Keamanan SIN(*Single Identification Number*) Sebagai Basis Data Terintegrasi

Deasy Ramadiyan Sari (135 03 008)

Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung
Jalan Ganesha 10 Bandung

E-mail: *if13008@students.if.itb.ac.id*

Abstrak

*Single Indetification N*umber (SIN) merupakan sebuah nomor identitas unik yang terintegrasi dengan gabungan data dari berbagai macam instansi pemerintahan dan swasta. SIN bisa digunakan di berbagai instansi, yang dirancang bisa menggantikan semua macam nomor identitas. Masalah keamanan dari SIN ini merupakan masalah penting yang harus dipertimbangkan dalam penerapan SIN di Indonesia nantinya.

Dalam hal ini sangat terkait dengan betapa pentingnya pesan, data, atau informasi tersebut di kirim dan di terima oleh pihak atau orang yang berkepentingan, apakah pesan, data, atau informasi masih authenticity. Pesan, data, atau informasi akan tidak berguna lagi apabila di tengah jalan informasi itu di sadap atau di bajak oleh orang yang tidak berhak atau berkepentingan.

Keamanan dan kerahasian data pada jaringan komputer saat ini menjadi isu yang sangat penting dan terus berkembang. Beberapa kasus menyangkut keamanan jaringan komputer saat ini menjadi suatu pekerjaan yang membutuhkan biaya penanganan dan pengamanan yang sedemikian besar. Sistem-sistem vital, seperti system pertahan, sistem perbankan, system bandara udara dan sistem-sistem yang lain setingkat itu, membutuhkan tingkat keamanan yang sedemikian tinggi. Hal ini lebih di sebabkan karena kemajuan bidang jaringan komputer dengan konsep open system-nya sehingga siapapun, di mananpun dan kapanpun, mempunyai kesempatan untuk mengakses kawasan-kawasan vital tersebut.

Untuk menjaga keamanan dan kerahasiaan pesan, data, atau informasi dalam suatu jaringan komputer maka di perlukan beberapa enkripsi guna membuat pesan, data, atau informasi agar tidak dapat di baca atau di mengerti oleh sembarang orang, kecuali untuk penerima yang berhak. Dalam tulisan ini, penulis mencoba menganalisis aplikasi sistem kriptografi yang layak diterapkan pada basis data terintegrasi di SIN

Kata kunci: *SIN, keamanan, informasi, kriptografi*

1. Pendahuluan

1.1. Latar Belakang SIN

Identitas menurut kamus bahasa Indonesia adalah keadaan, sifat, atau ciri-ciri khusus seseorang atau benda. Melalui identitas, manusia dapat dibedakan antara satu dengan yang lain.

Penduduk Indonesia dalam hal ini, juga mempunyai dokumen identitas. Dalam pembuatan dokumen identitas ini diperlukan suatu rangkaian kegiatan penataan dan penertiban melalui pendaftaran penduduk, pencatatan sipil, pengelolaan informasi penduduk serta pendayagunaan hasilnya untuk pelayanan publik dan pembangunan sektor lain. Pendaftaran penduduk merupakan pencatatan biodata penduduk, pelaporan peristiwa kependudukan, dan pendataan penduduk serta penerbitan dokumen yang berupa identitas, kartu atau surat keterangan penduduk.

Saat ini sudah ada data 29 dokumen identitas yang dikeluarkan oleh 24 instansi yang berbeda di Indonesia. Dokumen tersebut antara

lain akte kelahiran, Kartu Tanda Penduduk (KTP), Kartu Keluarga yang dikeluarkan oleh Pemerintah Daerah; Surat Izin Mengemudi (SIM), BPKB yang dikeluarkan oleh Kepolisian Indonesia; NPWP yang dikeluarkan oleh Direktorat Perpajakan; paspor yang dikeluarkan oleh Direktorat Imigrasi; serta dokumen-dokumen lain yang dikeluarkan TELKOM, PLN , PDAM, dan masih banyak lagi[01].

Minimnya koordinasi antar instansi pemerintah menyebabkan pendataan penduduk menjadi tidak efektif. Penduduk biasanya diharuskan untuk mendaftar berkali-kali kepada instansi yang berbeda dengan metode yang berbeda pula sementara data yang diberikan adalah sama [03]. Sebagai contoh, dalam membuat sebuah KTP biasanya penduduk harus memberikan data berupa nama, alamat, tanggal lahir, umur, golongan darah, jenis kelamin, dll. Sementara jika penduduk yang sama ingin membuat SIM di kepolisian setempat, data yang diperlukan serupa dengan data pada saat membuat KTP. Fenomena ini tidak hanya menyebabkan penduduk menjadi kewalahan karena harus mengurus dokumen identitas yang dikeluarkan oleh beragam instansi, tapi juga menyebabkan penggunaan sumberdaya pada satu instansi menjadi kurang efisien.

Untuk mengatasi hal tersebut, perlu satu referensi untuk mendapatkan data kependudukan yang akurat. Referensi itu dapat terwujud jika ada satu-satunya Single Identification Number(SIN) sesuai dengan Inpres No. 3/2003[05] dan Kepres No.72/2004 dalam rangka mengembangkan e-goverment di Indonesia melalui SIN yang direncanakan efektif berjalan pada 2006[06].

IDENTITAS UNIK YANG ADA DI INDONESIA

Basis Informasi	Dokumen	Identitas	Istansi
Personal (Kependudukan)	KTP	Nomor KTP	Pemda
Personal (Kependudukan)	Kartu Keluarga	Nomor KK	Pemda
Personal	Paspor	Nomor Paspor	Imigrasi
Personal	SIM	Nomor SIM	Kepolisian
Personal	BPKB	Nomor BPKB	Kepolisian
Personal	NPWP	Nomor NPWP	Ditjen Pajak
Personal	N.I.P	No. Induk Pegawai	BAKN
Personal	N.R.P.	No. Regist. Prajurit	Dephan/TNI
Personal	Perbankan	No. Kartu Kredit	Bank
Personal	Asuransi	Nomor Polis	Persh. Asuransi
Personal	Asuransi	Nomor ASKES	DEPKES
Personal	Asuransi	Nomor ASTEK	DEPNAKERTRANS
Personal	Akta Kelahiran	No. Akta Kelahr.	Ktr. Catatan Sipil
Personal	Akta Nikah	No. Akta Nikah	DEPAG
Bidang	Sertifikat HAT	Nomor Sertifikat	BPN
Bidang	IMB	Nomor IMB	Pemda
Bidang	SPPT	Nomor SPPT (NOP)	Ditjen Pajak
Bidang	Tagihan Listrik	Nomor Pelangan	PLN
Bidang	Tagihan Telepon	Nomor Pelanggan	TELKOM
Bidang	Tagihan PDAM	Nomor Pelanggan	PDAM
Bidang	Tagihan Gas	Nomor Pelanggan	Perum GAS
Bidang	Aset Daerah	No. Invent. Aset Daerah	Pemda
Bidang	Aset negara	No. Invent. Aset Negara	Pem. Pusat
Bidang & Personal	Sensus	Nomor Sensus	BPS
Bidang & Personal	Perusahaan	Nomor SIUP	DEPERINDAG
Bidang & Personal	Perusahaan	No. Surat Ijin Tempat Usaha	Pemda
Bidang & Personal	Perusahaan	Akte Pendirian Persh.	Dept. Kehakiman

