

## PERANCANGAN PEMBANGKIT TANDA TANGAN DIGITAL MENGGUNAKAN DIGITAL SIGNATURE STANDARD (DSS)

Sudimanto

Sekolah Tinggi Manajemen Informatika dan Komputer LIKMI  
Jl. Ir. H. Juanda 96 Bandung 40132

[sudianen@yahoo.com](mailto:sudianen@yahoo.com)

---

### Abstrak

Kriptografi merupakan salah satu metode yang digunakan untuk menjaga kerahasiaan dan keamanan data. Mekanisme kriptografi modern yang digunakan adalah metode tanda tangan digital menggunakan algoritma *Digital Signature Algorithm* (DSA) yang merupakan bagian dari metode *Digital Signature Standard* (DSS). Metode ini menggunakan kriptografi kunci umum (*Public-key cryptography*) yang memungkinkan seorang pengguna yang memiliki sebuah kunci rahasia yang bersifat pribadi untuk “menandatangani” dokumen. Sedangkan pihak lain yang memiliki kunci public sesuai dapat memverifikasikan dokumen apakah dokumen tersebut di tandatangani oleh pemilik kunci pribadi tersebut.

**Kata-kata Kunci:** *Digital Signature, Public Key, Cryptography*

---

### 1. PENDAHULUAN

Teknologi informasi semakin berkembang pesat sehingga mendorong perkembangan diberbagai bidang baik bidang pendidikan, kesehatan, industri, komunikasi dan kehidupan sehari-hari, sehingga peran komputer semakin tidak dapat terpisahkan. Hal ini tidaklah lain karena didorong oleh perkembangan teknologi informasi dalam jaringan internet.

Jaringan internet yang tersebar diseluruh dunia tidak dapat beroperasi sendiri tanpa adanya pengaturan. Internet sendiri memiliki protokol-protokol dan berbagai hukum yang mengatur pengaksesan internet oleh berbagai pengguna di seluruh dunia. Konsep jaringan internet merupakan salah satu contoh bentuk jaringan paling kompleks yang pernah ada, namun dalam kehidupan sehari-hari ternyata konsep jaringan tidak hanya digunakan pada internet.

Sebuah sistem jaringan sering dilakukan pertukaran data atau informasi antar pengguna dengan menggunakan koneksi yang sudah diterapkan oleh jaringan tersebut. Dalam kasus pertukaran informasi yang bersifat cukup penting, maka dibutuhkan sebuah sistem jaringan yang sudah memiliki aspek keamanan lengkap untuk menjamin keamanan data atau informasi yang berputar di dalam jaringan. Teknologi sekarang ini

memungkinkan pengguna saling mengirim informasi, baik dalam bentuk lisan maupun tulisan, pada waktu yang bersamaan seakan-akan orang yang diajak berkomunikasi ada di sebelahnya. Namun dengan adanya penemuan cara-cara baru untuk berkomunikasi maka bermunculan juga cara-cara baru untuk dapat merusaknya. Jadi dengan berkembangnya teknologi komunikasi maka diperlukan sebuah sistem yang dapat mengamankan komunikasi yang dibangun agar pengguna dapat dengan aman berkomunikasi.

Keamanan data sangat dibutuhkan oleh lembaga besar, dimana mereka harus menjaga kerahasiaan dan keamanan data-data penting milik mereka dari pihak luar yang tidak berkepentingan. Semakin besar sebuah lembaga, semakin banyak pula surat-surat penting yang harus dibuat dan diarsipkan. Begitu pula kasusnya yang terjadi dalam pengiriman surat-surat penting kepada pihak kedua, diperlukan jaminan keamanan agar surat-surat tersebut sampai ditempat tujuan dengan utuh tanpa kekurangan suatu apapun. Maka dari itu kerahasiaan dan keamanan saat melakukan pertukaran data adalah hal yang sangat penting, baik untuk keamanan bersama lembaga, maupun untuk kepentingan individu. Perlindungan terhadap kerahasiaan data perlu ditingkatkan, salah satu caranya dengan dengan penyandian data dengan metode kriptografi. Kriptografi adalah suatu ilmu atau seni mengamankan pesan, dan dilakukan oleh *cryptographer*. Sedangkan *cryptanalysis* adalah suatu ilmu dan seni membuka (*breaking*) *ciphertext* dan orang yang melakukannya disebut *cryptanalysis*. (Kurniawan, 2004).

