# PENYADAPAN SMS DAN GPS BERBASIS ANDROID MENGGUNAKAN ALGORITMA *ADVANCED ENCRYPTION STANDARD* (AES)

**Rahmayunita*[1], Isnawaty[2], Sutardi[2]**
[*1,2,3]Jurusan Teknik Informatika, Fakultas Teknik, Universitas Halu Oleo, Kendari
e-mail : [*1]**uundrahmayunita@gmail.com** , [2]isna.1711@gmail.com, [3]sutardi_hapal@yahoo.com

**Abstrak**

Salah satu fitur *handphone* yang paling sering digunakan saat ini adalah *Short Message Service* (SMS). SMS merupakan layanan yang disediakan oleh *handphone* untuk mengirim ataupun menerima pesan singkat. Selain itu, fitur *Global Positionig System* (GPS) saat ini juga sangat dibutuhkan oleh masyarakat dimana dapat membantu dalam pelacakan.

Tujuan dari penelitian ini adalah untuk merancang sebuah aplikasi yang dapat membantu dalam mengontrol kegiatan atau pun aktivitas yang dilakukan oleh kerabat ataupun orang lain, serta mengamankan data SMS dan lokasi GPS kerabat yang akan dipantau untuk menghindari ancaman pengaksesan dari pihak – pihak yang tidak berwenang.

Metode yang digunakan untuk penyadapan SMS dan GPS yaitu dengan menggunakan perantara *web service*, sedangkan metode yang digunakan untuk mengamankan data SMS dan GPS adalah metode *Advanced Encryption Standard* (AES). Metode AES merupakan metode kriptografi kunci simetri yaitu kunci untuk enkripsi sama dengan kunci untuk dekripsi.

Hasil penelitian ini menunjukkan bahwa SMS dan lokasi GPS dapat terkirim ke *web server* dengan adanya fungsi *web service* yang akan mentransfer data SMS yang ada pada *handphone* dan menangkap lokasi GPS pihak tersadap. Untuk penelitian enkripsi AES menunjukkan bahwa pesan yang sama dengan kunci yang berbeda dapat menghasilkan *chipertext* yang berbeda.

**Kata Kunci** : *Penyadapan, SMS, GPS, Android, Web Service, Algoritma AES, enkripsi, dekripsi*

***Abstract***

*One of feature from hand phone that mostly used by almost all people is Short Message Service (SMS). SMS is a service provided by hand phone to send or receive a short message. In other side, Global Positioning System (GPS) is one of the most important features that used for tracing.*

*The purpose of this research is to design an application that can help and control the activity that do by the people, and to secure the data from SMS and GPS location from the relation that will be monitored to avoid the threat from the people that try to access the data.*

*The method that used to tap the SMS and GPS is by using web service media, meanwhile, the method that used to secure the data from SMS is Advance Encryption Standard (AES) method. AES method is symmetry cryptographic keys method that is the key to encryption is equal with key to decryption.*

*The result of this research shows that SMS and GPS location can be sent to web server with the function of web service that transfer the SMS data from hand phone and detect target GPS location. The encryption AES research shows that the same message with different keys can result different chipper text.*

***Keywords*** : *Tap, SMS, GPS, Android, Web Service, AES Algorithm, Encryption, Decryption*

## 1. PENDAHULUAN

Penggunaan internet telah merasuk hampir ke semua aspek kehidupan manusia baik itu aspek sosial, hiburan, pendidikan, maupun ekonomi. Hal ini terbukti dengan pengunaan internet yang sangat besar di kalangan anak muda, terlebih mengetahui lokasi dan informasi secara *real-time* sudah merupakan hal yang sangat mudah untuk zaman sekarang.

Komunikasi jarak jauh sudah merupakan hal yang sangat mudah. Salah satunya yaitu dengan adanya teknologi *handphone* yang didalamnya terdapat fasilitas *Short Message Service* (SMS). Selain SMS, teknologi yang berkembang saat ini yaitu *Global Positioning System* (GPS). GPS merupakan pengembangan dari sebuah peta lokasi yang dimanifestasikan dalam bentuk teknologi dengan menggunakan satelit. GPS dapat menjadi sarana untuk mencari lokasi atau daerah tertentu yang tidak diketahui atau belum pernah dikunjungi sebelumnya.

Pertukaran informasi yang sangat cepat dan akurat maka dibutuhkan keamanan dalam setiap pertukaran informasi, baik pada SMS dan GPS untuk menjaga privasi atau tidak disebarluaskan kemasyarakat umum. Banyaknya yang menyalahgunakan fasilitas yang diberikan oleh teknologi dengan cara menyadap informasi pertukaran data seseorang tanpa diketahui, sehingga sangat diperlukan *enkripsi* untuk setiap pertukaran informasi baik SMS dan GPS. Dengan permasalahan diatas maka dibutuhkan sebuah sistem keamanan yang dapat mengamankan informasi, yaitu enkripsi AES yang diharapkan dapat menjaga privasi dan mengamankan data sehingga data tersebut tidak disalah gunakan oleh pihak yang tidak bertanggung jawab.

Saat ini mengontrol kegiatan anak ataupun kerabat merupakan hal yang harus diperhatikan untuk menghindari kegiatan menyimpang yang dilakukan terutama dengan adanya fasilitas *Short Message Service* (SMS). Oleh karena itu, sangat diperlukan aplikasi penyadapan untuk menghindari hal – hal yang tidak diinginkan. Pada aplikasi penyadapan ini dapat menyadap SMS yang masuk ataupun SMS yang keluar pada HP serta dapat mengetahui lokasinya, dimana aplikasi penyadapan ini dilengkapi dengan sistem keamanan dengan menggunakan *enkripsi* AES.

Penelitian ini diharapkan dapat membantu seseorang untuk mengakses lokasi dan kegiatan pihak tersadap melalui SMS.

## 2. METODE PENELITIAN

### 2.1 Kriptografi

Kriptografi pada awalnya dijabarkan sebagai ilmu yang mempelajari cara menyembunyikan pesan, namun pada pengertian modern, *kriptografi* adalah ilmu yang berdasarkan pada teknik matematika untuk berurusan dengan keamanan informasi seperti kerahasian, keutuhan data, dan otentikasi entitas. Jadi, pengertian kriptografi modern adalah tidak saja berurusan hanya dengan penyembunyian pesan, tetapi lebih pada sekumpulan teknik yang menyediakan keamanan informasi.

