Program StudiTeknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung

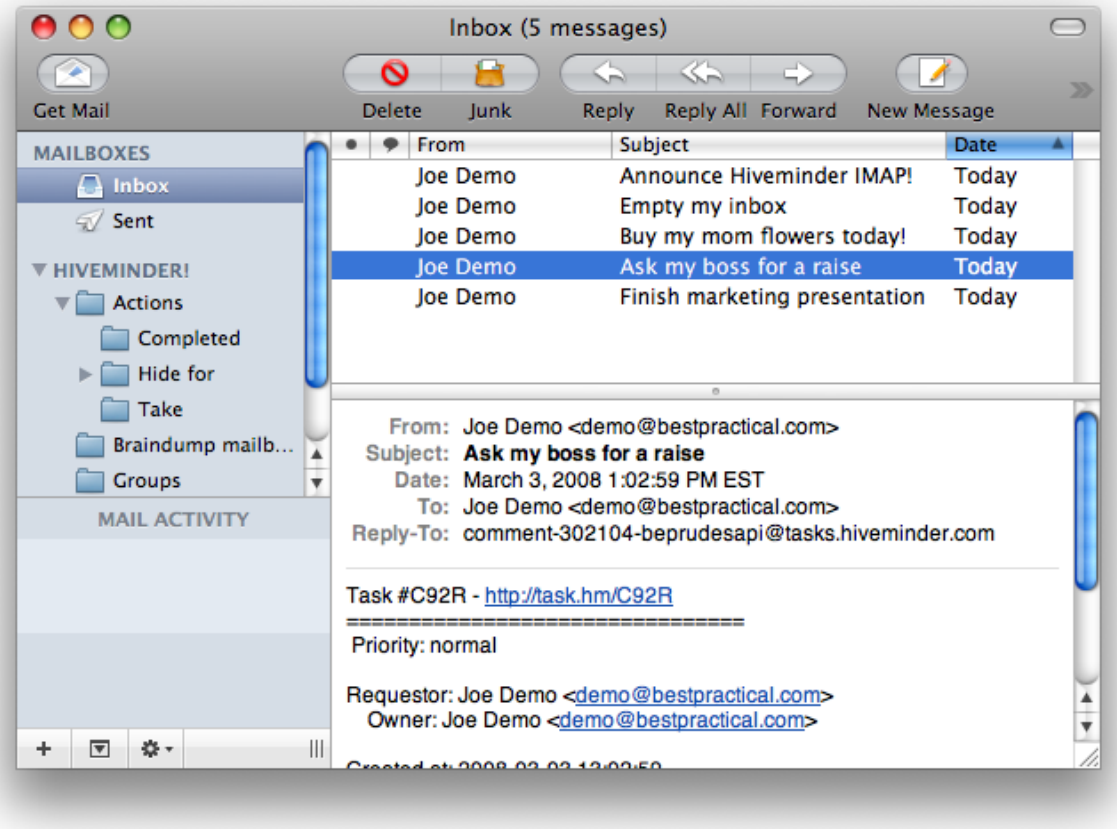
Tugas Besar ke-2 IF4020 Kriptografi

Penerapan *Elliptic Curve Cryptography* untuk Perangkat *Mobile*

Batas pengumpulan : Senin, 22 April 2019, jam 13.00
Tempat pengumpulan : Lab IRK
Arsip pengumpulan :
- CD/DVD berisi program, arsip *readme.txt*, laporan, arsip contoh, arsip parameter dan kunci.
- kertas A4 untuk laporan (*printout)*

Deskripsi tugas :

Aplikasi klien surel (*e-mail client*) banyak tersedia di Internet. Beberapa aplikasi klien surel adalah *Mozilla Thunderbird*, *Zimbra*, *Spicebird*, *Mailbird*, dll (Baca: *http://alfian-zc.blogspot.com/2011/01/5-aplikasi-email-client.html* dan *https://yunikosongdelapansembilanlima.wordpress.com/2014/06/07/macam-macam-software-email-client/*



Gambar 1. Contoh sebuah klien surel

Sebagian besar tidak memiliki fitur enkripsi surel dan fitur tanda tangan digital. Surel rawan untuk disadap dan dibaca oleh pihak yang tidak berhak, dimanipulasi, dan sebagainya. Enkripsi dapat digunakan untuk untuk menjaga kerahasiaan surel, sedangkan tanda tangan digital dapat digunakan untuk keperluan otentikasi (pengirim dan penerima surel), keaslian isi surel (*data integrity*), dan nirpenyangkalan (*non-repudiation*)

Pada tugas besar 2 anda diminta membuat aplikasi klien surel sederhana pada perangkat *mobile* yang dilengkapi dengan fitur enkripsi/dekripsi dan fitur tanda tangan digital. Surel dienkripsi dengan algoritma *block-cipher* yang sudah anda buat sebelumnya, sedangkan tanda tangan digital dibangkitkan dengan kolaborasi algoritma *Elliptic Curve ElGamal* atau ECDSA dan fungsi *hash SHA*-1 atau SHA-3 (Keccak).

