ALGORITMA RSA UNTUK PENGAMANAN DATA LOKASI PADA API BERBASIS RESTFUL WEB SERVICE

Akbar Maulana Putra[1], Painem[2]
Teknik Informatika Fakultas Teknologi Informasi, Universitas Budi Luhur
[1, 2]Jl. Raya Ciledug, Petukangan Utara, Kebayoran Lama, Jakarta Selatan 12260
Telp. (021) 5853753, Fax. (021) 5853752
E-mail : [1]putraakbarmaulana@gmail.com, [2]painem@budiluhur.ac.id

ABSTRAK

Pada era digital saat ini, alat komunikasi menjadi kebutuhan umum. Penggunaan smartphone adalah alat informasi yang paling populer digunakan di Indonesia pada saat ini. Negara di Asia Tenggara, yaitu Indonesia tercatat sebagi negara yang warganya terbanyak menggunakan Android dengan total pengguna sekitar 41 juta orang atau 94%. Smartphone digunakan untuk berbagai kegiatan, salah satunya untuk mempermudah pengguna dalam melakukan aktifitas sehari-hari dengan memanfaatkan aplikasi yang ada pada alat komunikasi tersebut. Namun, masih banyak kegiatan masyarakat yang masih dilakukan secara manual, dimana seharusnya kegiatan tersebut bisa dipermudah dengan membuat suatu sistem yang dapat digunakan dengan smartphone. Di Unversitas Budi Luhur masih terdapat kegiatan yang dilakukan secara manual diamana seharusnya kegiatan tersebut bisa dipermudah dengan aplikasi, kegitan tersebut adalah pemesanan fasilitas mobil kampus. Maka aplikasi transportasi online menjadi salah satu jalan keluar dari masalah ini, sehingga pembuatan aplikasi ini dapat menghemat waktu dan mempermudah proses pemesanan fasilitas tranportasi tersebut. Tujuan aplikasi ini yaitu untuk mempermudah dan mempersingkat proses pemesan mobil dan menjaga lokasi pemesan dari gangguan pihak yang tidak bertanggung jawab. Untuk menjaga lokasi pemesan maka digunakan metodologi kriptografi dengan menggunakan Algoritma RSA. Aplikasi dibangun berbasis RESTful dengan menggunakan bahasa PHP dan web server dimana tampilan akan diproses oleh Android. Proses berjalannya aplikasi yaitu diawali dengan dosen melakukan pesanan, lalu diterima atau ditolak pesanan tersebut oleh bos driver, dan terakhir proses pengantaran dosen oleh driver. Dengan penerapan metode Kriptografi RSA maka diharapkan bisa meminimalisir kemungkinan terjadinya pencurian bahkan jika terjadi pencurian data maka akan membutuhkan waktu untuk memecahkan cipher teks dari metode Kriptografi RSA. Berdasarkan hasil pengujian proses enkripsi dan dekripsi dapat dilakukan dengan baik, sehingga lokasi pengguna dapat diamankan.

Kata Kunci : RSA, RESTful, API, Web Service, BluDrive

1. PENDAHULUAN

1.1 Latar Belakang

Pada era digital saat ini, alat komunikasi menjadi kebutuhan umum. Penggunaan smartphone adalah alat informasi yang paling populer digunakan di Indonesia pada saat ini. Negara di Asia Tenggara, yaitu Indonesia tercatat sebagi negara yang warganya terbanyak menggunakan Android dengan total pengguna sekitar 41 juta orang atau 94% dan sisanya yaitu sekitar 2,8 juta orang menggunakan iOS (Rachman, 2015). *Smartphone* digunakan untuk berbagai kegiatan, salah satunya untuk mempermudah pengguna dalam melakukan aktifitas sehari-hari dengan memanfaatkan aplikasi yang ada pada alat komunikasi tersebut. Namun, masih banyak kegiatan masyarakat yang masih dilakukan secara manual, dimana seharusnya kegiatan tersebut bisa dipermudah dengan membuat suatu sistem yang dapat digunakan dengan *smartphone*.

Universitas Budi Luhur adalah salah satu univeristas swasta di Jakarta yang telah berdiri sejak 1 April 1979. Di Universitas Budi Luhur beberapa dosen sering menggunakan fasilitas transportasi yang disediakan oleh pihak Universitas. Namun, proses penggunaan fasilitas transportasi ini masih dilakukan secara manual diamana dosen yang ingin menggunakan fasilitas transportasi tersebut harus memesan terlebih dahulu melalui staff yang bertugas dibagian transportasi.