Kriptografi adalah ilmu dan seni untuk menjaga kerahasiaan berita. Ada empat tujuan mendasar dari ilmu kriptografi yang juga merupakan aspek keamanan informasi yaitu [1] :

1. Kerahasiaan adalah layanan yang digunakan untuk menjaga isi dari informasi dari siapapun kecuali yang memiliki otoritas atau kunci rahasia untuk membuka informasi yang telah disandi.
2. *Integritas* data adalah berhubungan dengan penjagaan dari perubahan data secara tidak sah. Untuk menjaga *integritas* data, sistem harus memiliki kemampuan untuk mendeteksi manipulasi data oleh pihak-pihak yang tidak berhak antara lain penyisipan, penghapusan, dan pensubsitusian data lain kedalam data yang sebenarnya.
3. *Autentikasi* adalah berhubungan dengan identifikasi, baik secara kesatuan sistem maupun informasi itu sendiri. Dua pihak yang saling berkomunikasi harus saling memperkenalkan diri. Informasi yang dikirimkan melalui kanal harus diautentikasi keaslian, isi datanya, waktu pengiriman, dan lain-lain.
4. *Non-repudiasi* adalah usaha untuk mencegah terjadinya penyangkalan

terhadap pengiriman suatu informasi oleh yang mengirim.

2.2 Penyadapan

Penyadapan telepon (atau penyadapan kawat) adalah pemantauan percakapan telepon dan Internet oleh pihak ketiga, sering kali dilakukan dengan cara rahasia. Percakapan telepon dapat direkam atau dipantau secara tidak resmi, baik oleh pihak ketiga tanpa sepengetahuan pihak yang disadap, ataupun direkam oleh salah satu pihak yang melakukan penggilan telepon. Penyadapan telepon dikontrol secara ketat dan pada umumnya dilarang dengan alasan privasi, namun juga bisa dilegalkan untuk alasan tertentu, sesuai dengan hukum yang berlaku di negara yang bersangkutan memberitahukan adanya isi baru tersebut atau langsung mengunduhnya.

ATIS (*Audio Telecommunication International Systems*) adalah sebuah generasi baru dari *Instant Recall Recorders* (IRC) dalam teknologi *solid-state*, yang dapat dikoneksikan ke dalam audio source berupa telepon atau handphone GSM/AMPS/CDMA dan akan merekam atau menyadap seluruh komunikasi suara dengan kapasitas aktif lebih dari 680 menit dan 1000 panggilan yang berbeda. Kompresi algoritma yang ada di dalam ATIS telah memperbesar kapasitas penyimpanan dan kualitas suara yang cukup jernih.Dengan menggunakan koneksi telepon [2].

2.3 Short Message Service (SMS)

SMS adalah singkatan untuk *Short Message Service*, lebih dikenal sebagai pesan teks singkat atau "*texting*". Teknologi SMS ini digunakan untuk mengirim pesan secara nirkabel hingga 160 karakter antara ponsel atau perangkat lainnya. SMS bukan hanya teknologi SMS saja, tetapi merupakan standar yang digunakan oleh sebagian besar jaringan ponsel utama. Selain itu SMS merupakan metode *store* dan *forward* sehingga keuntungan yang didapat adalah pada saat telepon selular penerima tidak dapat dijangkau, dalam arti tidak aktif atau diluar *service area*. Penerima tetap dapat menerima SMS apabila telepon selular tersebut sudah aktif kembali. SMS menyediakan mekanisme untuk mengirimkan pesan singkat dari dan menuju media - media *wireless* dengan menggunakan sebuah *Short Messaging Service Center* (SMSC), yang bertindak sebagai sistem yang berfungsi menyimpan dan mengirimkan kembali pesan-pesan singkat.

Proses pengiriman SMS antar teknologi jaringan yang berbeda dalam pengiriman antara dua teknologi jaringan yang berbeda terdapat beberapa tahap. Pertama, pesan di buat dan kirimkan oleh ESME ke SMSC pengirim. Selanjutnya SMSC pengirim meneruskan pesan melalui SMSC penerima dan SMSC penerima mengirimkan pesan ke ESME penerima. Jika status *report* diminta oleh pengirim pesan, maka SMSC penerima membuat status *report* dan mengirimkanya ke ESME pengirim [2].

2.4 Global Positioning System (GPS)

*Global Positioning System* (GPS) adalah sistem satelit *navigasi* dan penentuan posisi yang dimiliki dan dikelola oleh Amerika Serikat. Sistem ini didesain untuk memberikan posisi dan kecepatan tiga dimensi serta informasi mengenai waktu, secara *kontinyu* di seluruh dunia tanpa bergantung waktu dan cuaca bagi banyak orang secara simultan. Saat ini GPS sudah banyak digunakan diseluruh dunia dalam berbagai bidang aplikasi yang menuntut informasi tentang posisi, kecepatan, percepatan ataupun waktu yang teliti. GPS dapat memberikan informasi posisi dengan ketelitian bervariasi dari beberapa millimeter (orde nol) sampai dengan puluhan meter.

Sistem kerja GPS adalah dengan menstransmisikan sinyal dari satelit ke perangkat GPS (*portable GPS* murni, ataupun *smartphone* yang sudah memiliki fitur GPS). GPS membutuhkan transmisi dari 3 satelit untuk mendapatkan informasi dua dimensi (lintang dan bujur), dan 4 satelit untuk tiga dimensi (lintang, bujur dan ketinggian). Karena GPS bekerja mengandalkan satelit, maka penggunaannya disarankan di tempat terbuka. Penggunaan di dalam ruangan atau di tempat yang menghalangi arah satelit (di angkasa), maka GPS tidak akan bekerja secara akurat dan maksimal. Setiap daerah di atas permukaan bumi ini minimal terjangkau oleh 3-4 satelit [3].

2.5 Algoritma Advanced Encrpytion Standart (AES)

*Advanced Encryption Standard (AES)* merupakan algoritma *cryptographic* yang dapat digunakan untuk mengamankan data. Algoritma AES adalah blok *chipertext simetrik* yang dapat meng*enkripsi* (*encipher*) dan *dekripsi* (*decipher*) informasi. *Enkripsi* mengubah data yang tidak dapat lagi dibaca disebut *ciphertext*; sebaliknya *dekripsi* adalah merubah *ciphertext* data menjadi bentuk semula yang dikenal sebagai *plaintext*. Algoritma AES menggunakan kunci *kriptografi* 128, 192, dan 256 bits untuk mengenkrip dan dekrip data pada blok 128 bits.

*Advanced Encryption Standard* (AES) adalah lanjutan dari algoritma *Data Encryption Standard* (DES) yang masa berlakunya dianggap telah usai karena faktor keamanan. Kecepatan komputer yang sangat pesat dianggap sangat membahayakan DES, sehingga pada tanggal 2 Maret tahun 2001 ditetapkanlah algoritma baru AES sebagai AES. Kriteria pemilihan AES didasarkan pada 3 kriteria utama yaitu keamanan, harga, dan karakteristik algoritma beserta implementasinya.

