Penerapan Kriptografi Untuk Meningkatkan Keamanan Data Pribadi pada IKD (Identitas Kependudukan Digital)

Mochammad Fatchur Rochman - 13519009
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jalan Ganesha 10 Bandung
13519009@std.stei.itb.ac.id

***Abstrak*—Makalah ini menjelaskan mengenai penerapan algoritma kriptografi untuk meningkatkan keamanan data pribadi pada IKD (Identitas Kependudukan Digital) atau yang lebih tepatnya mengamankan data pribadi yang ada pada aplikasi IKD. Algoritma kriptografi yang dimaksudkan adalah enkripsi data pribadi menggunakan algoritma kriptografi simetris (AES) dan kriptografi kunci publik (RSA, ECC).**

Keywords—AES; ECC; IKD; RSA

I. Pendahuluan

Perkembangan teknologi yang pesat membawa banyak perubahan di berbagai sektor dalam kehidupan manusia yang sekarang menjadi serba digital, salah satunya adalah sektor administrasi kependudukan yaitu evolusi e-KTP (Kartu Tanda Penduduk Elektronik) menjadi KTP Digital yang dapat diakses melalui ponsel pintar/*smartphone* melalui aplikasi IKD (Identitas Kependudukan Digital). Perkembangan ini menghadirkan kemudahan dan kenyamanan baru bagi masyarakat dalam mengakses dan menggunakan identitas mereka.

IKD (Identitas Kependudukan Digital) adalah informasi elektronik yang digunakan untuk merepresentasikan dokumen kependudukan dan data balikan dalam aplikasi digital melalui gawai yang menampilkan data pribadi sebagai identitas yang bersangkutan [1]. Data yang disimpan dalam aplikasi meliputi:

- dokumen pribadi seperti KTP Digital
- data dan dokumen anggota keluarga seperti KK (Kartu Keluarga Digital)
- dokumen lainnya seperti Sertifikat Vaksin Covid-19, NPWP (Nomer Pokok Wajib Pajak), Kepemilikan Kendaraan BKN (Badan Kepegawaian Negara).

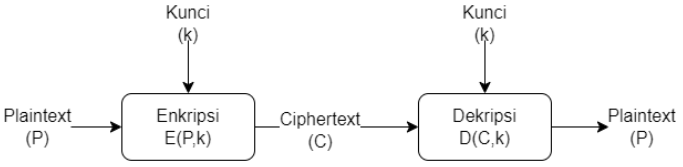
Selain itu ada juga fitur QR Code Identitas Digital, biodata dan histori aktivitas. Dengan begitu banyaknya data-data penting yang tersimpan pada aplikasi IKD diperlukan pengamanan yang kuat untuk melindungi data-data tersebut. Untuk itu aplikasi IKD telah dilengkapi pin ketika ingin mengakses aplikasi, kemudian ada juga fitur anti *screenshoot* sehingga tidak dimungkinkan untuk melakukan tangkapan layar pada data-data yang ada pada aplikasi.

Pengamanan data pada aplikasi tersebut sudah cukup baik, namun data-data yang disimpan tersebut tidak dilakukan enkripsi, sehingga informasi pribadi seperti biodata akan mudah diketahui ketika aplikasi sedang aktif dan dilakukan pemotretan data dengan ponsel pintar lainnya dan kemungkinan terburuknya adalah jika penyerang berhasil mendapatkan data-data tersebut dari sisi server, jika data-data tersebut tidak dienkripsi maka data-data tersebut akan dengan didapatkan oleh penyerang. Pada makalah ini akan membahas mengenai peningkatan keamanan data dengan melakukan enkripsi data-data pribadi (informasi dan file/gambar) yang ada pada aplikasi IKD menggunakan algoritma kriptografi.

II. Dasar Teori

A. Kriptografi Kunci Simetris

Kriptografi kunci simetri adalah sebuah metode kriptografi yang menggunakan kunci yang sama untuk melakukan enkripsi dan dekripsi. Pesan yang akan dikirim diubah menjadi ciphertext menggunakan suatu kunci, yang kemudian penerima pesan akan mengembalikan ciphertext ke bentuk pesan semula yang dapat dibaca dengan menggunakan kunci yang sama. Salah satu algoritma kriptografi kunci simetri yang terkenal adalah AES (*Advanced Encryption Standard*).