Aplikasi transportasi online menjadi salah satu dampak positif yang muncul dari perkembangan teknologi informasi dan komunikasi seperti saat ini. Transpotasi merupakan kebutuhan sehari-hari bagi masyarakat yang memliki *mobilitas* yang tinggi, tidak terkecuali bagi dosen Universitas Budi Luhur. Sehingga pembuatan aplikasi untuk penggunaan fasilitas tranpostasi Universitas Budi Luhur perlu dilakukan, agar menghemat waktu dan mempermudah proses pemesanan fasilitas tranportasi tersebut. Dalam pembuatan aplikasi tersebut juga perlu diperhatikan keaman informasi lokasi penjemputan dan lokasi tujuan yang dipesan oleh dosen, agar informasi lokasi yang dipesan tidak dapat dicuri informasinya oleh orang lain, dan untuk mengamankan

informasi tersebut bisa menggunakan salah satu teknik krtiptografi.

Kriptografi merupakan suatu ilmu yang digunakan untuk mengamankan infromasi. Karena itu, diperlukan sebuah teknik kriptografi yang mana pada apliakasi pemesanan fasilitas transportasi Univeritas Budi Luhur ini menggunakan metode RSA. Dengan menggunakan kriptografi RSA, diharapkan inforamasi lokasi yang dipesan dapat melindungi dan meminimalisir terjadinya pencurian data dari pihak yang tidak bertanggung jawab.

1.2 Tujuan Penelitian

Membuat aplikasi transportasi online untuk mempermudah dosen yang ingin menggunakan fasilitas transportasi yang ada di Univeritas Budi Luhur, dan aplikasi dapat digunakan oleh dosen, bos *driver* dan *driver*, sehingga mempermudah proses pemesanan hingga pengantaran dosen menuju kelokasi tujuan, serta mengamankan informasi lokasi penjemputan dan lokasi tujuan agar tidak disalahgunakan oleh pihak lain dengan metode pengamanan algoritma RSA dimana aplikasi tersebut diterapkan dalam RESTful web service.

1.3 Batasan Masalah

Batasan masalah yang dibut untuk membatasi permasalahan yang akan diselesaikan. Berikut batasan masalahnya :

a. Algoritma kriptografi yang digunakan untuk pengamanan infromasi lokasi adalah Algoritma RSA.
b. Aplikas ini dibuat dengan Metode RESTful *web service*, dimana data akan ditampilkan pada *platform* lain, dalam kasus ini *platform android*.
c. Sistem menggunakan bahasa pemrograman *PHP* dan sistem manajemen basis data *MySQL*.
d. *Tools* yang digunakan sebagai testing RESTful *web service* adalah POSTMAN.
e. Aplikasi dapat digunakan oleh dosen untuk memesan mobil, bos *driver* untuk meneruskan pesanan kepada *driver*, dan *driver* untuk menerima pesanan dari dosen yang telah diteruskan oleh bos *driver*.

2. STUDI LITERATUR

Kriptografi merupakan teknik pengamanan informasi yang dilakukan dengan cara mengolah informasi awal (*plaintext*) dengan suatu kunci (*key)* menggunakan metode enkripsi yang ditentukan sehingga menghasilkan suatu informasi baru (*ciphertext*) yang tidak dapat dimengerti secara langsung [3]. Keamanan dari suatu kriptografi terletak pada kerahasiaan kunci sedangkan algoritma kriptografi diasumsikan diketahui oleh umum. Sistem kriptografi yang kuat memiliki kemungkinan jangkauan kunci yang sangat besar sehingga sistem tidak dapat dipecahkan secara mudah dengan mencoba semua kemungkinan kunci yang ada (*brute force),* sistem kriptografi yang kuat juga menciptakan *ciphertext* yang acak sehingga mempersulit pihak ketiga untuk mengetahui isi informasi [5]. RSA merupakan salah satu algoritma kriptografi kunci publik. Algoritma ini merupakan algoritma pertama yang cocok untuk melakukan tanda tangan digital dan merupakan algoritma yang paling sering dugunakan [2]. Algoritma RSA terbagi menjadi tiga proses, yaitu pembangkitan kunci, enkripsi dan dekripsi. Dasar proses enkripsi dan dekripsi pada algoritma RSA yaitu konsep bilangan prima dan aritmatika modulo. Kunci enkrpsi tidak dirahasiakan dan diberikan kepada umum, sedangkan kunci untuk dekripsi bersifat rahasia [1]. REST merupakan s*tyle* protokol *web service* yang berdasarkan pada prinsip yang menjelaskan bagaimana sumber-sumber jaringan yang terhubung didefinisikan dan dialamatkan. RESTful merupakan repersentasi ketersediaan setiap teknologi dan setiap gaya pengembangan aplikasi tanpa adanya batasan [4].