Keamanan merupakan faktor terpenting dalam evaluasi, yang meliputi ketahanan terhadap semua analisis sandi yang telah diketahui dan diharapkan dapat menghadapi analisis sandi yang belum diketahui. Di samping itu, AES juga harus dapat digunakan secara bebas tanpa harus membayar royalti, dan juga murah untuk diimplementasikan pada *smart card* yang memiliki ukuran memori kecil [4].

1. Struktur Enkripsi AES

*Enkripsi* AES adalah transformasi terhadap *state* secara berulang dalam beberapa tahap. Pada awalnya teks asli direorganisir sebagai sebuah *state*. Kemudian *plaintext* diproses dengan kunci ronde ke-0 (*AddRoundKey*). Setelah itu, tahap ke-1 sampai dengan tahap ke-$(N_r - 1)$ dengan $N_r$ adalah jumlah tahap menggunakan empat jenis transformasi, yaitu *SubBytes*, *ShiftRows*, *MixColumns* dan *AddRoundKey*. Pada tahap terakhir, yaitu tahap ke-Nr dilakukan transformasi serupa dengan ronde lain namun tanpa transformasi *MixColumns* [4].

2. Struktur Dekripsi AES

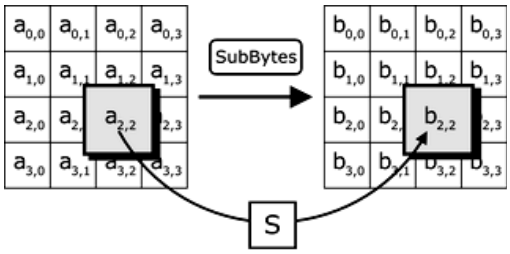
Secara ringkas algoritma *dekripsi* AES merupakan kebalikan algoritma *enkripsi* AES. Algoritma *dekripsi* AES menggunakan transformasi *invers* semua transformasi dasar yang digunakan pada algoritma *enkripsi* AES antara lain : *AddRoundKey, InvShiftRows* dan *InvSubBytes*. Setelah proses tersebut akan melakukan proses yang serupa dengan menambahkan transformasi *InvMixColoumns*. Hasil dari proses transformasi tersebut akan dilakukan proses *AddroundKey* untuk menghasilkan *output* berupa *plaintext* [4].

2.6 Transformasi pada AES

Algoritma *enkripsi* AES menggunakan empat jenis transformasi yaitu substitusi yang disebut dengan *SubBytes*, permutasi yang disebut dengan *ShiftRows*, pencampuran yang disebut dengan *MixColumns*, dan penambahan kunci yang disebut dengan *AddRoundKey* [4].

1. SubBytes

AES menggunakan substitusi nonlinear pada ukuran *byte* yang disebut dengan *SubBytes*. Ada dua cara untuk mengkomputasi substitusi dengan *SubBytes*, yaitu dengan menggunakan tabel substitusi *s-box*. Gambar 1 menunjukkan proses *SubBytes*.



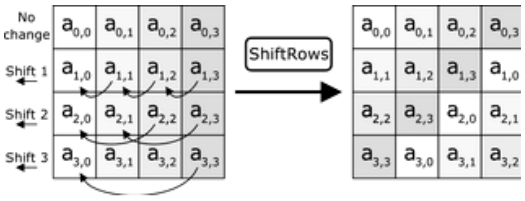

Gambar 1 Proses *SubBytes*

2. ShiftRows

Selain menggunakan substitusi untuk mengganti nilai pada elemen *state*, AES menggunakan permutasi pada *state*. Transformasi pada *state* disebut dengan transformasi *ShiftRows*. *ShiftRows* dilakukan dengan menjalankan operasi *circular shift left* sebanyak *i* pada baris ke-*i* pada *state*.

Transformasi *ShiftRows* merupakan jenis transformasi permutasi, yaitu pengubahan posisi elemen pada *state* tanpa

mengubah nilainya. Gambar 2 menunjukkan proses *ShiftRows*.




Gambar 2 Proses *ShiftRows*

3. MixColumns

Tujuan transformasi *MixColumns* adalah mencampur nilai kolom-kolom pada *state* pada satu elemen pada *state* keluaran. Untuk melakukan pencampuran itu, transformasi *MixColumns* menggunakan operasi perkalian *matrix* dengan operasi perkalian dan penjumlahan menggunakan operator pada GF ($2^8$) dengan *irreducible polynomial* ($x^8 + x^4 + x^3 + x + 1$).

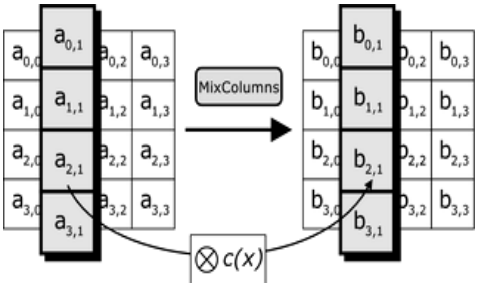
Langkah *MixColumns* dapat ditunjukkan dengan mengalikan empat bilangan di dalam *Galois field* oleh *matrix* berikut ini:

$$\begin{bmatrix} 2 & 3 & 1 & 1 \\ 1 & 2 & 3 & 1 \\ 1 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \end{bmatrix} \begin{bmatrix} a_0 \\ a_1 \\ a_2 \\ a_3 \end{bmatrix}$$

Jika dijabarkan menjadi :

$$r_0 = 2a_0 \oplus 3a_1 \oplus a_2 \oplus a_3$$
$$r_1 = a_0 \oplus 2a_1 \oplus 3a_2 \oplus a_3$$
$$r_2 = a_0 \oplus a_1 \oplus 2a_2 \oplus 3a_3$$
$$r_3 = 3a_0 \oplus a_1 \oplus a_2 \oplus 2a_3$$

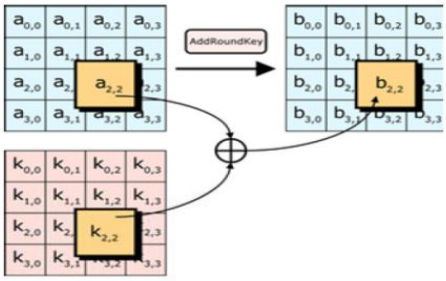
Gambar 3 menunjukkan proses *MixColumns*.




Gambar 3 Proses *MixColumns*

4. AddRoundKey

Transformasi keempat yang digunakan pada penyandian AES adalah transformasi *AddRoundKey*. Transformasi *AddRoundKey* mencampur sebuah *state* masukan dengan kunci ronde dengan operasi eksklusif OR ($\oplus$). Setiap elemen pada *state* masukan yang merupakan sebuah *byte* dikenakan operasi eksklusif OR dengan *byte* pada posisi yang sama di kunci ronde (kunci ronde direpresentasikan sebagai *state*). Gambar 4 menunjukkan proses *AddRoundKey*.




