BAB II

LANDASAN TEORI

2.1 Android

Menurut Safaat, "*Android* adalah sistem operasi berbasis *Linux* bagi telepon seluler seperti telepon pintar dan komputer tablet. *Android* juga menyediakan platform terbuka bagi para pengembang untuk menciptakan aplikasi mereka sendiri yang akan digunakan untuk berbagai macam piranti gerak. Sistem operasi ini diakusisi oleh *Google* dan terus dilakukan pengembangan" (Safaat, 2012). Beberapa fitur ungggulan yang terdapat dalam sistem operasi *Android* (Speckmann, 2008) adalah :

- Kerangka aplikasi yang memungkinkan penggunaan dan penghapusan komponen yang tersedia.
- *Dalvik* mesin virtual, mesin virtual yang dioptimalkan untuk perangkat telepon seluler.
- Grafik 2D dan 3D berdasarkan pustaka OpenGL.
- *SQLite* untuk penyimpanan data.
- Mendukung media seperti audio, video, dan berbagai format gambar.

2.2 Wi-Fi Direct

Wi-Fi Direct adalah teknologi yang memungkinkan perangkat *Wi-Fi* untuk terhubung secara langsung, sehingga dapat melakukan berbagai kegiatan seperti mencetak, berbagi data, dan sinkronisasi. Perangkat yang telah memiliki teknologi *Wi-Fi Direct* dapat terhubung dengan satu sama lain tanpa perlu bergabung dengan jaringan rumah, kantor, maupun *hotspot* konvensional. Ponsel pintar,

kamera, printer, komputer, dan peralatan bermain dapat terhubung secara langsung untuk mengirim konten dan berbagi aplikasi dengan mudah dan cepat. Perangkat dapat membuat hubungan *one-to-one connection* atau membuat gabungan dari beberapa perangkat dapat terhubung secara simultan. Dengan *Wi-Fi Direct* tidak diperlukan *access point* ataupun koneksi internet, sehingga perangkat *Wi-Fi* tidak hanya digunakan untuk mengakses internet tetapi dapat menghubungkan semua perangkat *Wi-Fi* untuk dapat berbagi konten. *Wi-Fi Direct* dapat dilakukan dimana saja dan kapan saja. Perangkat *Wi-Fi Direct* akan memancarkan sinyal ke perangkat lain pada jangkauan tertentu dan membiarkan perangkat lain mengetahui keberadaan perangkat tersebut untuk kemudian dapat terhubung. Pengguna dapat melihat daftar perangkat yang tersedia disekitarnya dan dapat menerima undangan untuk dapat terhubung ke perangkat lain. Penggunaan Wi-Fi Direct ini dapat diaplikasikan secara luas di berbagai *multi platform* seperti *Android, iOS, Blackberry, Windows,* bahkan hingga perangkat permainan seperti *Xbox* yang sudah mendukung *Wi-Fi Direct* (Wi-Fi Alliance, 2014).

2.3 Kriptografi

Kriptografi merupakan ilmu mengenai teknik enkripsi dimana data diacak menggunakan suatu kunci enkripsi menjadi sesuatu yang sulit dibaca oleh seseorang yang tidak memiliki kunci dekripsi. Untuk dapat membaca data tersebut, harus dilakukan dekripsi. Dekripsi dilakukan menggunakan kunci dekripsi untuk mendapatkan kembali data asli. Proses enkripsi dan dekripsi dilakukan menggunakan suatu algoritma dengan beberapa parameter. Pada umumnya terdapat dua teknik kriptografi (Kromodimoeljo, 2009) :

1. Kriptografi algoritma simetri

Algoritma ini mengharuskan pengirim dan penerima menyetujui satu kunci tertentu sebelum dapat berkomunikasi secara aman. Keamanan algoritma simetri tergantung pada rahasia kunci. Pemecahan kunci berarti memungkinkan setiap orang dapat mengenkripsi dan mendekripsi pesan dengan mudah. Kelebihan algoritma simetri ini adalah kecepatan prosess-nya sehingga memungkinkan untuk digunakan secara real-time. Kelemahan algoritma ini adalah pendistribusian kunci secara aman dan jumlah kunci. Beberapa algoritma yang menggunakan algoritma simetri ini adalah Data *Encryption Standard* (DES), *One Time Password* (OTP), *Advanced Encryption Standard* (AES), *International Data Encryption Algorithm* (IDEA), *Blowfish*, dan *Cash.*

2. Kriptografi algoritma asimetri

Algoritma asimetri ini menggunakan kunci enkripsi dan dekripsi yang berbeda, pada konsep ini kunci untuk mengenkrip pesan disebarkan (*public key*), sementara kunci rahasia tetap disimpan. Jadi setiap orang yang memiliki *public key* dapat mengenkripsi pesan, sementara yang bisa membaca hanya yang memiliki kunci rahasia. Kelebihan dari algoritma asimetri adalah keamanan data dapat lebih terjamin dan tidak banyak distribusi kunci, sementara kelemahannya adalah membutuhkan proses yang cukup lama dan membutuhkan kunci yang lebih panjang jika dibandingkan dengan algoritma simetri.