Gambar 1 Identitas Di Setiap Instansi

Sebagai data yang digunakan secara bersama, faktor keamanan sangat perlu dipertimbangkan dalam pertukaran data. Ada beberapa organisasi yang mempunyai hak akses dalam memasukkan data, melakukan perubahan data, dan menampilkan data. Ada juga beberapa organisasi yang hanya diberikan hak akses untuk dapat menampilkan dan melihat data tanpa dapat melakukan perubahan terhadap data. Data yang ditampilkan pun bukan merupakan keseluruhan data dari seseorang, tetapi hanya data yang terkait dengan organisasi tersebut. Di lain pihak, ada juga organisasi atau perorangan yang sama sekali tidak diberikan akses untuk melihat data, tetapi berusaha untuk melihat data seseorang. Tidak hanya melihat mungkin, tapi juga mampu untuk melakukan perubahan yang tidak bertanggung jawab terhadap data terkait. Hal ini merupakan salah satu yang perlu dipertimbangkan dalam penerapan SIN di Indonesia, yaitu keamanan SIN.

1.2. Single Identity

Identitas adalah representasi dari suatu kesatuan di suatu domain aplikasi tertentu. Sebagai contoh, pendaftaran data pribadi dari sebuah konsumen bank dan mungkin juga karakteristik fisik yang dimiliki oleh pelanggan yang diamati oleh staff bank. Itu yang mendasari identitas dari pelanggan dengan domain dari bank. Identitas pada umumnya terhubung dengan dunia nyata. Dunia nyata biasanya adalah organisasi atau orang-orang.

Asumsi penyederhanaan single identity tidak bisa dihubungkan dengan lebih dari satu entity.

Berbagi entity dimungkinkan contohnya kartu keluarga yang terhubung dengan beberapa orang dalam sebuah keluarga. Bagaimanapun, sejauh penyedia layanan sepakat sebagai satu entity (keluarga) dan bukan dengan banyak individu.

Seseorang atau organisasi mungkin punya nol atau lebih identitas di dalam suatu domain yang diberikan. Sebagai contoh, seseorang mungkin punya dua identitas di suatu sistem persekolahan karena dia adalah orangtua dan seorang guru di sekolah itu. Aturan untuk pendaftaran identitas di dalam suatu domain menentukan apakah banyak identitas untuk satu entity diijinkan. Sekalipun tidak diperbolehkan, banyak identitas untuk entity yang sama masih bisa terjadi di sistem itu, contohh karena kesalahan atau penipuan.

Seseorang boleh saja mempunyai identitas berbeda di domain yang berbeda. Sebagai contoh, seseorang mungkin punya satu identitas yang berhubungan denga pelanggan di suatu bank dan identitas yang lain berhubungan dengan menjadi pelanggan di suatu operator jasa telekomunikasi.

Sistem manajemen identitas ”tradisional” dibuat untuk lebih hemat biaya dan scalable terutama untuk penyedia jasa, tetapi tidak unuk pengguna. Sebagai contoh pengguna harus mengingat berbagai macam password untuk mengakses layanan yang berbeda dengan identitas yang berbeda domain. Shingga ini mengakibatkan ketidaknyamanan bagi pengguna. Pelayanan berbeda mengakibatkan penggunaan identitas dan/atau password yang berbeda pula (multiple identity)

Pengaturan identitas secara tradisional itu dilihat dari sisi penyedia jasa, yang artinya aktivitas yang dikerjakan oleh penyedia jasa untuk mengatur pemakai jasa identitas.

Mengatur identitas adalah suatu proses yang sulit namun dapat dibuat menjadi lebih mudah dengan menggunakan teknologi. Tetap ini bukan hanya mengembahkan suatu bagian teknologi dimana orang-orang yang menggunakannya untuk mengatur identitas. Sudah ada sejumlah produk yang dapat membantu seperti direktori, database, personal organizer, dan smart card. Apa yang diperlukan adalah suatu frameweork dimana produk ini dapat bekerja, dan dimana produk dan jasa baru dapat dikembangkan jika memang diperlukan.

Untuk mendapatkan nilai lebih dari investasi IT, banyak bisnis yang sedang mencari cara yang berbeda dan baru untuk mengintegrasikan sumber daya IT dan membuat seragam dalama ketersediaan melalui organisasi atau perusahaan dengan mengoptimalkan keperluan dari sumber daya IT.

Dengan menggunakan IT, dan pengembangan IT yang melibatkan sisi pandang penggunanya, maka Single Identity mengalami pergeseran fungsi, sehingga pengguna dapat menggunakan satu identitas tunggal di berbagai macam domain.

Single Identity ini membantu bisnis memenuhi kebutuhan bisnis yang penting:

- Meningkatkan Kualitas Layanan Bisnis

Single identity penanganannya tepat waktu, up-to-date, dan data identitas yang dapat dipercaya oleh aplikasi bisnis yang membuat.

- Mengurangi Manajemen Biaya

Dengan menyediakan suatu pendekatan yang lebih holistik untuk mengatur data identitas dan single identitas dapat mengurangi pemborosan pembiayaan, ketidakefisienan, dan ketidakcocokan di data identitas.

- Mengurangi Resiko

Single Identity dapat membantu bisnis mengurangi resiko dapat membuka organisasi mereka.

- Memperkuat Pemenuhan Legislatif

Single Identity dapat membantu bisnis mematuhi keinginan pemerintah yang sekarang, untuk merancang perundang-undangan yang melindungi konsumen dari penyingkapan yang disengaja maupun tidak disengaja tentang informasi pribadi.