Gambar 4 Proses *AddRoundKey*

2.7 Analisa Penjadwalan Kunci

Proses penjadwalan kunci merupakan proses di mana *cipherkey* dijadwalkan untuk menghasilkan *subkey-subkey* yang digunakan untuk proses *enkripsi* dan *dekripsi* pada algoritma AES. Contoh penjadwalan kunci pada algoritma AES jika diketahui kunci yang akan digunakan untuk *enkripsi* dengan panjang 16 *byte* atau matriks 4x4, yaitu:

$$Cipherkey = abcdefghijklmnop$$

Tahapan penjadwalan kunci, yaitu :

A. Tahapan awal ubah *cipherkey* ke dalam bentuk *hexadecimal* menggunakan tabel ASCII menjadi :

$$Cipherkey = 61\ 62\ 63\ 64\ 65\ 66\ 67\ 68\ 69\ 6A\ 6B\ 6C\ 6D\ 6E\ 6F\ 70$$

B. Tahap selanjutnya melakukan operasi-operasi penjadwalan kunci. Operasi-operasi yang dilakukan yaitu *RotWord*, *SubByte*, dan melakukan operasi XOR untuk menghasilkan *subkey*. Operasi-operasi yang dilakukan yaitu sebagai berikut:

1. Memasukan *cipherkey* tersebut ke dalam bentuk matriks 4x4 (blok 16 *byte)* menjadi :

$$W = \begin{bmatrix} 61 & 65 & 69 & 6d \\ 62 & 66 & 6a & 6e \\ 63 & 67 & 6b & 6f \\ 64 & 68 & 6c & 70 \end{bmatrix}$$

2. Melakukan operasi *RotWord* yaitu menggeser blok paling atas ke blok paling bawah pada kolom terakhir dari *ciphertext* (W).

$$\begin{bmatrix}6d\\6e\\6f\\70\end{bmatrix} = \begin{bmatrix}6e\\6f\\70\\6d\end{bmatrix}$$

3. Melakukan operasi *SubByte* dengan tabel *s-box*.

$$\begin{bmatrix}6e\\6f\\70\\6d\end{bmatrix} = \begin{bmatrix}9f\\a8\\51\\3c\end{bmatrix}$$

4. Hasil dari operasi *SubByte* dilakukan operasi XOR dengan *rcon* (kolom pertama) dan $W_1$ (kolom ke-1 dari W)

$$rcon = \begin{bmatrix}01 & 02 & 04 & 08 & 10 & 20 & 40 & 80 & 1b & 36\\00 & 00 & 00 & 00 & 00 & 00 & 00 & 00 & 00 & 00\\00 & 00 & 00 & 00 & 00 & 00 & 00 & 00 & 00 & 00\\00 & 00 & 00 & 00 & 00 & 00 & 00 & 00 & 00 & 00\end{bmatrix}$$

$$\begin{bmatrix}61\\62\\63\\64\end{bmatrix} \oplus \begin{bmatrix}9f\\a8\\51\\3c\end{bmatrix} \oplus \begin{bmatrix}01\\00\\00\\00\end{bmatrix} = \begin{bmatrix}ff\\ca\\32\\58\end{bmatrix}$$

5. Melakukan operasi XOR untuk kolom ke-2 dari kolom W

$$\begin{bmatrix}65\\66\\67\\68\end{bmatrix} \oplus \begin{bmatrix}ff\\ca\\32\\58\end{bmatrix} = \begin{bmatrix}9a\\ac\\55\\30\end{bmatrix}$$

6. Melakukan operasi XOR untuk kolom ke-3 dari kolom W

$$\begin{bmatrix}69\\6a\\6b\\6c\end{bmatrix} \oplus \begin{bmatrix}9a\\ac\\55\\30\end{bmatrix} = \begin{bmatrix}f3\\c6\\3e\\5c\end{bmatrix}$$

7. Melakukan operasi XOR untuk kolom ke-4 dari kolom W

$$\begin{bmatrix}6d\\6e\\6f\\70\end{bmatrix} \oplus \begin{bmatrix}f3\\c6\\3e\\5c\end{bmatrix} = \begin{bmatrix}9e\\a8\\51\\2c\end{bmatrix}$$

8. Hasil dari operasi XOR disimpan ke dalam *subkey*.

$$SubKey = \begin{bmatrix}ff & 9a & f3 & 9e\\ca & ac & c6 & a8\\32 & 55 & 3e & 51\\58 & 30 & 5c & 2c\end{bmatrix}$$

*Subkey* ini yang akan digunakan untuk proses *enkripsi* atau *dekripsi* pada algoritma AES pada *round* ke-1 untuk *round* selanjutnya dilakukan penjadwalan kunci kembali sampai *round* ke-10.

### 2.8 Aplikasi *Mobile*

Menurut [5], aplikasi *mobile* merupakan aplikasi yang dapat digunakan walaupun pengguna berpindah dengan mudah dari satu tempat ketempat lain tanpa terjadi pemutusan atau terputusnya komunikasi. Dengan aplikasi *mobile* memudahkan pengguna mengakses berbagai fitur yang disediakan seperti hiburan dimana fitur hiburan paling banyak digemari oleh hampir 70% pengguna telepon seluler, karena dengan memanfaatkan adanya *fitur game*, *music player* dan video *player* membuat penguna menjadi semakin mudah menikmati hiburan kapan saja dan dimanapun.

## 3. HASIL DAN PEMBAHASAN

Implementasi merupakan tahap dimana sistem siap untuk dioperasikan. Hasil analisis dan perancangan diimplementasikan dalam bentuk aplikasi pengenalan sidik jari dengan menggunakan bahasa pemrograman Java. Aplikasi ini merupakan aplikasi *executable* berformat JAR.

