)
14. Bonus (10): video Tugas 4 ini di-upload ke Youtube

Yang dikumpulkan adalah laporan (file PDF) yang berisi:

1. Deskripsi singkat aplikasi (max 1 halaman)
2. *Source kode program* lengkap
3. Skrinsut aplikasi dan skrinsut output program
4. Contoh tampilan basisdata (plainteks dan cipherteks)
5. Link ke *github* atau *google drive* yang berisi kode program
6. Link video di Youtube (opsional)
7. Tampilkan foto kelompok anda pada *cover* laporan.
8. Alamat drive pengumpulan:

https://drive.google.com/drive/u/1/folders/1QxkWocaVOGz4ub47MO-IuUsvkdmudWEF