2. Tinjauan Pustaka

Pada dasarnya keamanan dan kerahasian suatu pesan, data, ataupun informasi adalah merupakan hal yang mutlak yang harus kita lakukan. Sedangkan alat untuk melakukan pengamanan data dalam sistem komunikasi jaringan komputer sering disebut cryptography. Kriptografi (cryptography) merupakan ilmu dan seni penyimpanan pesan, data, atau informasi secara aman. Kritptanalisis (cryptanalysis) merupakan ilmu dan seni pembongkaran pesan, data, atau informasi rahasia seperti di atas. Kriptologi (cryptology) adalah panduan dari kriptografi dan kriptanalist. Fungsi-fungsi yang mendasar dalam kriptografi adalah enkripsi dan dekripsi.

Enkripsi adalah proses mengubah suatu pesan, data, atau informasi asli (plaintext) menjadi suatu pesan, data, atau informasi dalam bahasa sandi (ciphertext). Sedangkan dekripsi adalah proses mengubah pesan, data, atau informasi dalam suatu bahasa sandi kembali menjadi pesan, data, atau informasi asli. Berikut ini adalah hal-hal penting yang dicakup dan sering dibahas dalam teori kriptografi.

2.1 Kunci Simetris

Algoritma kriptografi (*cipher*) simetri dapat dikelompokkan menjadi dua kategori, yaitu:

1. *Cipher* aliran (*stream cipher*)
   Algoritma kriptografi beroperasi pada plainteks/cipherteks dalam bentuk bit tunggal, yang dalam hal ini rangkaian bit dienkripsikan/didekripsikan bit per bit.
2. *Cipher* blok (*block cipher*)
   Algoritma kriptografi beroperasi pada plainteks/cipherteks dalam bentuk blok bit, yang dalam hal ini rangkaian bit dibagi menjadi blok-blok bit yang panjangnya sudah ditentukan sebelumnya.

2.2 Kunci Asimetris

Kunci asimetris adalah pasangan kunci kriptografi yang salah satunya digunakan untuk proses enkripsi dan yang satu lagi untuk dekripsi. Semua orang yang mendapatkan kunci publik dapat menggunakannya untuk mengenkripsikan suatu pesan, data ataupun informasi, sedangkan hanya satu orang saja yang memiliki rahasia tertentu dalam hal ini kunci privat untuk melakukan pembongkaran terhadap sandi yang dikirim untuknya. Contoh algoritma terkenal yang menggunakan kunci asimetris adalah RSA.

2.3 Fungsi Hash Satu Arah

Fungsi hash satu arah (one-way hash function) digunakan untuk membuat sidik jari (fingerprint) dari suatu dokumen atau pesan X. Pesan X (yang besarnya dapat bervariasi) yang akan di-hash disebut pre-image, sedangkan outputnya yang memiliki ukuran tetap, disebut hash-value (nilai hash). Fungsi hash dapat diketahui oleh siapapun, tak terkecuali, sehingga siapapun dapat memeriksa keutuhan dokumen atau pesan X tersebut. Tak ada algoritma rahasia dan umumnya tak ada pula kunci rahasia. Contoh algoritma fungsi hash satu arah adalah MD-5 dan SHA. Message Authentication Code (MAC) adalah salah satu variasi dari fungsi hash satu arah, hanya saja selain pre-image, sebuah kunci rahasia juga menjadi input bagi fungsi MAC.

2.4 Tanda Tangan Digital

Selama ini, masalah tanda tangan digital masih sering di permasalahkan keabsahannya, hal ini terjadi karena pengertian dan konsep dasarnya belum dipahami. Penandatanganan digital terhadap suatu dokumen adalah sidik jari dari dokumen tersebut beserta timestamp-nya di enkripsi dengan menggunakan kunci privat pihak yang menandatangani. Tanda tangan digital memanfaatkan fungsi hash satu arah untuk menjamin bahwa tanda tangan itu hanya berlaku untuk dokumen yang bersangkutan saja. Keabsahan tanda tangan digital itu dapat diperiksa oleh pihak yang menerima pesan.

2.5 Masalah Pertukaran Kunci Publik

Misalkan ada dua pihak : Alice dan Bob, Alice hendak mengirimkan suatu dokumen rahasia melalui jaringan komputer kepada Bob. Maka sebelumnya Bob harus mengirimkan kunci publiknya kepada Alice agar Alice dapat melakukan enkripsi yang pesannya hanya dapat dibuka oleh Bob. Demikian juga pula sebaliknya, Alice harus mengirimkan kepada Bob kunci publiknya agar Bob dapat memeriksa keaslian tanda tangan Alice pada pesan yang dikirim. Dengan cara ini Alice dapat memastikan pesan itu sampai ke tujuannya, sedangkan Bob dapat merasa yakin bahwa pengirim pesan itu adalah Alice. Alice dan Bob bisa mendapatkan masing-masing kunci publik lawan bicaranya dari suatu pihak yang dipercaya, misalnya X. Setiap anggota jaringan diasumsikan telah memiliki saluran komunikasi pribadi yang aman dengan X.

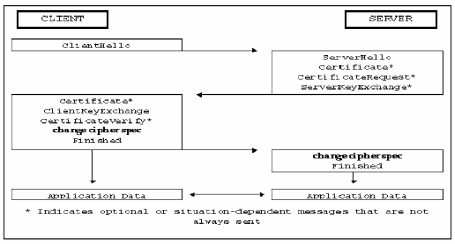
2.6 Sertifikat Digital

Sertifikat digital adalah kunci publik dan informasi penting mengenai jati diri pemilik kunci publik, seperti misalnya nama, alamat, pekerjaan, jabatan, perusahaan dan bahkan hash dari suatu informasi rahasia yang ditandatangani oleh suatu pihak terpercaya. Sertifikat digital tersebut ditandatangani oleh

sebuah pihak yang dipercaya yaitu Certificate Authority (CA).

2.7 Secure Socket Layer (SSL)

SSL dapat menjaga kerahasiaan (confidentiality) dari informasi yang dikirim karena menggunakan teknologi enkripsi yang maju dan dapat di-update jika ada teknologi baru yang lebih bagus. Dengan penggunaan sertifikat digital, SSL menyediakan otentikasi yang transparan antara client dengan server. SSL menggunakan algoritma RSA untuk membuat tanda tangan digital (digital signature) dan amplop digital (digital envelope). Selain itu, untuk melakukan enkripsi dan dekripsi data setelah koneksi dilakukan, SSL menggunakan RC4 sebagai algoritma standar untuk enkripsi kunci simetri. Saat aplikasi menggunakan SSL, sebenarnya terjadi dua kondisi, yakni handshake dan pertukaran informasi.



