Perancangan Sistem Keamanan Alternatif E-KTP Menggunakan Berbagai Algoritma Kriptografi

Muhammad Aulia Firmansyah - 13509039
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia
13509039@std.stei.itb.ac.id

***Abstrak* — E-KTP merupakan alat untuk melakukan identifikasi terhadap penduduk secara unik. E-KTP bertujuan agar bersifat unik dan aman. Untuk mencapai tujuan tersebut, E-KTP harus dirancang dengan sistem keamanan yang cukup kuat dan memiliki kinerja yang baik.**

Untuk hal tersebut, pada makalah ini, akan dicoba untuk dibangun suatu sistem keamanan sederhana yang dapat digunakan sebagai alternatif pada E-KTP. Sistem keamanan tersebut akan memanfaatkan data pada E-KTP. Algoritma kriptografi yang digunakan adalah AES, algoritma kunci publik, algoritma hashing, dan watermarking.

***Kata Kunci* — E-KTP, AES, kunci publik, hashing.**

I. PENDAHULUAN

E-KTP atau KTP Elektronik adalah suatu dokumen kependudukan yang dapat digunakan sebagai alat untuk mengidentifikasi seorang penduduk. E-KTP merupakan suatu proyek yang dicanangkan oleh pemerintah pada tahun 2011.

E-KTP ditargetkan merupakan perbaikan dari KTP konvensional yang memiliki beberapa kelemahan. Beberapa di antaranya ialah KTP konvensional memungkinkan sesorang dapat memiliki lebih dari sati KTP. Hal ini tentunya dapat berakibat fatal kepada pembangunan nasional, karena dengan KTP yang ganda, akan terjadi peluang untuk tindak kriminal, seperti menghindari pajak, memudahkan pembuatan paspor yang tidak dapat dibuat di seluruh kota, mengamankan korupsi, menyembunyikan identitas, dan sebagainya. E-KTP yang direncanakan pemerintah akan bersifat unik, yaitu satu orang hanya boleh memiliki satu KTP.

Selain itu, proyek E-KTP menargetkan terbentuknya KTP Elektronik yang dapat digunakan untuk berbagai keperluan, seperti pengurusan izin, pembukaan rekening bank, dan lainnya. Selain dari sisi penggunaan, E-KTP ditargetkan untuk bekerja dengan baik dari sisi keamanannya. E-KTP dirancang agar data pribadi yang tersimpan didalamnya aman dan tidak dapat dibobol oleh pihak – pihak yang tidak berkepentingan.

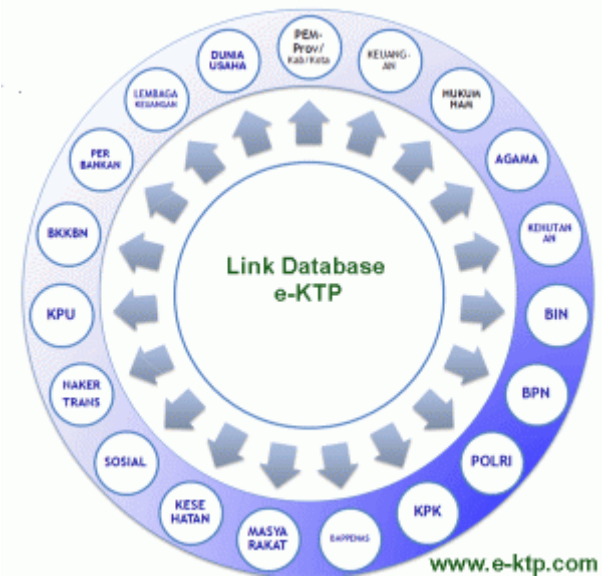
Untuk tujuan tersebut, dibutuhkan suatu sistem keamanan yang cukup aman, sehingga data yang tersimpan dalam KTP atau terhubung dengan KTP tidak jatuh ke pihak – pihak yang tidak diinginkan.

Sistem keamanan tersebut dapat dibangun dengan memanfaatkan beberapa algoritma kriptografi. Algoritma yang diterapkan pun bermacam – macam, sesuai fungsinya. Pada tulisan ini, akan dijelaskan beberapa algoritma yang dapat digunakan.