3. METODOLOGI PENELITIAN

3.1 Analisa Masalah

Pada era digital saat ini penggunaan teknologi sudah semakin berkembang ke seluruh aspek kehidupan, termasuk untuk mempermudah seseorang dalam beraktifitas sehari-hari. Di Universitas Budi Luhur masih terdapat beberapa kegitan yang dilakukan secara manual, dimana dengan pesatnya perkembangan teknologi seharusnya kegiatan tersebut dapat dipermudah dengan bantuan teknologi. Kegiatan tersebut salah satunya adalah proses peminjaman fasilitas transportasi Universitas Budi Luhur oleh dosen. Prosedur yang digunakan saat ini untuk meminjam fasilitas tranportasi kampus yaitu dosen harus memesan terlebih dahulu melalui staff yang bertugas dibagian transportasi. Namun, terkadang dosen memiliki jadawal yang padat, sehingga untuk memesan failitas transportasi melalui staff yang berada pada bagian transportasi sulit untuk dilakukan.

Masalah lain yang akan timbul ketika sistem telah dibuat terhadap masalah diatas yaitu tentang keaman informasi lokasi penjemputan dan lokasi tujuan. Karena jika ada pihak yang tidak bertanggung jawab, maka meraka akan memanfaatkan informasi tersbut untuk hal-hal yang dapat merugikan pemesan (dosen). Oleh

karena itu diperlukan suatu metode pengamanan terhadap informasi lokasi tersebut.

3.2 Penyelesaian Masalah

Dari permasalahan yang telah diuraikan diatas, maka dibutuhkan suatu aplikasi pemesanan transportasi Universitas Budi Luhur untuk mempermudah dosen dalam melakukan pemesanan tanpa harus mendatangi bagian staff yang berada pada bagian transportasi, sehingga meningkatkan efisiensi dan efektifias. Aplikasi tersebut nantinya hanya dapat digunakan oleh pihak Universitas Budi Luhur, yaitu Dosen, Bos *Driver* dan *Driver*.

Untuk mengatasi masalah keamanan informasi lokasi pengguna ketika sistem sudah dibuat, maka digunakan metode kriptografi untuk mengamankannya. Metode kriptografi yang digunakan adalah algortima RSA. Dengan digunakannya Algoritma RSA ini diharapkan informasi lokasi dapat terjaga dan meminimalisir terjadinya pencurian informasi dari luar.

3.3 Rancangan Layanan Web Service

Rancangan ini berisi berbagai layanan yang akan digunakan pada sistem bludrive, serta penjelasan dari masing-masing layanan seperti pengguna, nama layanan, fungsi, *route*, parameter dan keluaran yang akan diuraikan pada tabel berikut:

Table 1. Rancangan Route Web Service

Pengguna	Nama Layanan	Fungsi	Route	Parameter	Keluaran
User	Login	Post	/auth/signin	Parameter yang dibutuhkan : username, password, token	True or False
Dosen	Dosen melakukan pesanan	Post	/drive/user/pesan	Parameter yang dibutuhkan : id_mobil, posisi, posisi_tujuan, tanggal_pesanan, waktu_pemesanan, keterangan_user	True or False dan mengirim email
Dosen	Menampilkan semua pesanan dosen bersangkutan yang pesannya belum diterima atau ditolak oleh bos *driver*	Get	/drive/user/pesan		id, id_user, id_mobil, email, posisi, posisi_tujuan, latitude_jemput, longitude_jemput, latitude_tujuan, longitude_jemput, tanggal_pemesanan, waktu_pemesanan, status, keterangan_user, keterangan_driver, created_at, updated_at
Dosen	Menampilkan detail pesanan dosen bersangkutan	Get	/drive/user/pesan/{pesan}	Parameter untuk {pesan} adalah id	id, id_user, id_mobil, email, posisi, posisi_tujuan, latitude_jemput, longitude_jemput, latitude_tujuan, longitude_jemput, tanggal_pemesanan, waktu_pemesanan, status, keterangan_user, keterangan_driver, created_at, updated_at
Dosen	Menampilkan semua riwayat pesanan dosen bersangkutan yang sudah diantar	Get	/drive/user/order/riwayat		id, id_user, id_mobil, id_driver, email, posisi, posisi_tujuan, latitude_jemput, longitude_jemput, latitude_tujuan, longitude_jemput, tanggal_pemesanan, waktu_pemesanan, status, keterangan_user, keterangan_driver, created_at, updated_at
Dosen	Menampilkan detail riwayat pesanan dosen yang sudah diantar	Get	/drive/user/order/{order}	Parameter untuk {order} adalah id	id, id_user, id_mobil, id_driver, email, posisi, posisi_tujuan, latitude_jemput, longitude_jemput, latitude_tuj