Sedangkan Menurut Bruce Schneier dalam bukunya "*Applied Cryptography*", kriptografi adalah ilmu pengetahuan dan seni menjaga pesan atau data agar tetap aman (*secure*). (Schneier, 1996). Salah satu mekanisme kriptografi modern adalah metode tanda tangan digital dengan menggunakan algoritma *Digital Signature Algorithm* (DSA) yang merupakan bagian dari metode *Digital Signature Standard* (DSS). Metode ini menggunakan kriptografi kunci publik (*public-key cryptography*) yang memperbolehkan seorang pengguna dengan sebuah kunci rahasia pribadi 'menandatangani' dokumen, agar pihak lain yang memiliki kunci publik yang sesuai dengan kunci pribadi tadi, dapat memverifikasi dokumen tersebut apakah ditandatangani oleh si pemilik kunci pribadi tersebut. berdasarkan kunci yang digunakan untuk enkripsi dan dekripsi, kriptografi dapat dibedakan menjadi dua, yaitu algoritma kunci simetri (konvensional atau *symmetric-key cryptography*) dan algoritma kunci asimetri (kriptografi kunci publik atau *asymmetric-key cryptography*). (Munir, 2006:13)

Citra (*image*) adalah istilah lain untuk gambar sebagai salah satu komponen multimedia memegang peranan sangat penting sebagai bentuk informasi visual. Data atau informasi tidak hanya disajikan dalam bentuk teks, tetapi juga dapat berupa gambar, audio (bunyi, suara, musik), dan video. Ditinjau dari sudut pandang matematis, citra merupakan fungsi menerus (*continue*) dari intensitas cahaya pada bidang dwimatra. Sumber cahaya menerangi objek, objek memantulkan kembali sebagian dari berkas cahaya tersebut. Pantulan cahaya ini ditangkap oleh alat-alat optik, misalnya mata pada manusia, kamera, pemindai (*scanner*), dan sebagainya, sehingga bayangan objek yang disebut citra tersebut terekam. (Murni, 1992:90).

Pengenalan pola merupakan salah satu bidang studi yang berkaitan dengan citra yang berfungsi untuk mengelompokkan data numerik dan simbolik (termasuk citra) secara otomatis oleh mesin (dalam hal ini komputer). Tujuan pengelompokan adalah untuk mengenali suatu objek di dalam citra. Pengolahan citra merupakan proses awal (*preprocessing*) pada *computer vision*, sedangkan pengenalan pola merupakan proses untuk menginterpretasi citra. Teknik-teknik di dalam pengenalan pola memainkan peranan penting dalam *computer vision* untuk mengenali objek.

## **2. DESKRIPSI KONSEP PERANCANGAN PEMBANGKIT TANDA TANGAN DIGITAL MENGGUNAKAN *DIGITAL SIGNATURE STANDARD* (DSS)**

Konsep dari perangkat lunak ini adalah mengambil isi dari file untuk di bangkitkan tanda tangan digital yang kemudian di ubah ke suatu file lain oleh perangkat lunak yang berjenis EML. File EML ini adalah file teks biasa yang digunakan untuk menyimpan pesan E-mail. Yang mana terdiri dari header yang melingkupi alamat dari pengirim atau penerima, selain itu terdapat juga subjek, tanggal serta waktu pesan tersebut dikirim, serta isi dari E-mail itu sendiri.

Perangkat lunak ini dapat mengirimkan file, baik yang sudah di bubuhi tanda tangan ataupun belum ke alamat IP yang dituju melalui jaringan lokal yang sudah terhubung. Untuk melakukan proses pemberian tanda tangan dibutuhkan sepasang kunci, kunci privat dan kunci public serta parameter-parameter yang secara otomatis dibangkitkan oleh perangkat lunak yang kemudian disimpan dalam basis data. Hasil dari tanda tangan digital ini berupa dua baris string acak. Pengguna dapat menambahkan tanda-tangan asli yang berasal dari tulisan tangan yang sudah di rubah ke bentuk file gambar dengan ukuran 64 x 64 pixels. Gambar tersebut akan diproses dan di jadikan kunci untuk menentukan hasil dari tanda tangan digital.

Pesan yang sudah memiliki tanda tangan digital dapat di verifikasi dengan tepat oleh perangkat lunak untuk menunjukkan bahwa file tersebut asli berasal dari pengirim yang sebenarnya dan belum dirubah oleh pihak manapun. Penggunaan metode kriptografi kunci publik dan disediakannya system penyimpanan untuk kunci-kunci tersebut dapat mengatasi permasalahan dari pendistribusian kunci (key distribution problem).