I. PRINSIP DASAR

A. E-KTP (KTP Elektronik)

E-KTP atau KTP Elektronik adalah suatu dokumen kependudukan yang dapat digunakan sebagai alat untuk mengidentifikasi seorang penduduk. E-KTP mengandung data pribadi penduduk yang berbasis pada Database Kependudukan Nasional. Data tersebut kemudian dapat digunakan untuk berbagai keperluan.



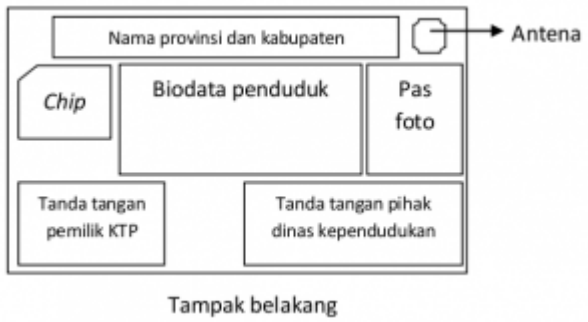
Gambar 1 – Penggunaan E-KTP

Informasi yang terdapat pada E-KTP ditanam pada suatu chip yang dimasukkan dalam kartu dan ditampilkan pada kartu. Informasi yang tersebut ialah,

1. NIK (Nomor Induk Kependudukan)
2. Nama lengkap
3. Tempat dan tanggal lahir
4. Jenis kelamin
5. Agama

6. Status perkawinan
7. Golongan darah
8. Alamat
9. Pekerjaan
10. Kewarganegaraan
11. Foto
12. Masa berlaku
13. Tempat dan tanggal dikeluarkannya Kartu Tanda Penduduk.
14. Tanda tangan pemegang Kartu Tanda Penduduk
15. Nama dan nomor induk pegawai pejabat yang menandatanganinya.

Gambar 2 – Tampilan fisik E-KTP



Gambar 3 – Struktur fisik E-KTP

Data tersebut diambil melalui proses pendaftaran E-KTP. Pada proses pendaftaran tersebut, selain mengambil data kependudukan, pendaftar juga diambil sidik jari dan sidik matanya. Data tersebut kemudian disimpan dalam kartu dan dalam Database Kependudukan Nasional.

B. Hashing

Hash adalah suatu fungsi matematis yang membentuk suatu data berdasarkan data yang dimasukkan. Pada aplikasinya, dari suatu data yang merupakan array of byte, akan dibentuk suatu array of byte yang memiliki panjang tertentu.

Yang membuat hashing menarik adalah dari data yang menjadi masukan, keluaran yang diberikan unik. Artinya apabila kita memasukkan data A, keluaran data tidak sama apabila kita memasukkan data B. Kelebihan ini sering dimanfaatkan untuk proses identifikasi data, mencocokkan suatu data dengan data yang lain, dan menjamin keaslian data tersebut.

Saat ini, cukup banyak metode hashing yang dapat dipakai. Salah satu yang paling terkenal ialah SHA. Metode hashing dapat mengubah data menjadi berbagai array of byte dengan panjang byte yang berbeda – beda.

C. AES (Advanced Encryption Standard)

Advanced Encryption Standard (AES) adalah sebuah algoritma kriptografi kunci simetris yang merupakan standar yang saat ini digunakan dalam enkripsi kunci simetris. Algoritma ini dapat melakukan enkripsi dan dekripsi data berukuran 128 bit dengan kunci yang berukuran 128, 192, atau 256 bit. Algoritma ini dikembangkan oleh dua kriptografer Belgia, yaitu Joan Daemen dan Vincent Rijmen dan dijadikan standar enkripsi oleh NIST.

D. Algoritma kunci publik

Disebut juga algoritma kriptografi kunci asimetris, algoritma ini menggunakan kunci yang berbeda untuk proses enkripsi dan dekripsinya. Pada aplikasinya, kunci untuk enkripsi biasanya disebar secara umum, tetapi kunci untuk dekripsi hanya diketahui oleh pemilik kuncinya saja.

Algoritma ini dianalogikan seperti kotak pos yang dapat dikirimi pesan oleh banyak orang. Akan tetapi, hanya pemilik kunci kotak pos tersebut yang dapat membacanya. Kelebihan dari algoritma ini ialah penggunaannya yang mudah untuk komunikasi ke banyak pihak secara aman. Hal ini dikarenakan jumlah kunci yang digunakan tidak sebanyak kunci yang digunakan pada algoritma kunci simetris.