					uan, longitude_jemput, tanggal_pemesanan, waktu_pemesanan, status, keterangan_user, keterangan_driver, created_at, updated_at
Bos *Driver*	Menampilkan pesanan semua dosen yang pesannya belum diterima atau ditolak oleh bos *driver*	Get	/drive/bos/pesan		id, id_user, id_mobil, id_driver, email, posisi, posisi_tujuan, latitude_jemput, longitude_jemput, latitude_tujuan, longitude_jemput, tanggal_pemesanan, waktu_pemesanan, status, keterangan_user, keterangan_driver, created_at, updated_at
Bos *Driver*	Menampilkan detail pesanan dosen yang pesannya belum diterima atau ditolak oleh bos *driver*	Get	/drive/bos/pesan/{pesan}	Parameter untuk {pesan} adalah id	id, id_user, id_mobil, id_driver, email, posisi, posisi_tujuan, latitude_jemput, longitude_jemput, latitude_tujuan, longitude_jemput, tanggal_pemesanan, waktu_pemesanan, status, keterangan_user, keterangan_driver, created_at, updated_at
Bos *Driver*	Menolak atau menerima pesanan dosen	Patch	/drive/bos/pesan/{pesan}	Parameter untuk {pesan} adalah id dan parameter lain yang dibutuhkan :status,	True or false dan mengirim email

				id_driver, keterangan_drive	
Bos *Driver*	Menampilkan pesanan semua dosen yang sudah diantar	Get	/drive/bos/order		id, id_user, id_mobil, id_driver, email, posisi, posisi_tujuan, latitude_jemput, longitude_jemput, latitude_tujuan, longitude_jemput, tanggal_pemesanan, waktu_pemesanan, status, keterangan_user, keterangan_driver, created_at, updated_at
Driver	Menampilkan semua pesanan dosen yang belum diantar oleh driver bersangkutan	Get	/drive/driver/order		id, id_user, id_mobil, id_driver, email, posisi, posisi_tujuan, latitude_jemput, longitude_jemput, latitude_tujuan, longitude_jemput, tanggal_pemesanan, waktu_pemesanan, status, keterangan_user, keterangan_driver, created_at, updated_at
Driver	Menampilkan semua riwayat pesanan dosen yang sudah diantar oleh driver bersangkutan	Get	/drive/driver/order/riwayat		id, id_user, id_mobil, id_driver, email, posisi, posisi_tujuan, latitude_jemput, longitude_jemput, latitude_tujuan, longitude_jemput, tanggal_pemesanan, waktu_pemesanan, status,

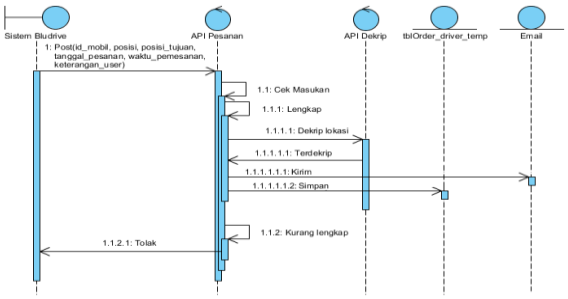
					keterangan_user, keterangan_driver, created_at, updated_at
Driver	Menampilkan detail pesanan dosen yang belum diantar	Get	/drive/driver/order/{order}	Parameter untuk {order} adalah id	id, id_user, id_mobil, id_driver, email, posisi, posisi_tujuan, latitude_jemput, longitude_jemput, latitude_tujuan, longitude_jemput, tanggal_pemesanan, waktu_pemesanan, status, keterangan_user, keterangan_driver, created_at, updated_at
Driver	Sudah mengantarkan dosen	Patch	/drive/driver/order/{order}	Parameter untuk {pesan} adalah id dan parameter lain yang dibutuhkan :status, keterangan	True or false dan mengirim email

3.4 Sequence Diagram

Di dalam menggambarkan urutan alur kerja dari setiap API, digunakan *sequence diagram*. Di bawah ini akan digambarkan *sequence diagram* berdasarkan setiap *route* API dari tabel diatas, sebagai berikut :

a. *Sequence Diagram* Pemesanan

Sequence diagram ini menjelaskan bagaimana proses pemesanan oleh dosen. *Sequence diagram* digambarkan seperti gambar 1.