Gambar 1. Kriptografi Kunci Simetris

B. AES

AES (*Advanced Encryption Standard*) adalah sebuah algoritma kriptografi kunci simetri yang berbasis *cipher* blok. Algoritma ini menggunakan panjang blok tetap yaitu 128 bit, dengan panjang kunci yang bervariasi yaitu 128 bit, 192 bit, dan 256 bit. Algoritmanya adalah sebagai berikut (diluar proses pembangkitan *round key*) [2]:

1) AddRoundKey: melakukan initial round yaitu melakukan XOR antara state awal (plainteks) dengan cipher key.
2) Putaran sebanyak Nr-1 kali, setiap putaran melakukan proses:
   a) SubBytes

      melakukan substitusi byte dengan menggunakan tabel substitusi (S-Box).

   b) ShiftRows

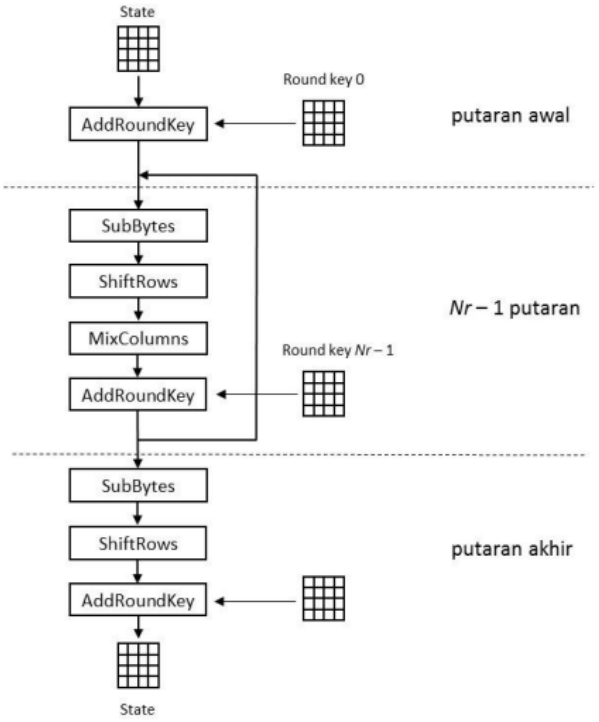
      melakukan pergeseran baris-baris array state secara wrapping.

   c) MixColumns

      melakukan pengacakan data di masing-masing kolom array state.

   d) AddRoundKey

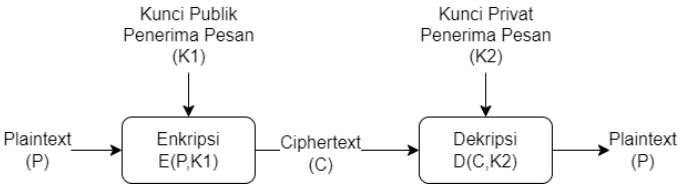
      melakukan XOR antara state sekarang dengan round key.
3) Final round, pada putaran terakhir melakukan proses:
   a) SubBytes
   b) ShiftRows
   c) AddRoundKey



Gambar 2. AES, algoritma Rijndael [2]

C. Kriptografi Kunci Publik

Kriptografi kunci publik (kriptografi kunci asimetris) adalah suatu metode kriptografi yang menggunakan sepasang kunci yang berbeda untuk melakukan enkripsi dan dekripsi, pasangan kunci tersebut terdiri dari kunci publik dan kunci privat. Pesan yang akan dikirim akan dienkripsi menggunakan kunci publik dari penerima pesan, yang kemudian penerima pesan akan mengembalikan ciphertext ke bentuk pesan semula yang dapat dibaca dengan menggunakan kunci privat miliknya. Algoritma kriptografi kunci publik diantaranya adalah RSA, ECC, ElGamal, dan Diffie-Hellman.