2.4 Algoritma Advanced Encryption Standard

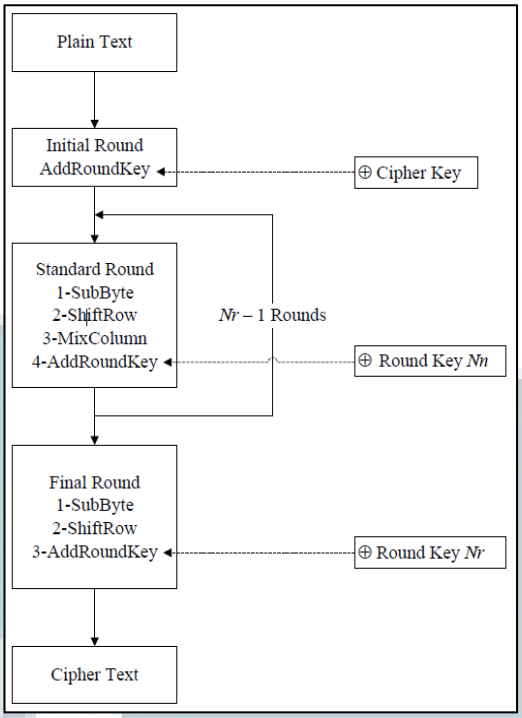
Menurut Selent (2010) dalam jurnal *Advanced Encryption Standard* mengatakan bahwa algoritma *Advanced Encryption Standard* menggunakan kombinasi operasi *Exclusive-OR* (XOR), substitusi dengan *S-Box*, rotasi baris dan kolom, dan *mixcolomn*. Algoritma ini cukup baik karena mudah untuk diterapkan dan dapat dijalankan dalam jumlah waktu yang wajar pada komputer biasa.

Jenis eksripsi *Advanced Encryption Standard* terbagi tiga, yaitu AES-128, AES-192 dan AES-256. Pengelompokan jenis AES ini adalah berdasarkan panjang kunci yang digunakan. Angka-angka di belakang kata AES menggambarkan panjang kunci yang digunakan pada setiap AES. Selain itu, hal yang membedakan dari masing-masing AES ini adalah banyaknya jumlah *round* yang dipakai. AES-128 menggunakan 10 *round*, AES-192 sebanyak 12 *round*, dan AES-256 sebanyak 14 *round* (Daemen, 1999). Perbandingan antara AES-128, AES-192, dan AES-256 dapat dilihat pada Tabel 2.1.

Tabel 2.1 Perbandingan Tipe Enkripsi AES (Daemen, 1999)

	Panjang Kunci (Nk)	Ukuran Blok (Nb)	Jumlah Ronde (Nr)
AES-128	4	4	10
AES-192	6	4	12
AES-256	8	4	14

Blok diagram proses enkripsi AES dapat dilihat pada Gambar 2.1. Dengan *Nr* merupakan banyaknya putaran yang dilakukan dan *Nn* adalah putaran ke-*n*.



Gambar 2.1 Blok Diagram Enkripsi AES (Stallings, 2003).

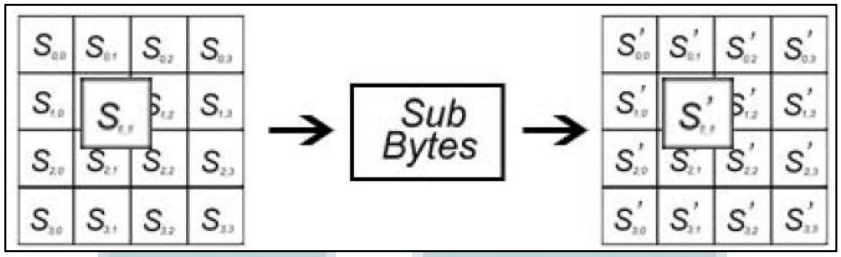
Berdasarkan paper dari NIST tentang spesifikasi algoritma AES tahun 2001, terdapat empat tahap utama untuk melakukan enkripsi dengan menggunakan algoritma AES yaitu *Add Round Key, SubBytes, ShiftRows*, dan *MixColumns*. Selain keempat tahap yang baru saja disebutkan, terdapat satu tahap lagi yang tidak kalah pentingnya, yaitu *Key Expansion*. Berbeda dengan keempat tahap utama sebelumnya, keempat tahap tersebut dilakukan ulang setiap rondenya, *Key Expansion* hanya dilakukan sekali dalam satu kali tahap enkripsi atau dekripsi.