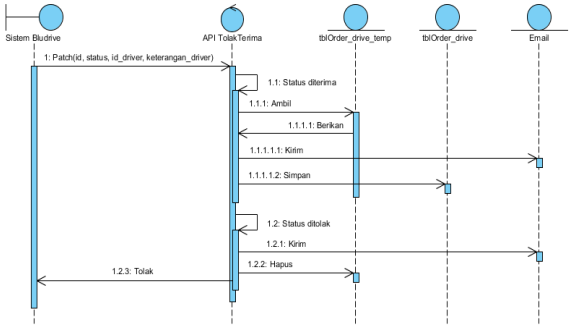
Gambar 1: Sequence diagram Pemesanan

Keterangan :

Dalam proses ini, dosen akan mengisikan sejumlah data yang diperlukan, lalu akan diperiksa apakah data yang dimasukan sudah lengkap atau tidak, jika data lengkap maka lokasi akan di dekrip dimana yang sebelumnya sudah di enkrip pada sistem *android*, jika belum lengkap maka proses pesanan ditolak oleh sistem. Setelah proses dekripsi selesai maka bos *driver* akan dikirimkan email dan data akan disimpan pada database.

b. *Sequence Diagram* Terima/Tolak Pesanan

Sequence diagram ini menjelaskan bagaimana proses pesanan diterima atau ditolak oleh bos *driver*. *Sequence diagram* digambarkan seperti gambar 2.



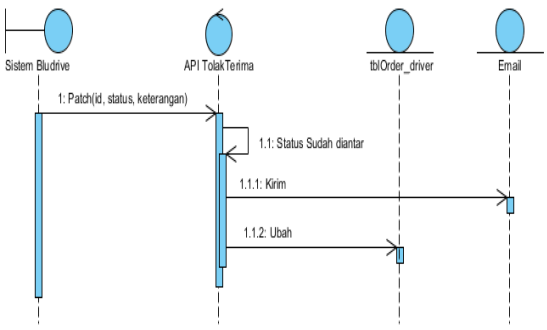
Gambar 2: Sequence Diagram Terima/Tolak Pesanan

Keterangan :

Dalam proses ini, bos *driver* akan menentukan apakah pesanan akan diterima atau ditolak. Jika pesanan diterima maka pesanan akan diteruskan menjadi orderan dan akan terkirim email menuju *driver* dan dosen bersangkuatan, namun jika ditolak maka pesanan akan dihapus dari database.

c. *Sequence Diagram* Pesanan Sudah Diantar

Sequence diagram ini menjelaskan bagaimana proses pesanan yang sudah diantar oleh *driver*. *Sequence diagram* digambarkan seperti gambar 3.



Gambar 3: Sequence Diagram Pesanan Sudah Diantar

Keterangan :

Dalam proses ini, *driver* yang sudah mengantarkan dosen akan mengupdate status bahwa pesanan sudah diantarkan. Lalu akan dikrimkan email kepada bos driver bahwa pesanan sudah diantarkan dan tabel orderan akan diupdate statusnya.

3.5 Enkripsi dan Dekripsi RSA

Proses enkripsi dan dekripsi untuk *plaintexs* blok M dan *ciphertext* blok C pada algoritma RSA dapat digambarkan sebagai berikut :

$C = M^e \bmod n$

$M = C^d \bmod n$

Secara lengkap, langkah-langkah yang dilakukan di dalam algoritma RSA adalah sebagai berikut :

a) Pilih dua bilangan prima secara acak untuk nilai p dan q, dimana nilai p>q.
b) Cari n = pq.
c) Hitung Φ(n) = (p-1)(q-1).
d) Pilih kunci publik e secara acak dengan syarat e>1, sehingga nilai e adalah bilangan prima dari GCD(e, Φ(n)) = 1, yang didapat dengan menggunakan algoritma euclidean.
e) Pilih kunci *private* d secara acak dengan syarat (d.e) mod Φ(n) = 1.
f) Untuk mengenkripsi *plaintext* M, 0≤M≤n-1, dilakukan perhitungan C= M^e(mod n).
g) Untuk mendekripsi ciphertext dilakukan perhitungan M = C^d(mod n).