E. Watermarking

Watermarking adalah suatu teknik penyembunyian data ke dalam suatu data digital. Watermarking biasa digunakan untuk menyisipkan suatu informasi tertentu baik itu yang bersifat umum ataupun rahasia ke dalam media digital seperti gambar, suara, ataupun media lainnya.

Pada aplikasinya, watermarking dapat digunakan untuk berbagai macam keperluan, seperti,

1. Tamper-proofing, yaitu menjadi indikator apakah data digital telah mengalami perubahan atau tidak.
2. Feature location, yaitu mengidentifikasikan isi dari data digital tersebut
3. Annotation/Caption, yaitu sebagai keterangan tentang data digital itu sendiri
4. Copyright-Labeling, yaitu untuk menyimpan data label hak cipta sebagai bukti otentik kepemilikan data digital tersebut.

III. RANCANGAN SISTEM

A. Sidik Jari Sebagai Kunci

Sidik jari adalah suatu bekas yang dihasilkan dari jari manusia, baik itu jari tangan ataupun jari kaki. Bekas tersebut terbentuk dari perbedaan kedalaman kulit pada

jari di mana perbedaan tersebut membentuk suatu struktur biometrik tertentu.

Sidik jari memiliki sifat unik untuk setiap orang. Artinya setiap orang memiliki sidik jari yang tidak persis sama dengan orang lain, kecuali pada beberapa kasus seperti penyakit tanpa sidik jari, sidik jari terbakar, atau sebagainya. Hal ini dimanfaatkan dalam melakukan identifikasi. Sidik jari merupakan salah satu alat untuk identifikasi manusia yang paling sederhana dan mudah digunakan.

Gambar 4 – Contoh sampel sidik jari

karena sifatnya yang unik, sidik jari dapat digunakan sebagai kunci dalam melakukan enkripsi dan dekripsi. Dengan menggunakan sidik jari sebagai kunci, hanya orang yang memiliki sidik jari tersebut yang dapat melakukan enkripsi dan dekripsi. Selain itu, tidak seperti kunci yang berupa string, sidik jari sangat sulit untuk dipalsukan. Teknologi identifikasi sidik jari saat ini pun telah dilengkapi dengan pendeteksi sidik jari palsu atau sidik jari buatan.

Akan tetapi, identifikasi dengan sidik jari seringkali menimbulkan masalah, yaitu akurasi dari identifikasi tersebut yang kemungkinan tidak akan menghasilkan hasil yang seratus persen tepat. Akan ada galat yang terjadi pada identifikasi tersebut. hal ini dapat menjadi masalah, karena kunci yang digunakan untuk enkripsi dan dekripsi dapat menimbulkan hasil yang salah apabila kunci tersebut berbeda walaupun hanya sebagian kecilnya saja.

solusi dari permasalahan ini adalah dengan menggunakan hanya satu sidik jari yang digunakan untuk melakukan enkripsi dan dekripsi. Sidik jari yang dimaksud ialah ketika melakukan pendaftaran E-KTP. Apabila hanya sidik jari tersebut yang digunakan untuk menjadi kunci, kunci yang dipakai tidak akan berubah, sehingga hasilnya akan tepat. Untuk pengambilan sidik jari selanjutnya, tidak akan dijadikan kunci dalam enkripsi dan dekripsi, tetapi tetap digunakan sebagai validasi E-KTP. Hal ini dilakukan dengan membandingkan sidik jari validasi dengan sidik jari pendaftaran. Apabila cocok (dengan galat tertentu), orang yang diambil sidik jarinya akan mendapatkan akses ke kunci yang dibuat berdasarkan sidik jari pendaftaran.

Dengan cara ini, E-KTP seolah – olah dapat diverifikasi penggunanya setiap pengambilan sidik jari dan hasilnya bisa lebih akurat.

B. Hashing untuk NIK

Nomor Induk Kependudukan atau disingkat dengan NIK adalah suatu nomor yang digunakan untuk mengidentifikasi seorang penduduk Indonesia. Hal ini mengakibatkan setiap NIK seorang penduduk tidak boleh sama dengan penduduk lainnya. Dengan demikian, NIK harus dirancang unik.