Gambar II Security Handshake

Biasanya, browser-browser seperti Netscape Navigator atau Microsoft Internet Explorer sudah menyertakan sertifikat digital dari CA utama yang terkenal, sehingga memudahkan pemeriksaan sertifikat digital pada koneksi SSL. Penyertaan serfikat digital CA utama pada browser akan menghindarkan client dari pemalsuan sertifikat CA utama.

2.8 Serangan Pertukaran Pesan Melalui Jaringan Komputer

Keseluruhan *point* dari kriptografi adalah menjaga kerahasiaan plainteks atau kunci (atau keduanya) dari penyadap (*eavesdropper*) atau kriptanalis (*cryptanalyst*).

Kriptanalis berusaha memecahkan cipherteks dengan suatu serangan terhadap sistem kriptografi.

Serangan adalah setiap usaha (*attempt*) atau percobaan yang dilakukan oleh kriptanalis untuk menemukan kunci atau menemukan plainteks dari cipherteksnya.

Berdasarkan keterlibatan penyerang dalam komunikasi:

1. Serangan Pasif (*passive attack*)
- penyerang tidak terlibat dalam komunikasi antara pengirim dan penerima
- penyerang hanya melakukan penyadapan untuk memperoleh data atau informasi sebanyak-banyaknya

2. Serangan Aktif (*active attack*)
- Penyerang mengintervensi komunikasi dan ikut
- mempengaruhi sistem untuk keuntungan dirinya
- penyerang mengubah aliran pesan seperti:
  - menghapus sebagian cipherteks
  - mengubah cipherteks
  - menyisipkan potongan cipherteks palsu,
  - me-*replay* pesan lama
  - mengubah informasi yang tersimpan, dsb

Berdasarkan bagaimana cara dan posisi seseorang mendapatkan pesan-pesan dalam saluran komunikasi, penyerangan dapat dikategorikan menjadi:

1. Sniffing
Sniffing secara harafiah berarti mengendus, tentunya dalam hal ini yang diendus adalah pesan (baik yang belum ataupun sudah dienkripsi) dalam suatu saluran komunikasi. Hal ini umum terjadi pada saluran publik yang tidak aman. Sang pengendus dapat merekap pembicaraan yang terjadi.

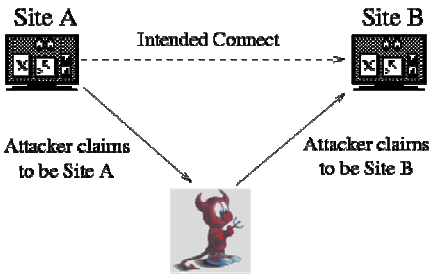
2. Replay attack
Jika seseorang bisa merekam pesan-pesan handshake (persiapan komunikasi), ia mungkin dapat mengulang pesan-pesan yang telah direkamnya untuk menipu salah satu pihak.

3. Spoofing
Penyerang – misalnya C – bisa menyamar menjadi A. Semua orang dibuat percaya bahwa C adalah A. Penyerang berusaha meyakinkan pihak-pihak lain bahwa tak ada salah dengan komunikasi yang dilakukan, padahal komunikasi itu dilakukan dengan sang penipu/penyerang. Contohnya jika orang memasukkan PIN ke dalam Card Acceptance Device (CAD) – yang benar-benar dibuat

seperti CAD asli – tentu sang penipu bisa mendapatkan PIN pemilik smartcard. Pemilik smartcard tidak tahu bahwa telah terjadi kejahatan.

4. Man-in-the-middle

Jika spoofing terkadang hanya menipu satu pihak, maka dalam skenario ini, saat A hendak berkomunikasi dengan B, C di mata A seolah-olah adalah B, dan C dapat pula menipu B sehingga C seolah-olah adalah A. C dapat berkuasa penuh atas jalur komunikasi ini, dan bisa membuat berita fitnah. Kabel koaksial yang sering digunakan pada jaringan sangat rentan terhadap serangan vampire tap, yakni perangkat keras sederhana yang bisa menembus bagian dalam kabel koaksial sehingga dapat mengambil data yang mengalir tanpa perlu memutuskan komunikasi data yang sedang berjalan. Seseorang dengan vampire tap dan komputer jinjing dapat melakukan serangan pada bagian apa saja dari kabel koaksial.



Gambar III Man in The Middle

Berdasarkan teknik yang digunakan untuk menemukan kunci:

1. Exhaustive attack /brute force attack

Mengungkap plainteks/kunci dengan mencoba semua kemungkinan kunci.
Pasti berhasil menemukan kunci jika tersedia waktu yang cukup

2. Analytical attack

Menganalisis kelemahan algoritma kriptografi untuk mengurangi kemungkinan kunci yang tidak mungkin ada.
Caranya: memecahkan persamaan-persamaan matematika (yang diperoleh dari definisi suatu algoritma kriptografi) yang mengandung peubah-peubah yang merepresentasikan plainteks atau kunci.
Metode *analytical attack* biasanya lebih cepat menemukan kunci dibandingkan dengan *exhaustive attack*.

Data yang digunakan untuk menyerang sistem kriptografi:

1. *Chipertext only.*
2. *Known plaintext* dan *corresponding chipertext*.
3. *Chosen plaintext* dan *corresponding chipertext*.
4. *Chosen chipertext* dan *corresponding plaintext*.

Berdasarkan ketersediaan data:

1. Chipertext-only attack

- Kriptanalis hanya memiliki cipherteks
- Teknik yang digunakan: *exhaustive key search*

2. Known-plaintext attack

- Diberikan:
  $P1, C1 = Ek(P1), P2, C2 = Ek(P2), \ldots Pi, Ci = Ek(Pi)$
- Deduksi: k untuk mendapatkan $Pi+1$ dari $Ci+1 = Ek(Pi+1)$.

3. Chosen-plaintext attack

Kriptanalis dapat memilih plainteks tertentu untuk dienkripsikan, yaitu plainteks-plainteks yang lebih mengarahkan penemuan kunci.

4. *Adaptive-chosen-plaintext attack*

Kriptanalis memilih blok plainteks yang besar, lalu dienkripsi, kemudian memilih blok lainnya yang lebih kecil berdasarkan hasil serangan sebelumnya, begitu seterusnya.

5. *Chosen-ciphertext attack*

- Diberikan:

1 $C1, P1 = Dk(C1), C2, P2 = Dk(P2), Ci, Pi = Dk(Ci)$

- Deduksi: k (yang mungkin diperlukan untuk mendekripsi pesan pada waktu yang akan datang).