Untuk mengetahui dengan lebih jelas proses kerja algoritma RSA ini, maka diterapkan langkah-langkah berikut sebagai contoh:

a) Pilih dua bilangan prima p=53 dan q=61.
b) Cari n = pq = 53 x 61 = 3233.
c) Hitung Φ(n) = (p-1)(q-1) = (53-1)(61-1) = 52 x 60 = 3120.
d) Dapatkan kunci publik e, dimana e adalah bilangan prima, misalkan nilai e yang akan diambil adalah 17, maka dilakukan pengecakan dengan rumus berikut :
GCD(e, Φ(n)) = 1
3120 mod 17 = 9
17 mod 9 = 8
9 mod 8 = 1
8 mod 1 = 0
GCD(17, 3120) = 1
Maka e=17 telah memenuhi syarat, karena GCD(e, Φ(n)) = 1.
e) Dapatkan kunci *private* d, misalkan nilai d yang akan diambil adalah 2753, maka dilakukan pengecakan dengan rumus berikut :
(d.e) mod Φ(n) = 1
(2753 x 17) mod 3120 = 1
= 46801 mod 3120
= 1
Maka d=2753 telah memenuhi syarat, karena (d.e) mod Φ(n) = 1.
f) *Plaintext* M = 12, dengan syarat 0≤M≤n-1, maka enkripsi *Plaintext* M :
C = M^e(mod n) = 12^{17} mod 3233
C = 1730

g) Dekripsi *ciphertext* C dengan rumus :
M = C^d(mod n) = 1730^{2753} mod 3233
M = 12

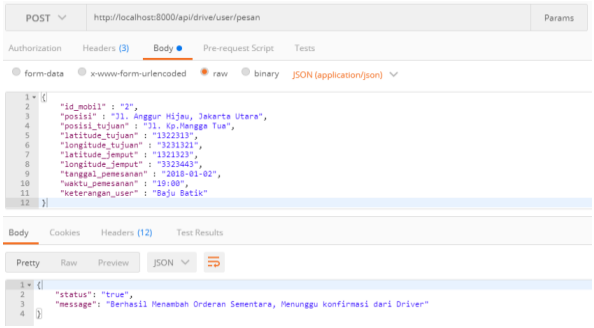
4. HASIL DAN PEMBAHASAN

4.1 Implementasi Tampilan

Tampilan akan ditampilkan dengan menggunakan *tools* tambahan, yaitu *postman*.

a. Tampilan Pesanan

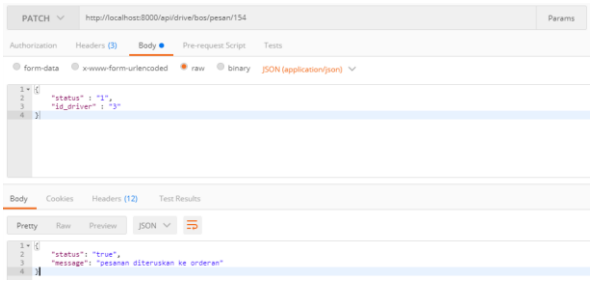
Tampilan pesanan merupakan tampilan yang akan diisi oleh dosen untuk melakukan pesanan seperti Gambar 4 berikut.



Gambar 4: Tampilan Pesanan

b. Tampilan Terima/Tolak Pesanan

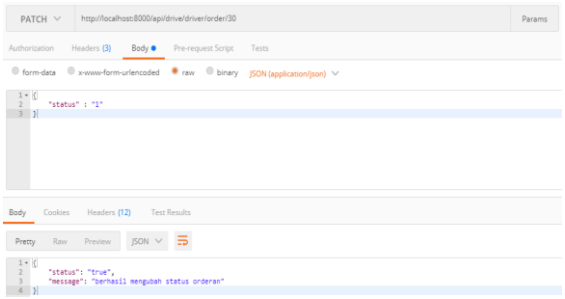
Tampilan Terima/Tolak pesanan merupakan tampilan yang akan diisi oleh bos *driver* untuk melakukan pesanan seperti gambar 5 berikut.