Spesifikasi perangkat keras dan perangkat lunak yang digunakan dalam implementasi adalah sebagai berikut:

1. Perangkat keras yang dibutuhkan (*required software*) ditunjukkan oleh Tabel 1.

Tabel 1 Kebutuhan perangkat keras

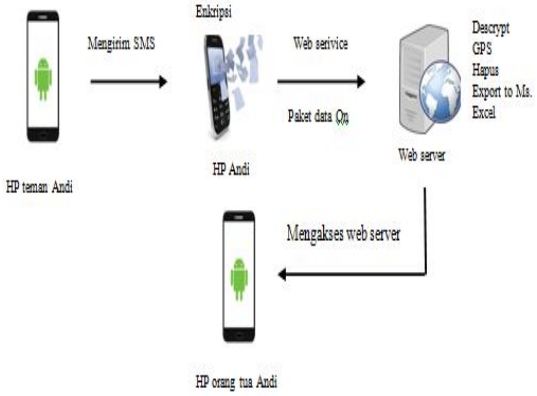
| No | Nama Perangkat | Spesifikasi |
|---|---|---|
| 1. | *Processor* | *Core i 3* |
| 2. | *Harddisk* | *500 GB* |
| 3. | *Memory* | *2 GB DDR3* |
| 4. | *Handphone* | Sistem operasi *Android Jelly Bean 4.1* |
| 5. | Modem | 7.2 Mbps |

2. Perangkat lunak yang dibutuhkan (*required software*) ditunjukkan oleh Tabel 2.

Tabel 2 Kebutuhan perangkat lunak

| No | Nama Perangkat | Spesifikasi |
|---|---|---|
| 1. | *Operating System* | *Microsoft Windows 7* |
| 2. | *Android Developer Tools* | 2.1.0 |
| 3. | *Netbeans* | *7.0.1* |
| 4. | *Java Development Kit* (*JDK*) | *JDK 1.7* |
| 5. | *Java Runtime Environment* (*JRE*) | *JRE 7* |
| 6. | *Xampp* | *2.5.10* |

Arsitektur umum sistem penyadapan SMS ditunjukkan oleh Gambar 5.

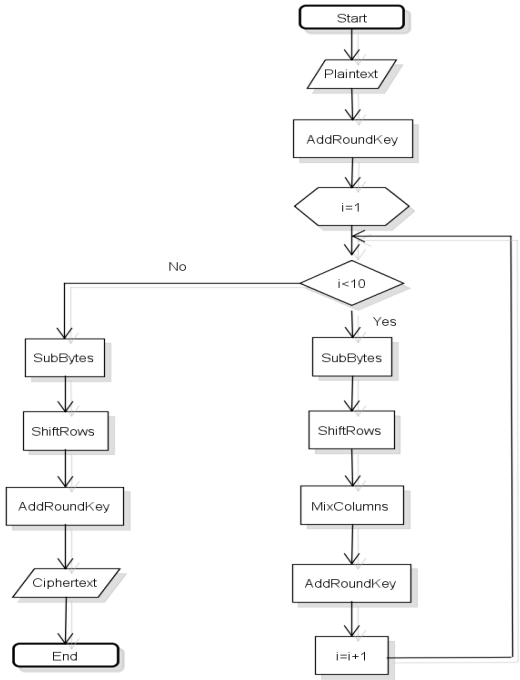



Gambar 5 Arsitektur umum penyadapan SMS dan GPS

Gambar 5 merupakan perancangan arsitektur sistem yang diilustrasikan sebagai berikut: Teman Andi mengirim SMS ke *handphone* Andi dimana pada *handphone* Andi telah diinstal aplikasi penyadapan SMS. Untuk menyimpan hasil sadapan ke *web server* dibutuhkan perantara *web service*. Fungsi dari *web service* ini sendiri menghubungkan *platform android* ke *web server* yang telah dibuat. Selain itu, fungsi dari *web service* adalah mengambil parameter yang ada pada *android* untuk dimasukkan kedalam *web server*. Setelah SMS sadapan masuk ke *web server* orang tua Andi bertindak sebagai *user* yang dapat mengakses *web server* tersebut.

Pada *web service* ini mengunakkan API (*Application Programming Interface*) untuk perantara antara android ke *web server*. API secara sederhana bisa diartikan sebagai kode program yang merupakan antarmuka atau penghubung antara aplikasi atau web yang dibuat dengan fungsi - fungsi yang dikerjakan. Misalnya dalam hal ini *Google* API berarti kode program (yang disederhanakan) yang dapat ditambahkan pada aplikasi atau web untuk mengakses, menjalankan, memanfaatkan fungsi atau fitur yang disediakan Google.

Proses enkripsi pada algoritma AES terdiri dari empat operasi yaitu *AddRoundKey*, *SubBytes*, *ShiftRows*, dan *MixColumns*. Operasi-operasi ini diulang terus-menerus hingga menghasilkan *ciphertext*. Jumlah perulangan yang dilakukan tergantung pada ukuran blok dan kunci yang digunakan, dalam hal ini ukuran blok dan kunci yang digunakan yaitu 128 *bit*. Sehingga perulangan yang dilakukan sebanyak 10 iterasi.




Gambar 6 *Flowchart* proses enkripsi algoritma AES

Contoh enkripsi pada algoritma AES, yaitu:

$$Cipherkey = ABCDEFGHIJKLMNOP$$
$$Plaintext = TEKNIK\ KENDARI\ !$$

Dengan solusi atau penyelesaian dengan tahap-tahap sebagai berikut:

a. Tahap awal mengubah *cipherkey* dan *plaintext* ke dalam bentuk *hexadecimal* menjadi sebagai berikut:

$Cipherkey$
= 41 42 43 44 45 46 47 48 49 4$a$ 4$b$ 4$c$ 4$d$ 4$e$ 4$f$ 50

$Plaintext$
= 54 45 4$b$ 4$e$ 49 4$b$ 20 4$b$ 45 4$e$ 44 41 52 49 20 21

b. Memasukan *cipherkey* dan *plaintext* ke dalam bentuk *matriks* 4x4 (blok 16 *byte)* sehingga menjadi:

$$Plaintext = \begin{bmatrix} 54 & 49 & 45 & 52 \\ 45 & 4b & 4e & 49 \\ 4b & 20 & 44 & 20 \\ 4e & 4b & 41 & 21 \end{bmatrix}$$

$$Cipherkey = \begin{bmatrix} 41 & 45 & 49 & 4d \\ 42 & 46 & 4a & 4e \\ 43 & 47 & 4b & 4f \\ 44 & 48 & 4c & 50 \end{bmatrix}$$

c. *Cipherkey* dan *plaintext* yang telah dimasukan ke dalam blok selanjutnya dapat dilakukan operasi-operasi enkripsi pada algoritma AES sebagai berikut:

1. Melakukan operasi *AddRoundKey* dengan melakukan operasi XOR pada setiap kolom di *plaintext* dengan kolom di *cipherkey*.

$$\begin{bmatrix} 54 & 49 & 45 & 52 \\ 45 & 4b & 4e & 49 \\ 4b & 20 & 44 & 20 \\ 4e & 4b & 41 & 21 \end{bmatrix} \oplus \begin{bmatrix} 41 & 45 & 49 & 4d \\ 42 & 46 & 4a & 4e \\ 43 & 47 & 4b & 4f \\ 44 & 48 & 4c & 50 \end{bmatrix}$$

$$= \begin{bmatrix} 15 & 0c & 0c & 1f \\ 04 & 0d & 04 & 07 \\ 08 & 67 & 0f & 6f \\ 0a & 03 & 0d & 71 \end{bmatrix}$$