Pemerintah telah menetapkan NIK merupakan string sepanjang 16 karakter yang terdiri dari karakter berupa angka (0-9). Karakter penyusun NIK terdiri dari 2 digit awal yang merupakan kode provinsi, 2 digit kota kabupaten, 2 digit kode kecamatan, 6 digit tanggal lahit dalam format hhbbtt (untuk wanita, tanggal ditambah 40), dan 4 digit yang merupakan nomor urut. Misalkan, seorang perempuan yang lahir 17 Agustus 1990 akan mendapat NIK adalah 10 50 24 570890 0001.

NIK yang berbentuk dengan bentuk tersebut sudah memenuhi aspek keunikan karena dapat membedakan semua penduduk Indonesia. Akan tetapi, muncul masalah ketika orang tidak ingin data pribadinya diketahui orang lain hanya dengan melihat NIK-nya saja. Pasalnya, pada NIK, dicantumkan secara tidak langsung tanggal lahirnya. Bagi sebagian pihak yang menganggap tanggal lahir tidak boleh diketahui umum, NIK tidak cocok untuk dia. Selain itu, pada NIK, tersimpan informasi – informasi terseirat yang sebenarnya tergolong cukup sensitif.

Untuk mengatasi masalah tersebut, diperlukan suatu NIK yang tidak menampilkan informasi tersirat tersebut namun tetap mempertahankan keunikan nomor tersebut. oleh karena itu, digunakanlah metode hashing.

Seperti yang telah dijelaskan pada bagian sebelumnya, hasing dapat membentuk suatu data unik dari suatu data tertentu. Dalam hal Nomor Induk Kependudukan, NIK dapat di-hash hingga menghasilkan suatu array of byte yang kemudian dapat dikonversi menjadi string angka yang bersifat unik. String angka tersebut dapat dikonversikan menjadi NIK yang baru, menggantikan NIK yang lama. Kelebihan metode hashing ialah, metode ini dapat menghasilkan string angka dengan panjang yang berbeda – beda, sesuai dengan kebutuhan, sehingga panjang NIK dapat disesuaikan dengan kebijakan pemerintah ataupun standar yang telah ditetapkan secara internasional. Dengan demikian, NIK dapat digunakan sebagai nomor pengenal yang sesuai untuk dokumen yang membutuhkan pengenal berupa string angka dengan panjang tertentu, seperti paspor dan sebagainya.

C. Watermarking pada Pas Foto

Dalam penggunaan E-KTP dalam berbagai keperluan, bisa saja foto penduduk akan dipakai untuk keperluan tertentu, seperti pembuatan SIM (Surat Izin Mengemudi), paspor, dan sebagainya. Hal ini membuat foto yang digunakan harus otentik, sesuai dengan foto yang ada pada E-KTP.

Kadangkala, ada pihak yang berusaha memalsukan data – data tersebut. salah satunya dengan memalsukan foto.

Tanpa penanganan khusus, ada kemungkinan foto yang dipalsukan tersebut lolos dari verifikasi sistem.

Oleh karena itu, dilakukan pengamanan tambahan pada foto tersebut menggunakan watermarking. Watermarking tersebut dilakukan dengan tujuan tamper-proofing, yaitu menjadi indikator keaslian foto sekaligus mengecek apakah pas foto yang digunakan telah mengalami perubahan atau tidak.

Watermarking dilakukan dengan menyisipkan informasi untuk mengidentifikasikan keaslian foto. Sala satu pilihan yang dapat digunakan ialah dengan menyisipkan gambar tanda tangan ke foto tersebut menggunakan sidik jari sebagai kuncinya. Jika tidak menggunakan sidik jari, bisa juga menggunakan NIK sebagai kunci. Dengan demikian, apabila foto yang diperiksa tidak menghasilkan tanda tangan yang benar, foto tersebut patut dicurigai palsu atau sudah diubah.

D. Fitur Keamanan dengan AES dan algoritma kunci publik

E-KTP direncanakan akan menjadi kartu serba guna yang dapat digunakan untuk berbagai keperluan. Semakin banyak dan penting keperluan tersebut, semakinpenting juga mempertimbangkan aspek keamanan E-KTP. Penggunaan E-KTP untuk transaksi perbankan akan membutuhkan tingkat keamanan yang tinggi karena menyangkut data yang penting, yaitu data keuangan.