Gambar 3. Kriptografi Kunci Publik

D. Algoritma RSA

RSA (Riverst-Shamir-Adleman) merupakan algoritma kriptografi kunci publik yang paling populer dan banyak aplikasinya, letak keamanan algoritma RSA terletak pada sulitnya memfaktorkan bilangan bulat yang besar menjadi faktor-faktor prima. Langkah-langkah untuk menghasilkan pasangan kunci RSA adalah sebagai beriku [4]:

- Pilih dua bilangan prima besar secara acak, misalnya p dan q (bilangan ini bersifat rahasia)
- Hitung nilai $n = p * q$, dimana n adalah modulus.
- Hitung $\phi(n) = (p-1) * (q-1)$ (bilangan ini bersifat rahasia)
- Pilih sebuah bilangan bulat e, dimana $1 < e < \phi(n)$dan e saling prima dengan $\phi(n)$. e akan menjadi kunci publik.
- Hitung nilai d, dimana $e * d \equiv 1(mod\ \phi(n))$. d akan menjadi kunci privat.

Untuk mengenkripsi pesan m dilakukan dengan rumus $c = E(m,e) = m^e\ mod\ n$ dan akan dihasilkan ciphertext c untuk setiap m yang dienkripsi.

Untuk melakukan dekripsi suatu ciphertext c dapat dilakukan dengan rumus dekripsi $m = D(c,d) = c^d\ mod\ n$ dan akan dihasilkan pesan m untuk setiap ciphertext c yang dienkripsi.

E. Kriptografi ECC

ECC (*Elliptic Curve Cryptography*) merupakan algoritma kriptografi kunci publik yang memanfaatkan kesulitan dalam menyelesaikan masalah matematika yang dikenal sebagai "logaritma diskret kurva eliptik" untuk menjaga keamanannya, masalah tersebut melibatkan operasi perkalian titik pada kurva eliptik dan mencari kelipatan dari suatu titik pada kurva tersebut. Persamaannya sebagai berikut [5]:

$$Q = kP = P^k$$

dengan Q adalah titik pada kurva eliptik dan akan menjadi kunci publik, k merepresentasikan kelipatan dari suatu titik pada kurva dan akan menjadi kunci privat, dan P adalah sebarang titik pada kurva eliptik yang dijadikan *base point*.

III. Analisa Permasalahan dan Pembahasan

Data pribadi yang akan kita enkripsi adalah data yang tersimpan dalam sebuah aplikasi IKD yang merupakan ponsel pintar/*smartphone*, yang mana selain kekuatan keamanan yang

jadi faktor yang diperhitungkan namun kinerja, efisiensi, dan penggunaan sumber daya yang diperlukan saat algoritma tersebut digunakan pada ponsel pintar/*smartphone*, faktor-faktor tersebut juga menjadi faktor yang penting untuk diperhitungkan sebagai parameter pemilihan suatu algoritma.

Dalam hal keamanan untuk mengenkripsi data pribadi (informasi dan file) yang ada pada aplikasi IKD diantara AES, RSA, dan ECC semuanya adalah algoritma enkripsi yang aman jika digunakan dengan benar. Tingkat keamanan yang diinginkan tergantung pada tingkat sensitivitas data dan ancaman yang mungkin ada. Secara umum, AES dianggap sebagai algoritma kriptografi kunci simetris yang sangat aman, sedangkan RSA dan ECC adalah algoritma kunci asimetris / kunci publik yang juga memiliki tingkat keamanan yang baik, yang artinya dalam hal kemananan keduanya sama baiknya.

Dalam hal kecepatan AES lebih cepat daripada RSA dan ECC dalam proses enkripsi dan dekripsi. Hal ini dikarenakan AES dirancang dengan operasi matematika yang efisien yaitu pergantian bit (subtitusi), pergeseran bit (shift), dan operasi XOR sederhana. Sedangkan ECC dan RSA melibatkan operasi matematika yang lebih kompleks seperti operasi pada kurva eliptik dan operasi perkalian modular yang membutuhkan waktu yang lebih lama dibandingkan operasi matematika yang digunakan AES.