2. Setelah dilakukan operasi *AddRoundKey* tersebut dilakukan perulangan dengan urutan operasi pertama yaitu operasi *SubByte*. Operasi ini yaitu melakukan subtitusi dengan tabel *s-box.*

$$\begin{bmatrix} 15 & 0c & 0c & 1f \\ 04 & 0d & 04 & 07 \\ 08 & 67 & 0f & 6f \\ 0a & 03 & 0d & 71 \end{bmatrix} \rightarrow \begin{bmatrix} 59 & fe & fe & c0 \\ f2 & d7 & f2 & c5 \\ 30 & 85 & 76 & a8 \\ 67 & 7b & d7 & a3 \end{bmatrix}$$

3. Hasil dari operasi *SubByte* dilakukan operasi *ShiftRows* yaitu memutar tiga baris terakhir dari state seperti berikut:

$$\begin{bmatrix} 59 & fe & fe & c0 \\ f2 & d7 & f2 & c5 \\ 30 & 85 & 76 & a8 \\ 67 & 7b & d7 & a3 \end{bmatrix} \rightarrow \begin{bmatrix} 59 & fe & fe & c0 \\ d7 & f2 & c5 & f2 \\ 76 & a8 & 30 & 85 \\ a3 & 67 & 7b & d7 \end{bmatrix}$$

4. Melakukan operasi *MixColumns* yaitu melakukan perkalian tiap kolom pada hasil operasi *ShiftRows* dengan matriks seperti berikut:

$$\begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \times \begin{bmatrix} 59 & fe & fe & 15 \\ d7 & f2 & c5 & c5 \\ 76 & a8 & 30 & 85 \\ 51 & 67 & 7b & d7 \end{bmatrix}$$

- $02 * 59$ = 0000 0010 $*$ 0101 1001
  = $x * x^6 + x^4 + x^3 + 1$
  = $x^7 + x^5 + x^4 + 1$
  = 1011 0001
- $03 * d7$ = 0000 0011 $*$ 1101 0111
  = $x + 1 * x^7 + x^6 + x^5 + x^3 + x^2 + x$
  = $x^8 + x^6 + x^5 + x^4 + x^3$
- Karena lebih dari 8 *bit* maka harus dilakukan XOR dengan 11B.

1 0111 1000 $\oplus$ 1 0001 1011 = 0110 0011

- $01 * 76$ = 0000 0001 $*$ 0111 0110 = 0111 0110

  $01 * a3$ = 0000 0001 $*$ 1010 0011
  = 1010 0011

  1011 0001 $\oplus$ 0110 0011 $\oplus$ 0111 0110 $\oplus$ 1010 0011
  = 0000 0111
  = 07

Setelah melakukan perkalian matriks tiap baris dan kolom, diperoleh

$$\begin{bmatrix} 07 & 66 & 72 & 54 \\ 18 & 85 & 47 & 7a \\ a2 & ed & d3 & a3 \\ 17 & 8e & 15 & ca \end{bmatrix}$$

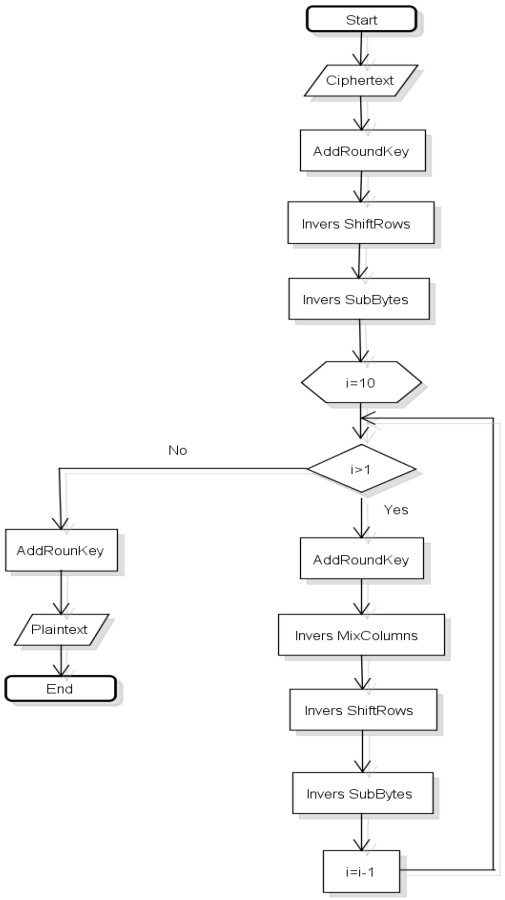
5. Melakukan *AddRoundKey* kembali dengan menggunakan *SubKey* hasil dari penjadwalan kunci *CipherKey*.

$$\begin{bmatrix} 07 & 66 & 72 & 54 \\ 18 & 85 & 47 & 7a \\ a2 & ed & d3 & a3 \\ 17 & 8e & 15 & ca \end{bmatrix} \oplus \begin{bmatrix} 6f & 2a & 63 & 2e \\ c6 & 80 & ca & 84 \\ 10 & 57 & 2c & 53 \\ a7 & df & a3 & f3 \end{bmatrix}$$

$$= \begin{bmatrix} 68 & 4c & 11 & 7a \\ de & 05 & 8d & fe \\ b2 & ba & ff & f0 \\ b0 & 51 & b6 & 39 \end{bmatrix}$$

Semua operasi tersebut diulang sebanyak 10 iterasi hingga mendapatkan *ciphertext*. Untuk iterasi 1 sampai 9 dilakukan operasi *SubByte*, *ShiftRow*, *MixColumns*, dan *AddRoundKey*. Sedangkan untuk iterasi terakhir hanya dilakukan operasi *SubByte*, *ShiftRow*, dan *AddRoundKey*.

Proses dekripsi menggunakan algoritma AES merupakan kebalikan dari proses enkripsi. Operasi-operasi yang dilakukan yaitu *InvSubByte*, *InvShiftRow*, *InvMixColumn* dan *AddRoundKey*. Penjadwalan kunci pada proses dekripsi pada tiap *round* berkebalikan dengan proses enkripsi yaitu dimulai dari *SubKey* ke-10 sampai dengan *cipher key*.