Tanda tangan digital bergantung pada isi surel dan kunci. Tanda-tangan digital direpresentasikan sebagai karakter-karakter heksadesimal dan ditaruh pada akhir surel. Untuk membedakan tanda-tangan digital dengan isi dokumen, maka tanda-tangan digital diawali dan diakhiri dengan *tag* `<ds>` dan `</ds>`, atau tag lain (diserahkan kepada anda).

Contoh: `<ds>4EFA7B223CF901BAA58B991DEE5B7A</ds>`.

atau

```
*** Begin of digital signature ****
     4EFA7B223CF901BAA58B991DEE5B7A
*** End of digital signature ****
```

Contoh surel dan tanda tangan digital:

Kepada Yth.
Bapak Dekan
Di Tempat

Dengan hormat.
Bersama surat ini saya ingin mengabarkan bahwa nilai skripsi mahasiswa yang bernama Faisal Saleh dengan NIM 13902021 adalah 86,5 atau dalam nilai indeks A. Sidang skripsi sudah dilakukan pada Hari Rabu Tanggal 21 Januari 20 Juli 2005.

Atas perhatian Bapak saya ucapkan terima kasih.

Bandung, 25 Juli 2005

Dosen Pembimbing Skripsi

Ir. Ahmad Agus

-----BEGIN PGP SIGNATURE-----

iQA/AwUAQnibsbPbxejK4Bb3EQJXvQCg8zN6UL0xnwBTPR5
FfWNt4uxh3AEAn2NC/G2VTUrLpcSyo2l/S/D/+rUl=pZeh

-----END PGP SIGNATURE-----

Spesifikasi program:

1. Klien surel dilengkapi dengan menu untuk membangkitkan kunci publik dan kunci privat untuk berdasarkan *Elliptic Curve Cryptography*.
2. Klien surel memiliki editor untuk mengetikkan isi surel, memasukkan alamat surel penerima, mengetikkan subyek surel, dll.
3. Klien surel dapat menampilkan *inbox*, *sent email*, dan fitur-fitur umum yang terdapat di dalam klien surel.
4. Klien surel boleh menyediakan *attachment*, tetapi file yang di-*attach* tidak perlu dienkripsi.
5. Pengguna dapat memilih apakah surel dienkripsi atau tidak (ada *toggle icon* untuk memilihnya)
6. Pengguna dapat memilih apakah surel ditandatangani atau tidak (ada *toggle icon* untuk memilihnya).
7. Jika pengguna memilih mengenkripsi/dekripsi surel, maka klien surel meminta pengguna memasukkan kunci.
8. Isi surel dienkripsi/dekripsi dengan *block cipher* yang sudah andfa buat pada tugas pengganti UTS.
9. Program SHA-1 atau SHA-3 harus dibuat sendiri (tidak menggunakan *library* atau fungsi *built-in*)
10. Jika pengguna memilih menandatangani surel (baik surel terenkripsi atau tidak), maka klien meminta kunci privat. Untuk memverifikasi tanda tangan digital, klien surel meminta kunci public. Kunci public/privat dapat dibaca dari file atau diketikkan oleh pengguna.
11. Bahasa dan kakas yang digunakan bebas (Java, C#, C++, Phyton, dll).
12. Sistem operasi yang digunakan bebas (WindowsPhone, Android, iOS, dll).
13. Untuk program klien surel sendiri boleh menggunakan *open source* atau dibuat sendiri.

Isi laporan :

1. Deskripsi masalah.
2. Dasar teori.
3. Strategi penyelesaian masalah (lingkungan implementasi dan trik khusus).
4. Struktur data dan spesifikasi subrutin.
5. Pengujian dan analisis hasil. Pengujian menggunakaan contoh email yang disertakan di dalam laporan.

   Pengujian kerahasiaan surel
   - Jalankan program *wireshark* untuk memantau *data traffic*
   - Tangkap surel dengan program *wireshark* untuk memastikan bahwa surek terenkripsi selama proses pengiriman dari pengirim ke penerima.
   -

   Pengujian *otentikasi* dan *integrity* dengan kasus-kasus berikut:
   - karakter di dalam surel diubah (dihapus, ditambah)
   - karakter di dalam tanda-tangan digital diubah
   - kunci privat yang digunakan tidak berpadanan dengan pasangan kunci publiknya.
   - tanda-tangan digital dihapus dari surel

   Untuk aplikasi SMS, prinsip pengujiannya sama seperti di atas.

6. Lampiran yang berisi:

- antarmuka program
- contoh surel (asli/terenkripsi/diberi tanda tangan digital
- contoh nilai-nilai paramater ECC

7. Tampilkan foto kelompok anda bertiga pada *cover* laporan.
8. Kesimpulan dan saran.