6. *Chosen-key attack*

Kriptanalis memiliki pengetahuan mengenai hubungan antara kunci-kunci yang berbeda, dan memilih kunci yang tepat untuk mendekripsi pesan

7. *Rubber-hose cryptanalysis*

Mengancam, mengirim surat gelap, atau melakukan penyiksaan sampai orang yang memegang kunci memberinya kunci untuk mendekripsi pesan

Penyerang juga bisa mendapatkan kunci dengan cara yang lebih tradisional, yakni dengan melakukan penyiksaan, pemerasan, ancaman, atau bisa juga dengan menyogok seseorang yang memiliki kunci itu. Ini adalah cara yang paling ampuh untuk mendapat kunci.

Sebuah algoritma kriptografi dikatakan aman (*computationally secure*) bila ia memenuhi tiga kriteria berikut:

1. Persamaan matematis yang menggambarkan operasi algoritma kriptografi sangat kompleks sehingga algoritma tidak mungkin dipecahkan secara analitik.
2. Biaya untuk memecahkan cipherteks melampaui nilai informasi yang terkandung di dalam cipherteks tersebut.
3. Waktu yang diperlukan untuk memecahkan cipherteks melampaui lamanya waktu informasi tersebut harus dijaga kerahasiaannya.

2.9 Konsep Single Identification Number

Konsep SIN diwujudkan dengan suatu nomor unik yang terpadu dalam satu kartu identitas yang diberikan kepada seorang warga negara yang telah memenuhi syarat sesuai peraturan perundangan yang berlaku.

SIN dianggap sebagai pendekatan terbaik karena SIN bersifat sebagai "kode pemersatu" yang menyatukan berbagai sistem informasi kependudukan yang dimiliki instansi-instansi tanpa merombak bentuk dasar dari sistem database instansi tersebut.

Contoh paling dekat dengan konsep SIN ini adalah Nomor Induk Kependudukan (NIK) yang selama ini melekat pada Kartu Tanda Penduduk (KTP). Sampai saat ini belum ada mekanisme yang bisa enjamin tidak terjadinya NIK ganda atau KTP ganda.

Di sisi lain, hampir semua transaksi layanan publik, seperti pembuatan Surat Izin Mengemudi (SIM), passport, sertifikat tanah, dll., harus menyertakan KTP. Kalau dari hulunya sudah tidak ada mekanisme yang bisa menjamin identitas tunggal, maka seluruh identitas turunannya juga sulit untuk bisa dilakukan verifikasi, authentikasi, dan validasi. Akibat selanjutnya, hal ini dapat menimbulkan ancaman terhadap keamanan negara, karena seseorang bisa memperoleh identitas ganda.

Penerapan konsep SIN dinegara seperti Indonesia yang penduduknya lebih dari 200 juta orang dengan letak geografisnya yang tersebar di ribuan pulau-pulau, bukanlah hal yang mudah. Pengalaman beberapa negara yang telah menerapkan identitas tunggal dan mempunyai database nasional kependudukan, menjadi "guru" yang baik untuk dipelajari.

3. Analisis

3.1 Linkungan Pengguna SIN

Ada banyak pihak yang terlibat dalam sistem SIN, baik dari segi pembuatan, penggunaan, maupun pengaksesan. Diantaranya adalah pihak pembuat SIN dalam bentuk kartu atau *chip* yang diletakkan pada kartu, pihak pembuat perangkat lunak SIN, pihak pemegang kartu, pemilik data SIN, 27 instansi yang terkait secara langsung dari segi pengaksesasn data, pusat penyimpanan data SIN, dan pihak yang mengatur sistem operasi dari SIN.

1. Pihak pembuat SIN
   Merupakan pihak yang membuat SIN dalam bentuk chip yang diletakkan pada kartu. Dalam hal ini, pihak pembuat kartu belum tentu pihak yang memiliki pabrik pembuatan atau pemilik teknologi. Desain kartu atau proses pembuatan kartu bisa saja menggunakan tools dari pihak lain. (*third party*).

2. Pihak pembuat perangkat lunak SIN
   Pihak ini merupakan pihak yang membuat perangkat lunak yang berjalan di dalam SIN. Sama halnya dengan pembuat kartu, pihak pembuat perangkat lunak dapat menggunakan tools pihak lain (compiler, dll) untuk membuat perangkat lunak.

3. Pihak pemegang kartu
   Pihak yang sedang membawa kartu tersebut, baik itu adalah pihak yang mempunyai data ataupun bukan. Pemegang kartu hanya merupakan pihak yang memiliki kartu saja. Pihak ini tidak memiliki kontrol terhadap protokol, perangkat lunak, atau perangkat keras dari kartu.

4. Pihak pemilik data

Pihak yang merupakan pemilik dari data-data yang terkandung pada basisdata.

5. Instansi yang terkait
   Instansi terkait yang mengakses data untuk keperluan dari pihaknya.
6. Terminal
   Pihak ini adalah pihak yang menjembatani interaksi kartu dengan dunia luar. Semua input output ke dan dari kartu dikontrol oleh pihak ini. Contoh: keyboard, perangkat yang memungkinkan data dimasukkan ke dalam kartu; Layar, jika data yang ada di kartu ditampilkan; ATM service provider, jika kartu digunakan sebagai kartu ATM.
7. Pihak yang mengatur system operasi dari SIN
   Pihak ini menginisialisasi data yang disimpan apda kartu. Jika kartu adalah kartu pembayaran telepon maka pihak pengaturnya adalah perusahaan telekomunikasi. Dalam beberapa kasus, pihak pengatur hanya menerbitkan kartu saja dan tidak terkait lagi dengan kartu.

Berdasarkan banyaknya jumlah dari pihak yang terlibat dalam sistem SIN ini, ada banyak jenis serangan yang perlu dipertimbangkan. Tujuannya disini adalah mengelaskan jenis serangan tersebut berdasarkan perbedaan fungsi. Yaitu melihat jenis serangan ini dari pihak yang terlibat dalam system ini terhadap pihak lainnya.