Dengan demikian, E-KTP akan lebih baik jika dilengkapi dengan fitur keamanan. Misalkan, agar E-KTP dapat digunakan dalam transaksi perbankan, E-KTP dilengkapi dengan data nasabah. Tentunya data ini merupakan data yang sangat sensitif dan apabila jatuh ke tangan pihak yang ridak bertanggung jawab, dapat berakibat penyalahgunaan data tersebut. oleh karena itu, data personal yang disimpan ke dalam E-KTP sebaiknya dienkripsi. Enkripsi dapat dilakukan menggunakan algoritma AES menggunakan sidik jari sebagai kuncinya.

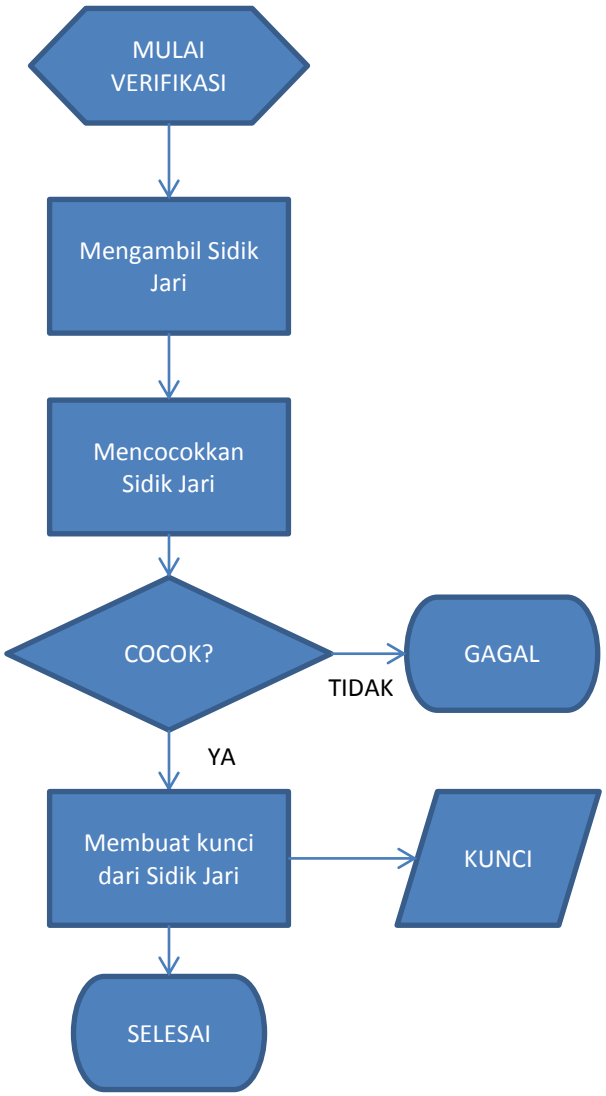
Selain itu, dengan menggunakan kunci tersebut, dapat dibuat kunci publik dan kunci privat untuk transaksi – transaksi perbankan. Pihak bank merupakan pihak yang memiliki kunci publik, sedangkan pihak nasabah merupakan pihak yang memiliki kunci privat.

E. Gambaran Sistem

Dengan menggunakan algoritma yang telah dijelaskan sebelumnya, dapat dibentuk suatu sistem keamanan sederhana yang memungkinkan penggunaan yang aman. Sistem keamanan tersebut dirancang sebagai berikut.

Pertama, pada tahap verifikasi, dilakukan pengambilan sidik jari. Data sidik jari yang telah diambil kemudian dibandingkan dengan data sidik jari yang ada pada E-KTP. Apabila tidak cocok, pemegang E-KTP dianggap bukan merupakan pemilik E-KTP dan perlu ditangani lebih lanjut. Apabila cocok, artinya pemegang E-KTP adalah pemilik asli kartu tersebut. Setelah itu, pemegang berhak untuk menggunakan E-KTP di tempat tersebut sesuai keperluannya.

Berikut adalah skema tahap verifikasi yang terjadi.



Gambar 5 – Skema tahap verifikasi

Tahap selanjutnya seperti penggunaan E-KTP untuk keperluan tertentu dijelaskan di skenario penggunaan sistem.

IV. SKENARIO PENGGUNAAN SISTEM

Setelah sistem keamanan sederhana berhasil dibuat, dilakukan simulasi penggunaan E-KTP untuk melakukan beberapa keperluan kependudukan. Beberapa skenario yang akan dilakukan ialah pembuatan nomor paspor, dan melakukan transaksi di ATM menggunakan E-KTP.