Dalam hal kinerja, AES memiliki kecepatan enkripsi dan dekripsi yang baik, membuatnya lebih efisien dalam mengenkripsi dan mendekripsi data pribadi (informasi pribadi dan file) pada aplikasi *smart phone*. AES telah dioptimalkan dengan baik dan dapat diterapkan pada perangkat keras dan perangkat lunak secara efisien serta mendukung penggunaan cepat dan responsif dengan sumber daya terbatas. Sedangkan ECC memiliki keunggulan dalam efisiensi ruang kunci, keunggulan ini cenderung lebih relevan dalam skenario dengan keterbatan sumber daya sepert perangkat kecil yang menyimpan daya yang terbatas, misalnya: IoT. Dalam konteks aplikasi *smartphone*m ruang penyimpanan dan daya yang tersedia cenderung cukup mengakomodasi penggunaan AES secara efektif. Sedangkan RSA masih kalah dengan ECC karena dengan panjang kunci yang lebih pendek ECC dapat memberikan kualitas enkripsi data dengan tingkat keamanan yang sama.

Dari analisa yang telah dipaparkan dari segi keamanan, kecepatan, kinerja, efisiensi, dan penggunaan sumber daya diambil kesimpulan AES adalah algoritma kriptografi yang paling cocok untuk enkripsi file pada aplikasi smartphone. Implementasi AES dalam mengamankan data pribadi dapat dilakukan dengan melakukan enkripsi data pribadi (informasi pribadi maupun file) pada sisi server maupun lokal dan melakukan *hashing* juga pada kunci/*secret key* tersebut ketika disimpan pada sisi server. Berikut adalah hasil enkripsi informasi pribadi seperti NIK dan file gambar KTP Digital dengan algoritma AES dengan kunci supersecretkey07, ketika NIK dan file gambar KTP dienkripsi maka NIK tersebut tidak akan terbaca dan begitupun file gambar KTP akan tidak dapat dibuka.

NIK	NIK Terenkripsi
3326160101810021	{‰N8UÚeÝº¼"½Þhä

Tabel 1. Enkripsi NIK dengan AES

KTP	
	, «à(o—¯.¡ˆ]>T÷Äù„¬äJŠg: nØ0ëx~dÙ

Tabel 2. Enkripsi file gambar KTP dengan AES

IV. KESIMPULAN

AES adalah alg`oritma kriptografi yang paling cocok untuk enkripsi file pada aplikasi smartphone dikarenakan kehandalannya dalam segi keamanan, kecepatan, efisiensi dan penggunaan sumber daya yang dapat diakomodasi oleh *smartphone*. Implementasi AES dalam mengamankan data pribadi dapat dilakukan dengan melakukan enkripsi data pribadi (informasi pribadi maupun file) pada sisi server maupun lokal dan melakukan *hashing* juga pada kunci/*secret key* tersebut ketika disimpan pada sisi server.

UCAPAN TERIMA KASIH

Puji syukur penulis panjatkan pada hadirat Tuhan Yang Maha Esa. Atas rahmat dan kemudahan yang diberikan kepada penulis, sehingga makalah yang berjudul "Penerapan Kriptografi Untuk Meningkatkan Keamanan Data Pribadi pada IKD (Identitas Kependudukan Digital)" dapat diselesaikan. Penulis ingin menyampaikan rasa syukur dan terima kasih kepada Bapak Dr. Ir. Rinaldi Munir, M.T., selaku Dosen Mata Kuliah IF4020 Kriptografi yang telah memberikan banyak masukan, referensi, dan dukungan

REFERENCES

[1] "Apa itu IKD dan Bagaimana Proses Aktivasinya". Disdukcapil Kota Pekanbaru. disdukcapil.pekanbaru.go.id/post/172-apa-itu-ikd-dan-bagaimana-proses-aktivasinya.

[2] Munir, Rinaldi. 2023. Slide Kuliah IF4020 Kriptografi:Review Beberapa Block Cipher (Bagian 3: Advanced Encryption Standard (AES)). Di akses Mei 22, 2023, melalui *https://informatika.stei.itb.ac.id/*.

[3] Munir, Rinaldi. 2023. Slide Kuliah IF4020 Kriptografi: Kriptografi Kunci-Publik. Di akses melalui *https://informatika.stei.itb.ac.id/*.

[4] Munir, Rinaldi. 2023. Slide Kuliah IF4020 Kriptografi: Algoritma RSA. Di akses melalui *https://informatika.stei.itb.ac.id/*.

[5] Munir, Rinaldi. 2023. Slide Kuliah IF4020 Kriptografi: Algoritma ECC. Di akses melalui *https://informatika.stei.itb.ac.id/*.