1. Serangan oleh Pihak Terminal terhadap Pihak Pemegang Kartu atau Pihak Pemilik Data
   Pihak terminal dapat melakukan perubahan data atau penyimpanan atau penyediaan data yang tidak benar. Hal ini dapat menyebabkan data yang dimiliki oleh pihak pemilik data tidak benar. Contoh: jika kartu digunakan sebagai alat pembayaran vending machine. Pihak terminal (dalam hal ini perangkat lunak vending machine) dapat saja mencatat data yang tidak benar terhadap pembayaran yang dilakukan pengguna kartu. Hal lain yang dapat terjadi adalah data yang ditampilkan oleh vending machine merupakan data yang tidak benar. Misalkan sisa credit dari kartu ditampilkan tidak benar.
2. Serangan oleh Pemegang Kartu terhadap Pihak Terminal
   Pihak pembuat kartu dapat melakukan manipulasi terhadap kartu sehingga data yang dikenali oleh pihak terminal merupakan data yang tidak benar. Contoh: pihak pemegang kartu yang pandai dapat melakukan manipulasi terhadap protokol komunikasi antara kartu dan terminal sehingga dapat menguntungkan pihak pemegang kartu.
3. Serangan oleh Pemegang Kartu terhadap Pihak Pemilik Data
   Pihak pemegang kartu seharusnya tidak memiliki otoritas terhadap data yang dimiliki oleh pihak pemilik data. Contoh: pihak pemegang kartu ATM dimana kartu ATM tersebut dimiliki oleh orang lain. Namun seringkali pihak pemegang kartu memegang suatu data penting yang memungkinkan pihak pemegang kartu dapat mengakses data yang dimiliki oleh pihak pemilik data. Contoh sederhana adalah pin ATM. Pihak pemegang kartu yang mengetahui pin ATM dapat melakukan manipulasi data yang terhadap rekening seseorang (pemilik data).
4. Serangan oleh Pemegang Kartu terhadap Pihak yang mengatur sistem operasi di SIN
   Pihak pengatur sistem operasi pada awalnya sudah memasukkan data di dalam kartu. Data tersebut merupakan data identitas dari pemilik data. Pihak pemegang kartu merupakan pihak yang memegang kartu dan belum tentu pihak pemilik data sehingga penggunaan kartu (data dalam kartu) oleh pemegang kartu yang bukan pemilik data dapat membuat pihak pengatur sistem operasi kartu bingung akan kepemilikan kartu.
5. Serangan oleh Pemegang Kartu terhadap Pihak Pembuat Perangkat Lunak SIN
   Pada dasarnya kartu yang dipegang sudah memiliki perangkat lunak yang tertanam di dalamnya. Dalam hal ini pihak pembuat perangkat lunak bertanggung jawab atas

perangkat lunak yang ada di kartu. Oleh karena itu, pihak pemegang kartu seharusnya tidak memiliki akses untuk mengubah perangkat lunak yang ada di dalam kartu.
Namun tak jarang pihak pemegang kartu memiliki kemampuan untuk melakukan hal tersebut, sehingga perangkat lunak yang ada di dalam kartu bukan lagi merupakan perangkat lunak yang dibuat oleh pihak pembuat perangkat lunak.

6. Serangan oleh Pihak Terminal terhadap Pihak yang mengatur sistem operasi di SIN
   Pihak terminal merupakan pihak yang mengatur komunikasi antara pihak pemegang kartu dan pihak pengatur sistem operasi kartu. Terminal berfungsi untuk memfasilitasi transaksi yang dilakukan terhadap data. Pihak terminal bisa saja melakukan kecurangan dengan cara menyimpan data yang tidak konsisten satu sama lain, sehingga dapat membuat informasi yang diperoleh oleh pihak pengatur sistem operasi tidak benar.

7. Serangan dari Pihak yang mengatur sistem operasi di SIN terhadap Pihak Pemegang Kartu

   Pihak pengatur sistem operasi merupakan pihak yang menerbitkan kartu yang dimiliki oleh pihak pemegang kartu. Pihak pengatur sistem operasi seharusnya dapat menjaga agar data yang dimiliki oleh pihak pemegang kartu terjamin keamanannya.

8. Serangan dari Pihak Pembuat SIN terhadap Pemilik Data
   Pihak pembuat kartu dapat melakukan serangan dengan melakukan desain yang buruk terhadap kartu yang dibuat. Hal ini dapat berakibat data yang disimpan di dalam kartu tidak terjamin keamanannya, atau tidak bekerja sesuai protokol yang seharusnya, atau kartu mudah rusak hanya dengan beberapa kali pemakaian, dll. Hal ini tentu saja dapat merugikan pihak pemilik data.

4. Keamanan

Tujuan paling realistis bisa dilakukan oleh desainer sistem keamanan adalah untuk menjamin bahwa usaha yang dilakukan untuk menyerang sistem itu lebih mahal dari hasil yang akan didapat. Hal ini akan membuat orang menjadi tidak tertarik untuk menyerang sistemnya. Ada banyak cara untuk melakukannya, antara lain:

- Membatasi bagian sistem yang terpengaruh ketika diserang.harus ada pembagian sistem sehingga kehilangan satu data hanya mempengaruhi subsistem saja
- Membatasi lifespan suatu sistem. Hal ini bisa dicapai dengan cara mengurangi jangka waktu kunci Dan data kritis lainnya.
- Membatasi jumlah resiko, dengan cara mengasosiasikan tingkat akses data di sistem dengan tingkat keamanan yang dipunyai di kartu
- Mengurangi motivasi penyerangan, dengan cara hanya berhubungan dengan komunitas orang-orang yang bisa dipercaya yang mempunyai sistem kontrol.

4.1 Kriteria

Dalam usaha untuk membuat sistem keamanan yang baik, tentu saja perlu suatu perencanaan. Lalu hal yang pertama kali dilakukan dalam perencanaan adalah menentukan kebutuhan dasar keamanan yang diperlukan. Karena keamanan bisa mempunyai arti yang berbeda bagi tiap orang. Tapi berikut ini adalah beberapa kriteria yang bisa dipilih untuk menentukan tingkat keamanan yang diperlukan:

a. *Safety*, meliputi tingkat keselamatan manusia dan tindakan yang dilakukan untuk tiap resiko yang
mungkin terjadi.

b. *Nondelivery* yaitu resiko kehilangan data (transaksi) ketika terjadi komunikasi antar sistem. Perencanaan mekanisme deteksi resiko ini sangat penting.

c. *Accuracy*, berurusan kemungkinan kesalahan yang terjadi ketika penyimpanan dan pertukaran data.
Pengaruhnya tergantung dari jenis data yang bersangkutan.

d. *Data Integrity*, mengatur integritas data yang disimpan dari pengubahan data baik yang

sengaja maupun tidak. Pengubahan ini kemungkinan besar akan terjadi. Oleh karena itu, sistem harus bisa menananganinya dengan baik.

e. *Confidentiality*, menangani keamanan kerahasiaan informasi yang terkandung baik di kartu dan sistem yang berhubungan dengannya. Kebocoran yang terjadi mungkin karena kesalahan logic sistemnya atau ada kelemahan dalam sistem yang akhirnya disalahgunakan.

f. *Impersonation*, resiko yang terjadi jika ada orang yang tidak mempunyai hak akses tetapi menggunakan kartu tersebut.

g. *Repudiation*, harus ada meknisme pembuktian bahwa suatu transaksi terjadi dengan menggunakan kartu ayng bersangkutan. Mekanisme ini biasanya dilakukan dengan digital signature menggunakan kriptografi kunci publik.