Gambar 5: Tampilan Terima/Tolak Pesanan

c. Tampilan Pesanan Sudah Diantar

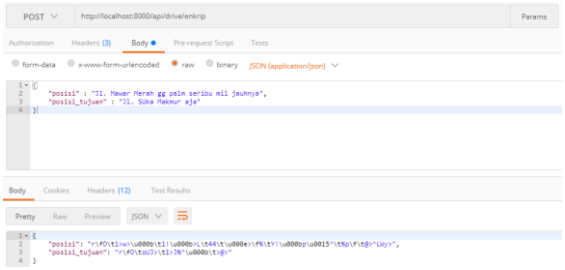
Tampilan Pesanan Sudah Diantar pesanan merupakan tampilan yang akan diisi oleh *driver* untuk melakukan pesanan seperti gambar 6 berikut.



Gambar 6: Tampilan Pesanan Sudah Diantar

d. Tampilan Enkripsi

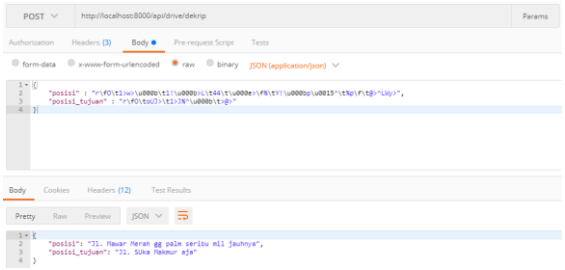
Tampilan ini merupakan tampilan hasil enkripsi data lokasi seperti gambar 7 berikut.



Gambar 7: Tampilan Enkripsi

e. Tampilan Dekripsi

Tampilan ini merupakan tampilan hasil enkripsi data lokasi seperti gambar 8 berikut.



Gambar 8: Tampilan Dekripsi

4.2 Hasil Uji Coba Program

Pada tabel dibawah ini adalah hasil pengujian dari enkripsi dan dekripsi dengan data registrasi untuk 10 user pada aplikasi BluDrive dengan iterasi 10 kali menggunakan *tools RestFull Stress*.

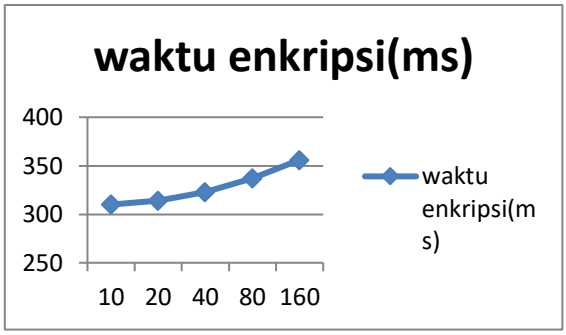
Tabel 2 menunjukan hasil rata-rata pengujian enkripsi dan dekripsi vernam des dengan parameter pengujian Encryption Time(ET), Decryption Time(DT) dan waktu tanpa enkripsi

Table 2. Pengujian Enkrip Dan Dekrip

No	karakter	Ukuran data sebelum dienkrip	Ukuran data setelah dienkrip	ET(ms)	RE(%)	DT(ms)	Waktu tanpa enkripsi(ms)
1	10	88 bytes	188 bytes	310	43,98	217	190
2	20	148 bytes	228 bytes	314	43,34	234	212
3	40	198 bytes	273 bytes	323	42,75	273	231
4	80	228 bytes	355 bytes	337	41,22	295	269
5	160	268 bytes	427 bytes	356	40,19	323	294

a. Grafik Waktu Enkripsi

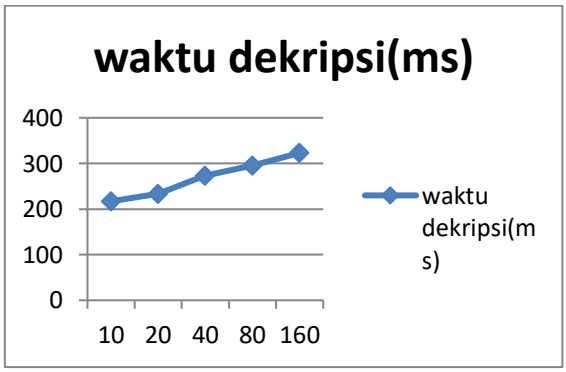
Berikut ini merupakan grafik waktu enkripsi yang diperlukan sistem untuk mengenkrip data.