Parameter-parameter, sepasang kunci serta tanda tangan digital yang diperlukan oleh sistem dibangkitkan menggunakan algoritma DSA (*Digital Standard Algorithm*). Algoritma ini menghasilkan lima buah nilai tiga buah nilai yang disusun sebagai parameter serta dua buah nilai yang disusun sebagai sepasang kunci. Dalam membuat sebuah tanda tangan digital digunakan sebuah fungsi yaitu fungsi *hash* satu arah (SHA). Fungsi *hash* adalah fungsi yang menerima masukkan *string* yang panjangnya sembarang dan mentransformasikannya menjadi *string* yang panjangnya tetap (nilai *hash*), umumnya berukuran jauh lebih kecil daripada *string* masukkannya (Munir,2006).

Pesan awal yang dibuat ditambahkan dengan sejumlah bit penganjal untuk membuat panjang sebuah pesan menjadi 64 bit yang kurang dari kelipatan 512. 512 ini merupakan hasil proses dari SHA yang memproses pesan-pesan ke dalam blok-blok yang berukuran 512. Setiap blok pesan diproses bersama dengan penyangga *Message Digest* (MD). Parameter, kunci privat, XKey (nilai acak XKey ditentukan dari pola tanda tangan) dan MD digunakan untuk menghasilkan sepasang nilai katakanlah nilai A dan B yang disebut sebagai tanda tangan digital. Nilai inilah yang nantinya akan ditambahkan ke dalam pesan. Dalam memverifikasi keabsahan sebuah tanda tangan digital, pesan digital dirubah menjadi MD sepanjang 160 bit. Nilai A yang diambil dari tanda tangan digital, MD, dan parameter dipakai sebagai masukan untuk menghasilkan sebuah nilai C. jika nilai C dan B ini sama maka tanda tangan digital dinyatakan sah jika berbeda maka tanda tangan digital dinyatakan tidak sah.

### **3. REALISASI RANCANGAN PERANGKAT LUNAK**

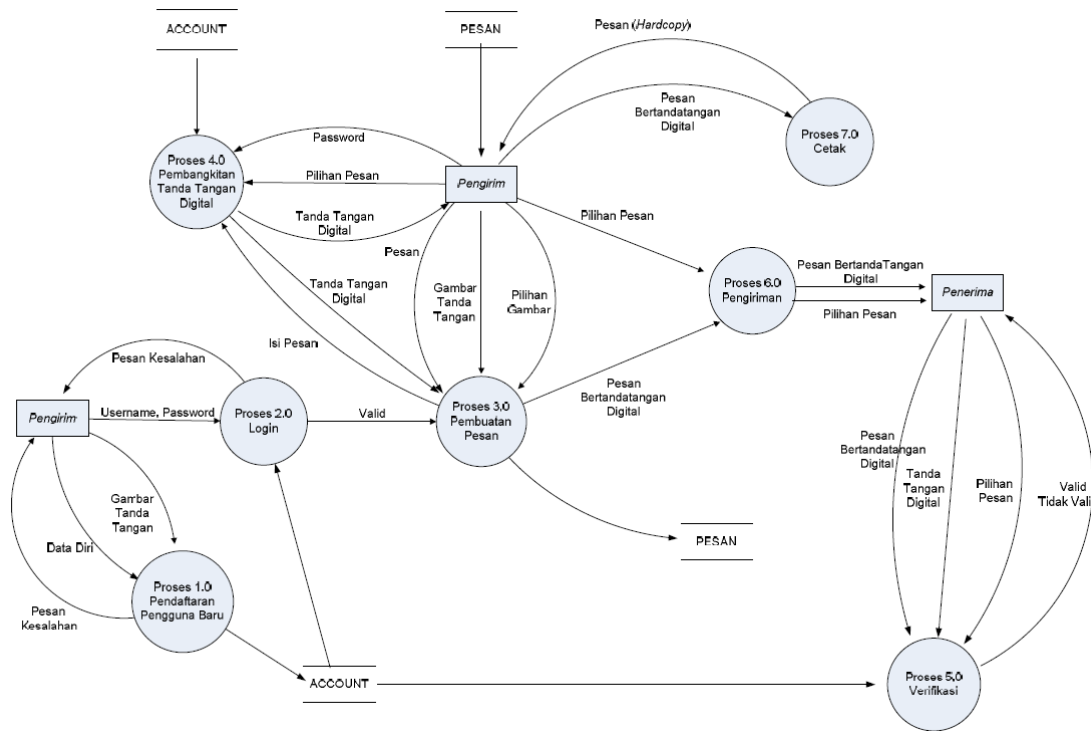
Secara keseluruhan perancangan ini melibatkan 3 buah entitas yaitu pengirim, penerima dan system itu sendiri. Perangkat lunak ini dirancang agar dapat diakses oleh semua pengguna, namun pengguna tersebut harus mendaftar terlebih dahulu. Peran penerima dibatasi sebagai pihak yang menerima pesan dan memverifikasi pesan tersebut. Pengisian data-data pengguna juga diperlukan untuk memverifikasi saat mengirim pesan. Pada