4.2 Model

Sistem keamanan sendiri bisa dimodelkan tingkat keamanannya berdasarkan proses yang dialami oleh
suatu data yaitu *Storage*, *Transmission*, dan *Use*.

4.2.1. Storage

Jika suatu data harus bisa diakses secara *offline* dan harus portable, maka sebaiknya disimpan di *smart card* . Sebaliknya data lainnya lebih baik disimpan di komputer dan *smart card* dapat digunakan untuk mengaksesnya. Data dibuat agar tidak dapat dimengerti oleh orang lain dengan enkripsi. Data juga harus dicek apakah tidak terjadi perubahan yang tidak diinginkan atau kesalahan baik fungsi dan operasi di sistem

4.2.2. Transmission

Proses pengiriman data juga harus dicek untuk menjaga tidak adanya perubahan baik sengaja atau tidak. Pengecekan ini biasanya dilakukan dengan *cyclic redundancy check* (CRC), *transaction counter*,
dan *message authentication check* (MAC).

4.2.3. Use

Harus ada pengecekan untuk menjamin bahwa orang yang menggunakan adalah *cardholder* sebenarnya.
Ada berbagai macam cara antara lain:

- Tanda tangan dan foto digunakan untuk pengecekan secara manual untuk kondisi dimana terjadi komunikasi tatap muka
- Teknik menggunakan *Personal Identification Number* (PIN). Walaupun mempunyai banyak
- keterbatasan, teknik ini mempunyai catatan yang baik karena teknik ini mudah diimplementasikan dan diterima dengan baik oleh konsumen.
- Teknik menggunakan pengecekan biometris untuk tingkat keamanan yang lebih baik.

5. Algoritma

5.1 Penjelasan Algoritma

RC4 merupakan salah satu jenis *stream cipher*, yaitu memproses unit atau input data, pesan atau informasi pada satu saat. Unit atau data pada umumnya sebuah *byte* atau bahkan kadang kadang bit (*byte* dalam hal RC4). Dengan cara ini enkripsi atau dekripsi dapat dilaksanakan pada panjang yang variabel.

Algoritma ini tidak harus menunggu sejumlah input data, pesan atau informasi tertentu sebelum diproses, atau menambahkan byte tambahan untuk mengenkrip. Contoh *stream cipher* adalah RC4, Seal, A5, Oryx, dan lain-lain. Tipe lainnya adalah *block cipher* yang memproses sekaligus sejumlah tertentu data (biasanya 64 bit atau 128 bit blok), contohnya : Blowfish, DES, Gost, Idea, RC5, Safer, Square, Twofish, RC6, Loki97, dan lain-lain.

RC4 merupakan enkripsi *stream simetrik proprietary* yang dibuat oleh *RSA Data Security Inc* (RSADSI). Penyebarannya diawali dari sebuah source code yang diyakini sebagai RC4 dan dipublikasikan secara '*anonymously*' pada tahun 1994. Algoritma yang dipublikasikan ini sangat identik dengan implementasi RC4 pada produk resmi.

RC4 digunakan secara luas pada beberapa aplikasi dan umumnya dinyatakan sangat aman. Sampai saat ini diketahui tidak ada yang dapat memecahkan/membongkarnya, hanya saja versi ekspor 40 bitnya dapat dibongkar dengan cara "*brute force*" (mencoba semua kunci yang mungkin). RC4 tidak dipatenkan oleh RSADSI, hanya saja tidak diperdagangkan secara bebas (*trade secret*).

Algoritma RC4 cukup mudah untuk dijelaskan. RC4 mempunyai sebuah *S-Box*, $S_0,S_1,...,S_{255}$, yang berisi permutasi dari bilangan 0 sampai 255, dan permutasi merupakan fungsi dari kunci dengan panjang yang variabel. Terdapat dua indeks yaitu i dan j, yang diinisialisasi

dengan bilangan nol. Untuk menghasilkan random byte langkahnya adalah sebagai berikut :

$i = (i + 1) \bmod 256$
$j = (j + S_i) \bmod 256$
swap S_i dan S_j
$t = (S_i + S_j) \bmod 256$
$K = S_t$

Byte K di XOR dengan *plaintexs* untuk menghasilkan *cipherteks* atau di XOR dengan cipherteks untuk menghasilkan plainteks. Enkripsi sangat cepat kurang lebih 10 kali lebih cepat dari DES.

Inisialisasi S-Box juga sangat mudah. Pertama isi secara berurutan $S_0 = 0$, $S_1 = 1$,...,$S_{255} = 255$. Kemudian isi array 256 byte lainnya dengan kunci yang diulangi sampai seluruh array K_0, K_1,...,K_{255} terisi seluruhnya. Set indeks j dengan nol, Kemudian lakukan langkah berikut :

for i = 0 to 255
$j = (j + S_i + Ki) \bmod 256$
swap S_i dan S_j

Salah satu kelemahan dari RC4 adalah terlalu tingginya kemungkinan terjadi tabel S-box yang sama, hal ini terjadi karena kunci user diulang-ulang untuk mengisi 256 bytes, sehingga 'aaaa' dan 'aaaaa' akan menghasilkan permutasi yang sama. Untuk mengatasi ini maka pada implementasinya nanti kita menggunakan hasil hash 160 bit SHA dari password kita untuk mencegah hal ini terjadi.

Kekurangan lainnya ialah karena enkripsi RC4 adalah XOR antara data bytes dan *pseudo-random byte stream* yang dihasilkan dari kunci, maka penyerang akan mungkin untuk menentukan beberapa byte pesan orisinal dengan meng-XOR dua *set cipher byte*, bila beberapa dari pesan input diketahui (atau mudah untuk ditebak).

Untuk mengatasinya pada aplikasinya initialization vector (IV) yang berbeda-beda lebh baik dignakan untuk setiap data, sehingga bahkan untuk file yang sama akan dihasilkan *ciphertext* yang berbeda. IV ini tidak perlu dirahasikan karena digunakan hanya agar setiap proses enkripsi akan menghasilkan *ciphertext* yang berbeda.