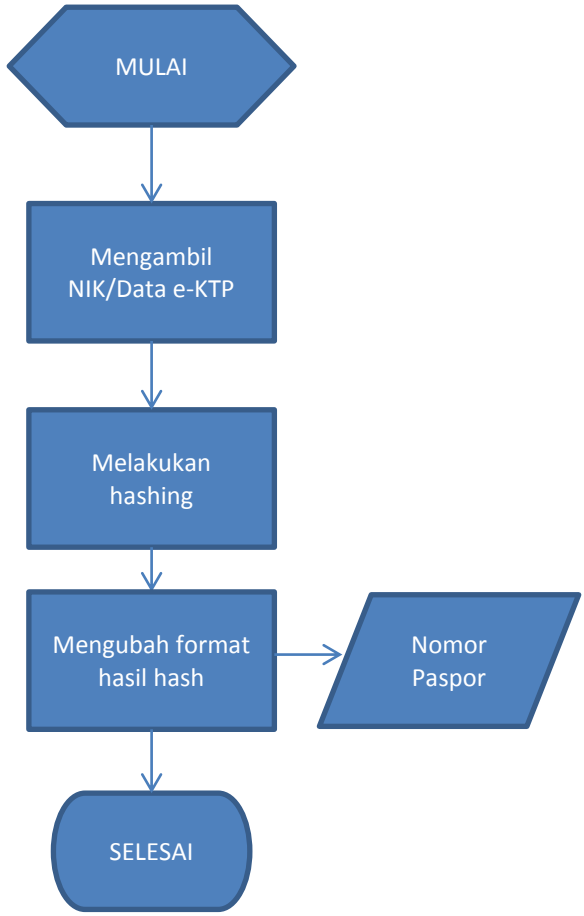
A. Kasus Pembuatan Nomor Paspor

Proses pembuatan paspor merupakan proses yang mirip dengan proses pembuatan E-KTP. Dengan memanfaatkan penggunaan hashing pada NIK, dapat dibuat paspor yang unik dengan panjang nomor paspor yang sesuai.

Ada dua alternatif yang dapat dilakukan dalam pembuatan nomor paspor. Alternatif pertama ialah menggunakan hashing pada NIK. Sedangkan alternatif kedua ialah menggunakan hashing pada data yang ada

pada E-KTP, seperti nama lengkap, tanggal lahir, dan informasi lainnya yang tidak terdapat pada NIK.

Berikut adalah skema penggunaan hashing pada pembuatan nomor paspor.