Gambar 7 *Flowchart* proses dekripsi algoritma AES

Contoh dekripsi pada algoritma AES, jika diketahui kunci dan *ciphertext* yang akan digunakan untuk dekripsi dengan bentuk matriks 4x4 (blok 16 *byte*), yaitu:

$$Ciphertext = \begin{bmatrix} 08 & 44 & 55 & 42 \\ 5a & 5f & d2 & 91 \\ e1 & 5b & a8 & 58 \\ 8f & de & 68 & 51 \end{bmatrix}$$

$$Subkey\ ke\ 10 = \begin{bmatrix} b3 & 67 & 07 & 92 \\ d3 & d9 & 08 & 2a \\ ac & 56 & eb & 21 \\ 0d & ad & 9f & d9 \end{bmatrix}$$

Dengan solusi atau penyelesaian dengan tahap - tahap sebagai berikut:

A. Melakukan operasi *AddRoundKey* dengan melakukan operasi XOR pada setiap kolom di *ciphertext* dengan kolom di *subkey* ke-10

$$\begin{bmatrix} 08 & 44 & 55 & 42 \\ 5a & 5f & d2 & 91 \\ e1 & 5b & a8 & 58 \\ 8f & de & 68 & 51 \end{bmatrix} \oplus \begin{bmatrix} b3 & 67 & 07 & 92 \\ d3 & d9 & 08 & 2a \\ ac & 56 & eb & 21 \\ 0d & ad & 9f & d9 \end{bmatrix} = \begin{bmatrix} bb & 23 & 52 & d0 \\ 89 & 86 & da & bb \\ 4d & 0d & 43 & 79 \\ 82 & 73 & f7 & 88 \end{bmatrix}$$

B. Melakukan operasi *Invers ShiftRows*

$$\begin{bmatrix} bb & 23 & 52 & d0 \\ 89 & 86 & da & bb \\ 4d & 0d & 43 & 79 \\ 82 & 73 & f7 & 88 \end{bmatrix} \rightarrow \begin{bmatrix} bb & 23 & 52 & d0 \\ 86 & da & bb & 89 \\ 43 & 79 & 4d & 0d \\ 88 & 82 & 73 & f7 \end{bmatrix}$$

C. Melakukan operasi *Invers SubBytes*

Setelah itu masuk *round* ke-2 sampai *round* ke-10 yang terdiri dari operasi:

1. Operasi *AddRoundKey*. Melakukan operasi XOR pada *Invers SubBytes* dengan *SubKey* ke-9

$$\begin{bmatrix} fe & 32 & 48 & 60 \\ dc & 7a & fe & 90 \\ 64 & af & 65 & f3 \\ 97 & 11 & 8f & 26 \end{bmatrix} \oplus \begin{bmatrix} 21 & d4 & 60 & 95 \\ a7 & 0a & d1 & 22 \\ f8 & fa & bd & ca \\ 24 & a3 & 32 & 46 \end{bmatrix} = \begin{bmatrix} df & e6 & 28 & f5 \\ fb & 70 & 2f & b2 \\ 9c & 55 & d8 & 39 \\ b3 & b2 & bd & 60 \end{bmatrix}$$

2. Operasi *Invers MixColumns*

$$\begin{bmatrix} 0e & 0b & 0d & 09 \\ 09 & 0e & 0b & 0d \\ 0d & 09 & 0e & 0b \\ 0b & 0d & 09 & 0e \end{bmatrix} \times \begin{bmatrix} df & e6 & 28 & f5 \\ fb & 70 & 2f & b2 \\ 9c & 55 & d8 & 39 \\ b3 & b2 & bd & 60 \end{bmatrix}$$

- $0e * df$

$0e = 0000\,1110$

$= 0000\,1000 \oplus 0000\,0100 \oplus 0000\,0010$

$df = 1101\,1111$

Dijabarkan:

df ∗ 0001 = 1101 1111 ∗ 0000 0001
= 1101 1111
df ∗ 0010 = 1101 1111 ∗ 0000 0010
= 1
1011 1110 ⊕ 1 0001 1011
= 0010 0101
df ∗ 0100 = 1101 1111 ∗ 0000 0100
= 0100 1010
df ∗ 1000 = 1101 1111 ∗ 0000 1000
= 1001 0100
= 0001 0001
0e ∗ df = 1001 0100 ⊕ 0100 1010 ⊕
0010 0101
= 1111 1011

- 0b ∗ fb

0b = 0000 1011
= 0000 1000 ⊕ 0000 0010
⊕ 0000 0001
fb = 1111 1011
Dijabarkan:
fb ∗ 0001 = 1111 1011 ∗ 0000 0001
= 1111 1011
fb ∗ 0010 = 1111 1011 ∗ 0000 0010
= 1110 1101
fb ∗ 0100 = 1111 1011 ∗ 0000 0100
= 1100 0001
fb ∗ 1000 = 1111 1011 ∗ 0000 1000
= 1
1000 0010 ⊕ 1 0001 1011
= 1001 1001
0b ∗ fb
= 1001 1001 ⊕ 1110 1101
⊕ 1111 1011
= 1000 1111

- 0d ∗ 9c

0d = 0000 1101 = 0000 1000 ⊕
0000 0100 ⊕ 0000 0001
9*c* = 1001 1100
Dijabarkan:
9c ∗ 0001 = 1001 1100 ∗ 0000 0001
= 1001 1100
9c ∗ 0010 = 1001 1100 ∗ 0000 0010
= 0010 0011
9c ∗ 0100 = 1001 1100 ∗ 0000 0100
= 0100 0110
9c ∗ 1000 = 1001 1100 ∗ 0000 1000
= 1000 1100
0d ∗ 9c = 1000 1100 ⊕ 0100 0110
⊕ 1001 1100
= 0101 0110

- 09 ∗ b3

09 = 0000 1001
= 0000 1000 ⊕ 0000 0001
b3 = 1011 0011
Dijabarkan:
b3 ∗ 0001 = 1011 0011 ∗ 0000 0001
= 1011 0011
b3 ∗ 0010 = 1011 0011 ∗ 0000 0010
= 0111 1101
b3 ∗ 0100 = 1011 0011 ∗ 0000 0100
= 1111 1010
b3 ∗ 1000 = 1011 0011 ∗ 0000 1000
= 1110 1111
09 ∗ 3b = 1110 1111 ⊕ 1011 0011
= 1101 1100
1111 1011 ⊕ 1000 1111 ⊕ 0101 0110
⊕ 1101 1100
= 1111 1110 = fe

Setelah melakukan perkalian matriks tiap baris dan kolom, diperoleh:

$$\begin{bmatrix} fe & 5f & 20 & 88 \\ 6b & 0b & fb & 34 \\ 98 & 0e & a0 & 78 \\ b5 & 2f & 06 & da \end{bmatrix}$$