Gambar 3.1 menggambarkan secara terperinci proses-proses yang akan di jalankan oleh system. Pengguna baru diharuskan mendaftar dengan memberikan masukan berupa username, password dan data-data lainnya. Pengguna juga di minta memasukan gambar tanda tangan yang berupa file bitmap guna untuk membangkitkan nilai Xkey, dan password yang dimasukan digunakan untuk membangkitkan sepasang kunci dan parameter-parameter yang dibutuhkan kemudian data-data tersebut disimpan dalam *data store Account*. Sedangkan pengguna yang sudah mendaftar akan diminta *username* dan *password* untuk mendapatkan hak akses. Jika *username* dan *password* cocok maka pengguna dapat langsung masuk ke bagian pembuatan pesan jika tidak cocok maka akan muncul pesan kesalahan.

Pengguna dapat memilih untuk membuat pesan sendiri atau mengambil dari sumber lain. Pembangkitan tanda tangan digital dilakukan pada proses pembangkitan tanda tangan digital yang akan di mulai saat pengguna memasukan password guna memeriksa keaslian pengguna, jika password benar maka system akan menambahkan tanda tangan digital pada pesan dan menyimpannya pada data store Pesan atau dapat mengirim ke jaringan lokal yang sudah terhubung.

Pihak penerima menentukan pesan yang akan di verifikasi, yang mana tersimpan di data store pesan. Jika penerima mengambil pesan yang bertanda tangan digital maka pesan tersebut akan dipecah secara otomatis oleh system untuk mengambil isi pesan dan tanda tangan saja. Sedangkan jika penerima mengambil pesan yang tidak ada tanda tangan digital maka pengguna perlu memasukkan tanda tangan digital secara manual untuk dilakukan proses verifikasi. System mengambil kunci dan parameter milik pengirim yang terdapat di *data store Account* yang diambil berdasarkan *username* pengirim. Validitas dari sebuah pesan ditampilkan kepada penerima yang didapat dari masukan pilihan pesan, isi pesan, tanda tangan digital, kunci publik dan parameter.

Pemisahan nilai yang didapat dari tanda tangan digital diproses untuk mendapatkan nilai C yang kemudian dicocokkan kesamaan dengan nilai B yang di dapat dari *data store Account*.



**Gambar 3.1 Data Flow Diagram**

#### 4. KESIMPULAN

Kesimpulan yang dapat ditarik dalam proses pembuatan perangkat lunak pembubuhan tanda tangan digital menggunakan metode DSS, yang terdiri dari algoritma DSA (*Digital Signature Algorithm*) dan fungsi hash satu arah (SHA) yaitu :

1. Metode kriptografi kunci-nirsimetri (*asymmetric-key cryptography*) ternyata lebih sulit untuk diimplementasikan dalam perangkat lunak, namun dapat memberikan kemudahan dan kelebihan dalam pendistribusian kunci, dan juga memenuhi aspek nirpenyangkalan
2. Algoritma DSA mampu membangkitkan tanda tangan dari berbagai macam tipe data, karena yang diproses adalah *bit* dari data. Namun, perangkat lunak hanya mampu mengambil isi tulisan dari tipe data tertentu saja.
3. Metode tanda tangan digital menggunakan algoritma DSA tidak mampu memenuhi salah satu aspek keamanan, yaitu kerahasiaan data, karena isi dari pesan dapat dilihat oleh pihak lain

## 5. DAFTAR PUSTAKA

- [1] Kurniawan, Yusuf. 2004. *Kriptografi Keamanan Internet dan Jaringan Telekomunikasi*. Bandung: Penerbit Informatika.
- [2] Munir, Rinaldi. 2006. *Kriptografi*. Bandung : Penerbit Informatika.
- [3] Murni, Aniati, *Pengantar Pengolahan Citra*, Elex Media Komputindo, 1992.
- [4] Schneier, Bruce. 1996. *Applied Cryptography. Second Edition : Protocol, Algorithms and Source Code in C*, John Wiley and Son,In.