Gambar 6 – Skema pembuatan nomor paspor dengan hashing

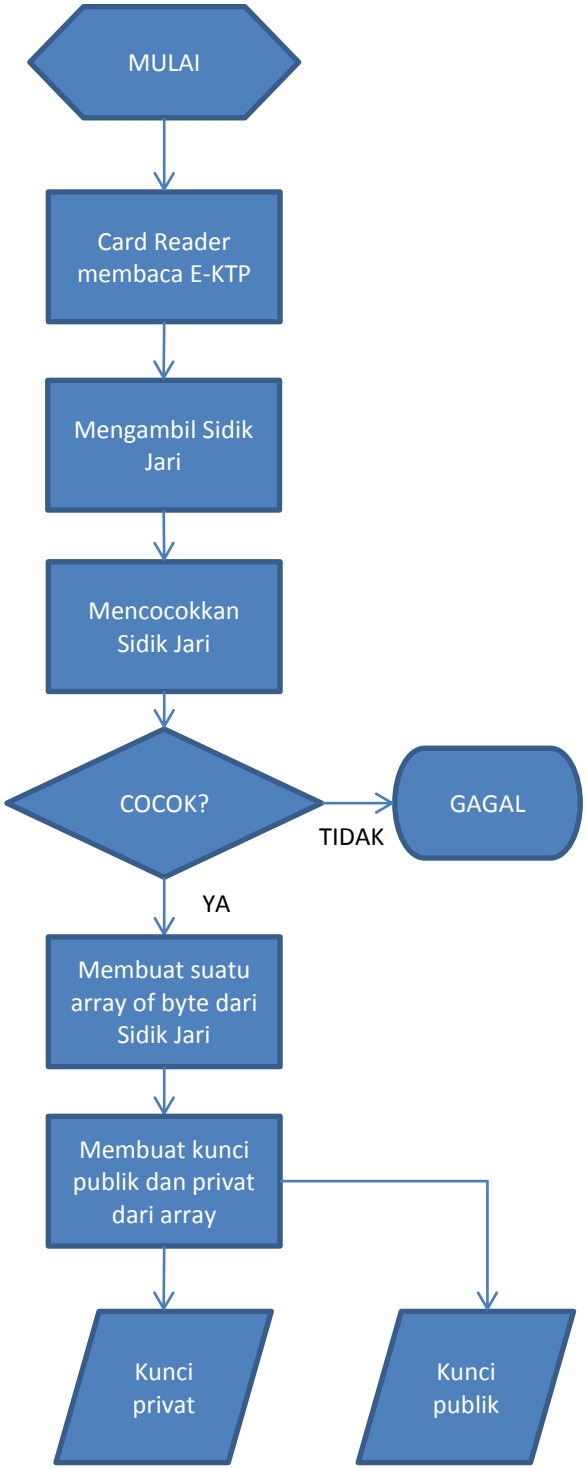
B. Kasus Transaksi dengan ATM Bank

Transaksi dengan E-KTP dapat dilakukan dengan menggunakan verifikasi yang sama, yaitu menggunakan sidik jari sebagai kunci. Dengan demikian, transaksi akan lebih aman karena tidak harus menghafal nomor PIN yang cukup rawan dibajak oleh pihak – pihak yang tidak bertanggung jawab.

Tahap – tahap yang terjadi pada transaksi dengan ATM bank adalah sebagai berikut,

1. Menghubungkan E-KTP dengan Card Reader dengan cara menggesekkan kartu pada slot yang tersedia.
2. Melakukan verifikasi dengan sidik jari. Apabila cocok, maju ke langkah selanjutnya. Sedangkan, apabila tidak cocok, harus mengulangi dari langkah pertama.
3. Card reader akan menghasilkan suatu pasangan kunci publik dan privat. Kunci tersebut dapat digunakan untuk sesi penggunaan ATM tersebut. Kunci publik diberikan kepada pihak server ATM, sedangkan kunci privat diberikan kepada pemegang E-KTP.
4. Transaksi dapat dilakukan menggunakan kunci publik dan kunci privat selama sesi tersebut. jika sudah selesai, sesi dimatikan dan keadaan ATM kembali seperti semula.

Berikut adalah skema penggunaan E-KTP pada transaksi di ATM.



Gambar 7 – Skema penggunaan E-KTP untuk transaksi di ATM

V. KESIMPULAN

E-KTP adalah suatu tanda pengenal bagi penduduk yang merupakan perbaikan dari KTP yang lama, yaitu dengan adanya kemampuan untuk menyimpan informasi kependudukan dalam bentuk data. Hal ini dapat menciptakan pengolahan data pada E-KTP melalui komputer. Salah satu pengolahan tersebut ialah dari segi keamanan dari E-KTP tersebut.

Dalam perancangan suatu sistem keamanan, yang harus diperhatikan tidak hanya kekuatan algoritmanya saja, tetapi juga bagaimana algoritma tersebut dapat digunakan secara efektif dan efisien.

REFERENSI

[1] http://www.e-ktp.com/2011/06/fungsi-dan-kegunaan-e-ktp,"*e-KTP , KTP Elektronik Indonesia » Fungsi dan Kegunaan E-KTP*".

[2] http://www.e-ktp.com/2011/06/hello-world,"e-KTP , KTP Elektronik Indonesia » Apa dan Mengapa e-KTP".

[3] http://www.e-ktp.com/2011/04/bentuk-gambar-foto-e-ktp,"e-KTP , KTP Elektronik Indonesia » Seperti Apa Bentuk e-KTP?"

[4] http://id.wikipedia.org/wiki/Kriptografi,"Kriptografi - Wikipedia bahasa Indonesia, ensiklopedia bebas".

PERNYATAAN

Dengan ini saya menyatakan bahwa makalah yang saya tulis ini adalah tulisan saya sendiri, bukan saduran, atau terjemahan dari makalah orang lain, dan bukan plagiasi.

Bandung, 14 Mei 2012

Muhammad Aulia Firmansyah
13509039