Penjabaran mengenai proses umum algoritma Advanced Encryption Standard adalah sebagai berikut (Stallings, 2003) :

1. SubBytes

   Forward subtitute byte transformation atau *SubBytes* merupakan proses subtitusi sederhana dari 16 nilai matriks 4x4 kepada 16 nilai baru

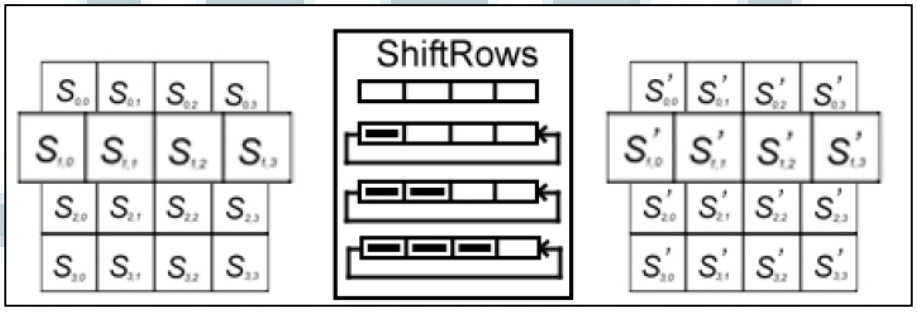
mengikuti aturan permutasi *S-Box*. Proses *SubBytes* ditunjukkan pada Gambar 2.2.



Gambar 2.2. Proses *SubBytes* (Stallings, 2003).

2. ShiftRows

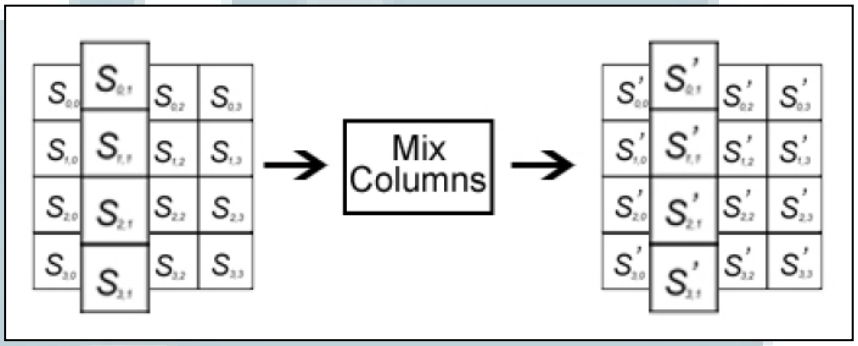
Forward shift rows atau *ShiftRows* merupakan proses permutasi sederhana dari 16 nilai matriks 4x4 kepada 16 nilai baru matriks 4x4. *Shift Rows* adalah tahap dimana baris-baris yang ada pada *state array* dirotasikan ke kiri, yang artinya kolom pertama dipindahkan ke kolom terakhir di baris yang sama. Pada baris keempat rotasi dilakukan sebanyak tiga kali, sedangkan untuk baris ketiga rotasi dilakukan sebanyak 2 kali dan untuk baris kedua rotasi dilakukan sebanyak 1 kali. Baris pertama tidak dilakukan rotasi sama sekali. Proses ShiftRows ditunjukkan Gambar 2.3.



Gambar 2.3. Proses *ShiftRows* (Stallings, 2003).

3. MixColumns

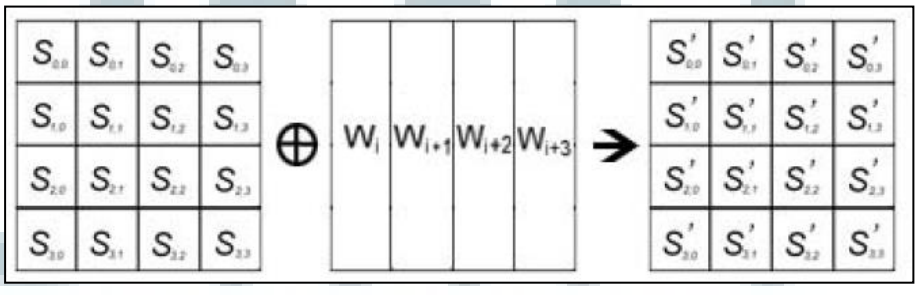
Forward mix column atau *MixColumns* merupakan operasi terhadap setiap kolom secara terpisah. Transformasi tersebut didefinisikan dengan proses mengalikan matriks *mix column* yang berukuran 4x4 dengan matriks *state* berukuran 4x4. Proses MixColumns ditunjukkan pada Gambar 2.4.



Gambar 2.4. Proses *MixColumns* (Stallings, 2003).

4. AddRoundKey

Forward add round key atau *AddRoundKey* merupakan proses XOR sederhana antara matriks *state* 4x4 dengan matriks 4x4 yang merupakan *key* dari *round* yang bersesuaian hasil ekspansi *key*. Proses *AddRoundkey* ditunjukkan pada Gambar 2.5.



Gambar 2.5. Proses *AddRoundkey* (Stallings, 2003).