Untuk lebih meningkatkan keamanan dari metoda ini dapat juga mengembangkan inisialisasi kunci yang baru yang kita sebut saja inisialisasi SK (*strengtened key*), pada proses ini kunci user di-*expand* hingga 260 byte (tetapi kemudian hanya 256 byte saja yang digunakan) dengan menggunakan SHA-1, caranya pertama kunci user dijadikan kunci, kemudian 1-20 byte pertama pada buffer diproses dengan SHA kemudian digestnya diletakan pada 20 byte pertama, kemudian diambil byte 1-40 diproses dengan SHA dan hasilnya diletakan mulai pada byte 20, berikutnya byte 1-60 hasilnya diletakkan pada mulai byte 40, dan seterusnya. Kemudian buffer ini dienkrip dengan RC4, lalu buffer dijadikan kunci kembali, proses terakhir ini diulang sebanyak 16 kali untuk mencoba mencampur dengan baik sehingga dihasilkan kunci yang se-random mungkin.

5.2 Performansi

Kecepatan enkripsi dari RC4 cukup baik, hal ini terjadi karena proses enkripsinya yang cukup sederhana dan hanya melibatkan beberapa operasi saja per bytenya. Berdasarkan pada data hasil dari pengukuran yang telah dilakukan oleh **Budi Sukmawan** pada September 1998.

Untuk lebih jelasnya mari kita perhatikan hasil pembandingan pada beberapa platform hardware yang telah di lakukan. Kecepatan ini adalah kecepatan enkripsi di memori, karena dalam proses enkripsi file sesungguhnya melibatkan banyak faktor lain seperti interface IO, tipe Hardisk, dan lain-lain.

Hasil perbandingan ini dapat dilihat pada tabel, yang didapat dengan enkripsi 256 byte per blok sebanyak 20480 kali, atau setara dengan kurang lebih 5MB data.

Delphi 1.0 pada Windows for Workgroups 3.11

Prosesor	**Memori (MB)**	**Kecepatan (KBytes/dtk)**
486/DX4-100	16	557,067
Pentium 100	32	1.079,713
Pentium 166	16	1.792,717

Delphi 4.0 pada Windows 95, kecuali Pentium Pro pada Windows NT 4.0 Server

Prosesor	**Memori (MB)**	**Kecepatan (KBytes/dtk)**
486/DX4-100	16	2.563,846
Pentium 100	16	4.285,714
Pentium 133	32	5.380,035
Pentium 166MMX	32	7.191,522
Pentium 200MMX	32	8.668,172
Pentium Pro 200	64	10.651,872

Test dilakukan masing-masing sebanyak tiga kali kemudian hasilnya dirata-ratakan. Sebagai perbandingan kecepatan Blowfish adalah sekitar 2.300 KB/detik pada Pentium 133 (pada 8 byte per blok).

5.3 Keamanan

Bagaimana tingkat keamanan dengan kunci 160 bit ini. Bila kita anggap tidak ada kelemahan lain pada RC4 dan SHA maka untuk memecahkannya yang paling mungkin adalah dengan serangan "brute force", maka keamanan data tergantung sepenuhnya pada panjang kunci. Dengan 160 bits terdapat 2^{160} kunci yang mungkin. Bila kita anggap rata-rata diperlukan setengahnya untuk mendapat kunci yang benar (kurang lebih 10^{48}). Lalu kita buat beberapa asumsi tentang peralatan yang digunakan untuk memecahkan kunci tersebut :

1. Terdapat 1 milyar komputer yang digunakan.
2. Setiap komputer digunakan sepenuhnya untuk memecahkan kunci tersebut.
3. Setiap komputer dapat mencoba 1 milyar kunci per detik.

Dengan peralatan demikian maka dibutuhkan 10^{13} tahun untuk mendapatkan kunci tersebut. Ini sama dengan 1000 kali usia alam semesta.

6. Kesimpulan

Dari analisis mengenai aplikasi sistem kriptografi yang layak diterapkan pada basis data terintegrasi SIN ini, RC4 dapat digunakan sebagai salah satu cara untuk mengamankan SIN dari segi data yang dikandungnya, hal ini disebabkan oleh:

1. Kecepatan enkripsi dari RC4 cukup baik, hal ini terjadi karena proses enkripsinya yang cukup sederhana dan hanya melibatkan beberapa operasi saja per bytenya.
2. Kemananan RC4 sangat baik, karena untuk memecahkannya yang paling mungkin adalah dengan serangan "brute force".

Untuk dapat memecahkan RC4:

1. Terdapat 1 milyar komputer yang digunakan.
2. Setiap komputer digunakan sepenuhnya untuk memecahkan kunci tersebut.
3. Setiap komputer dapat mencoba 1 milyar kunci per detik.

Selain kemanan dari segi data, kemananan sosial juga harus diterapkan disini.

Yang dimaksud dengan keamanan sosial adalah keamanan dari segi manusianya. Sebagai contoh: jika pemilik data memiliki pin untuk mengakses datanya maka kewajiban dari pemilik data tersebut untuk menjaga kerahasiaan pin nya agar tidak diketahui orang lain.

7. Daftar Pustaka

(01) Suharno, “Menuju Terciptanya Single Identification Number di Indonesia”, Jakarta 2005

(02) Lusmiarwan, Driana, ”Perancangan Prototype Single Identity Number(SIN) Untuk Menunjang E-Goverment”, Bandung 2006

(03) Setiadi, Herald, ”Database Kependudukan Nasional Sebagai Prasyarat Untuk Pelaksanaan Good Governance”, Bandung 2006

(04) http://www.indonesia.go.id.
Akses 12 September 2006, pukul 16.00 WIB

http://www.sidoarjo.go.id/hukum/inpres/2003/th_2003_no_3.php.
Akses 13 September 2006, pukul 17.00 WIB

(06) http://www.bpkp.go.id/unit/hukum/kp/2004/072-04.pdf
Akses 13 September 2006, pukul 17.00 WIB

(07) http://www.ebizzasia.com/0214-2004/specialnote,0214,02.html.
Akses 13 September 2006, pukul 17.00 WIB

(08) http://www.depkominfo.go.id/index.php?action=view&pid=news&id=75.
Akses 13 September 2006, pukul 18.00 WIB

(09) http://www.detiknet.com/index.php/detik.read/tahun/2005/bulan/01/tgl/03/time/12111/idnews/266178/idkanal/88
Akses 13 September 2006, pukul 18.00 WIB

(10) Munir, Rinaldi, *Bahan Kuliah IF5054 Kriptografi*, Departemen Teknik Informatika.

(11) Ir. Fathansyah, *Basis Data*, Informatika, Bandung, 1999.

(12) T. Marcus, A. Prijono dan J.Widiadhi, *DELPHI DEVELOPER dan SQL Server 2000*, Informatika, Bandung, 2004.