Gambar 9: Grafik Waktu Enkripsi

b. Grafik Waktu Dekripsi

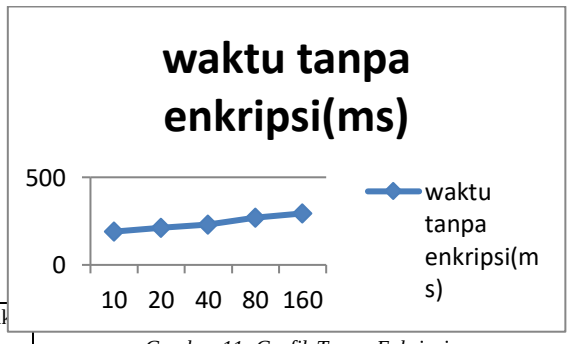
Berikut ini merupakan grafik waktu dekripsi yang diperlukan sistem untuk mendekrip data.



Gambar 10: Grafik Waktu Enkripsi

c. Grafik Tanpa Enkripsi

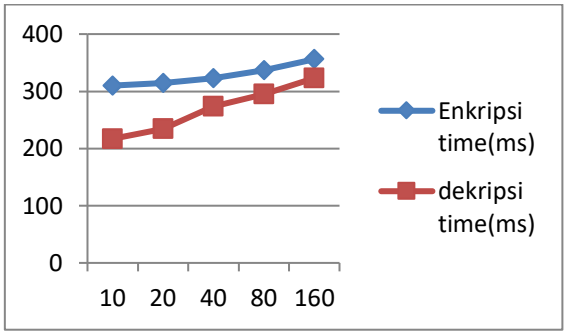
Berikut ini merupakan grafik hasil waktu yang dibutuhkan sistem tanpa enkripsi.



Gambar 11: Grafik Tanpa Enkripsi

d. Grafik Perbandingan Waktu Dengan Enkripsi Dan Tanpa Enkripsi

Berikut ini merupakan grafik waktu perbandingan dengan enkripsi dan tanpa enkripsi yang dibutuhkan sistem.



Gambar 12: Grafik Perbandingan Waktu Dengan Enkripsi Dan Tanpa Enkripsi

4.3 Evaluasi Program

Berdasarkan pengujian dan analisa program yang telah dilakukan diatas, maka dapat diketahui kelebihan dan kekurangan dari aplikasi ini, yaitu:

a. Kelebihan Program
   1) Membantu mempermudah dosen untuk melakukan pemesanan fasilitas transportasi kampus.
   2) Aplikasi mudah digunakan dan dipahami oleh user.
   3) Data yang sudah dienkrip dapat didekrip kembali menjadi data asli.

5. PENUTUP

5.1 Kesimpulan

Berdasarkan perancangan, pembuatan, serangkaian uji coba dan analisa program dari aplikasi ini, maka dapat diambil beberapa kesimpulan antara lain:

a. Penggunaan RESTful sebagai media pertukaran data untuk aplikasi ini sangat membantu.
b. Memudahkan dosen untuk melakukan pemesan fasilitas mobil kampus.
c. Navigasi pada aplikasi *driver* membantu memepermudah *driver* untuk mengantarkan dosen.
d. *Route* API yang disediakan belum digunakan semua.

5.2 Saran

Adapun saran yang mungkin diperlukan untuk membuat aplikasi ini dapat berjalan lebih baik lagi antara lain :

a. Aplikasi ini diharapkan dapat dikembangkan untuk melakukan pemesanan fasilitas lain di kampus.
b. Diharapkan data yang dienkrip tidak hanya data lokasi saja.
c. Diharapkan *route* yang disediakan dapat digunakan semua.

DAFTAR PUSTAKA

[1] Arifin, Zainal, 2009. Studi Kasus Penggunaan Algoritma RSA Sebagai Algoritma Kriptografi yang Aman. *Jurnal Informatika Mulawarman*.

[2] Devha, Chandra P., 2013. Pengamanan Pesan Rahasia Menggunakan Algoritma Kriptografi Rivest Shank Adlemen (RSA). *Jurnal Informatika*.

[3] Kurniawan, A., Yuliana, M. dan Hadi, M.Z.S, 2013. Analisa Dan Implementasi Sistem Keamanan Data Dengan Menggunakan Metode Enkripsi Algoritma Rc-5. *Jurnal Informatika*.

[4] Rumiyati R., Hendry, dan Tanone R., 2013. Pemanfaatan Teknologi Web REST Service pada Perancangan Portal Artikel Ilmiah Berbasis Android. *Jurnal Ilmiah*.

[5] Siregar, Syahrial R. 2010. Pengamanan Basis Data Keuangan RSUD Bangkinang Menggunakan Algoritma Kriptografi RC-6. *Tugas Akhir*.