3. Operasi *Invers ShiftRows*

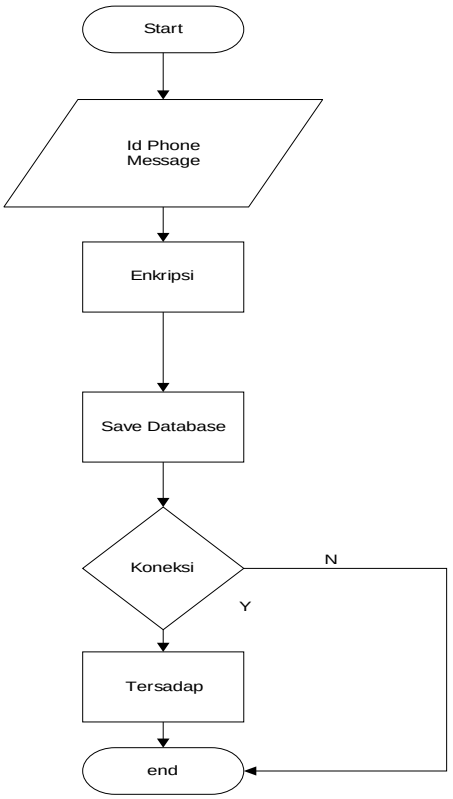
$$\begin{bmatrix} fe & 5f & 20 & 88 \\ 6b & 0b & fb & 34 \\ 98 & 0e & a0 & 78 \\ b5 & 2f & 06 & da \end{bmatrix} \rightarrow \begin{bmatrix} fe & 5f & 20 & 88 \\ 34 & 6b & 0b & fb \\ a0 & 78 & 98 & 0e \\ 2f & 06 & da & b5 \end{bmatrix}$$

4. Operasi *Invers SubBytes*

$$\begin{bmatrix} fe & 5f & 20 & 88 \\ 34 & 6b & 0b & fb \\ a0 & 78 & 98 & 0e \\ 2f & 06 & da & b5 \end{bmatrix} \rightarrow \begin{bmatrix} 0c & 84 & 54 & 97 \\ 28 & 05 & 9e & 63 \\ 47 & c1 & e2 & d7 \\ 4e & a5 & 7a & d2 \end{bmatrix}$$

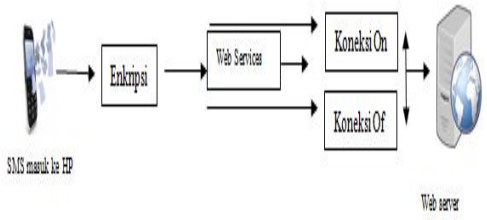
Semua operasi tersebut diulang sebanyak 10 iterasi hingga mendapatkan *plaintext*. Untuk iterasi 1 dilakukan operasi *AddRoundKey*, *Invers ShiftRows*, dan *Invers SubBytes*. Sedangkan untuk iterasi 2 sampai 10 dilakukan operasi *AddRoundKey*, *Invers MixColumns*, *Invers ShiftRows*, dan *Invers SubBytes*.

Gambar 8 menunjukkan *flowchart* penyadapan SMS. Prosesnya dimulai dengan masuk dan keluarnya SMS pada *handphone* pihak tersadap yang akan dienkripsi terlebih dahulu, kemudian dikirim pada *web server* yang keluarannya berupa SMS dalam bentuk *plaintext*. Penyadapan SMS terjadi pada *handphone* android menuju ke *web server* karena dihubungkan melalui *web service*.




Gambar 8 *Flowchart* penyadapan SMS

Gambar 9 menjelaskan tentang fungsi *web service*.




Gambar 9 Fungsi *web service*

## 4. KESIMPULAN

Kesimpulan yang dapat diambil dari penulisan tugas akhir ini adalah :

1. Pembangunan aplikasi penyadapan SMS dan GPS dengan memanfaatkan *database* HP sebagai penyimpanan sementara, setelah itu akan ditransfer ke *web server* jika paket data HP yang telah diinstal *software* penyadapan dalam keadaan ON.
2. Aktivitas dapat diketahui dengan membaca kiriman SMS dan lokasi GPS pihak tersadap yang terdapat dalam *web server* yang telah dikirm oleh *web service*. *Google maps* akan menemukan posisi GPS pihak tersadap dengan menentukan posisi *latitude* dan *longitude* sehingga *google maps* akan menampilkan lokasi GPS pihak tersadap dalam bentuk *maps* sesuai dengan *database google maps* .
3. Aplikasi penyadapan SMS dan GPS ini menerapkan algoritma AES pada 2 (dua) bahasa pemrograman yaitu java dan PHP dengan menggunakan modul atau *library* bahasa pemrograman PHP dan java yang telah disediakan sehingga memudahkan penerapan Algoritma AES pada sistem.
4. Aplikasi penyadapan SMS dan GPS dapat berjalan pada sistem operasi Android versi 4.1 ke atas tanpa dipengaruhi oleh kapasitas RAM dan kecepatan *prossesor* serta kesesuaian lokasi GPS pihak tersadap sesuai dengan *database Google maps.* SMS yang masuk pada *web server* mengikuti waktu yang sebenarnya tanpa dipengaruhi oleh waktu HP pihak tersadap.
5. kesesuaian lokasi GPS pihak tersadap sesuai dengan *database Google maps.* SMS yang masuk pada *web server* mengikuti waktu yang sebenarnya tanpa dipengaruhi oleh waktu HP pihak tersadap.

## 5. SARAN

Agar memperoleh hasil yang lebih baik kedepannya untuk aplikasi penyadapan SMS berbasis *android*, maka penulis memberikan saran sebagai berikut :

1. Pengembangan metode AES tanpa memanfaatkan *library* JCE (*Java Cryptography Extension*).
2. Untuk penelitian selanjutnya pengembangan Aplikasi Penyadapan SMS dan GPS dapat dikembangkan menjadi penyadapan berupa *file digital* lainnya seperti *audio* dan *video*, serta dapat menyiapkan *software notification* pada *handphone* pihak tersadap sehingga *user* tidak perlu mengakses *web server*.

DAFTAR PUSTAKA

[1] Herwingoernial, 2013, *Kriptografi* Metode Algoritma AES. *http://herwingoernia19.blogspot.com/2013/12/kriptografi-metode-algoritma-aes.html,* diakses 5 Januari 2015

[2] Muchlisin, R., 2012, Pengertian dan sejarah SMS, *http://www.kajian pustaka.com/2012/12/teori-sms-short-message-service.* html, diakses 26 September 2014.

[3] Habi, 2007, *Global Positioning System. http://habi3.blogspot.com/2007/05/global-positioning-system-gps.html,* diakses 26 September 2014.

[4] Karim, I, 2014, Enkripsi dan Dekripsi Layanan SMS untuk Pengamanan Data Transaksi Bisnis Menggunakan Algoritma Rijndael Berbasis Multi Operating System, *Skripsi*, Fakultas Teknik, Jurusan Informatika, Universitas Halu Oleo.

[5] Lee, W. M., 2011, *Beginning Android Application Development*, Indianapolis: Wiley Publishing