ALGORITMA ENKRIPSI RC4 (*RIVEST CODE* 4) PADA APLIKASI CATATAN TEKS ANDROID PADA PT INTERNUSA FOOD

Berliana Putri Natalia[1)], **Ferdiansyah**[2)]
[1]Teknik Informatika, Fakultas Teknologi Informasi, Universitas Budi Luhur
[1,2]Jl. Raya Ciledug, Petukangan Utara, Kebayoran Lama, Jakarta Selatan 12260
E-mail : bputrinatalia@gmail.com[1)], ferdiansyah@budiluhur.ac.id[2)]

Abstrak

Dalam perusahaan yang bergerak di bidang produksi makanan ringan seperti snack dan biskuit anak-anak keamanan dalam pencatatan data perusahaan menjadi sangat penting. Selama ini para pegawai menulis catatan yang berisi data perusahaan, kegiatan pegawai maupun catatan hasil meeting masih ditulis manual pada sebuah notepad atau sticky notes pada komputer, atau pada kertas notes yang di tempelkan pada sebuah komputer, atau bahkan pada buku tulis lalu disimpan pada tempat-tempat tertentu agar isi dari buku tersebut tidak dibaca oleh orang lain. Hal ini tentu merupakan peluang bagi orang-orang yang tidak berhak misalnya hacker untuk mengambil atau mengubah informasi pemilik data dengan membuka notepad atau bahkan kertas catatan yang berisi data atau informasi perusahaan tersebut terselip lalu hilang. Dengan demikian hal tersebut akan sangat merugikan bagi pemilik data dan perusahaan. Aplikasi Notes berbasis mobile merupakan salah satu solusi yang tepat untuk menjawab kesulitan yang dialami oleh pegawai oleh pegawai PT Internusa Food. Dimana dalam aplikasi notes ini proses penyimpanan data atau informasi dienkripsi atau diubah menjadi susunan tulisan yang acak dan saat membuka kembali notes tersebut akan didekripsi untuk menampilkan informasi aslinya dengan key yang sesuai yang diinputkan oleh user saat proses simpan. Aplikasi ini dirancang dengan menggunakan algoritma enkripsi Rivest Code 4 dan dibangun dengan bahasa pemograman Android dan database menggunakan MySQL. Dengan adanya aplikasi notes ini diharapkan dapat membantu kinerja pegawai dalam penyimpanan catatan berupa data atau informasi perusahaan secara aman dan flexible.

Kata kunci: *Key*, *Notes*, Algoritma RC4, Android

1. PENDAHULUAN

Kemajuan teknologi yang sangat cepat mendorong setiap instansi untuk tetap mengikuti perkembangan teknologi dan terus meningkatkan kemampuannya dalam mengelola data-data dan informasi yang lebih aman, akurat, dan efisien yang dibutuhkan suatu instansi. Pencatatan sebuah informasi saat ini juga tidak terlepas dari kecanggihan sebuah teknologi. Selama ini masih banyak perusahaan yang belum menggunakan secara maksimal teknologi yang ada, dimana sebenarnya teknologi ini sangat berguna bagi perusahaan untuk menunjang kinerja operasional baik perusahaan maupun pegawainya.

Sehingga perkembangan teknologi informasi berpengaruh besar pada banyaknya perubahan aktifitas manusia, tak terkecuali dalam hal menulis catatan. Selama ini pada PT Internusa Food, para pegawai menulis catatan yang berisi data perusahaan, kegiatan pegawai maupun catatan hasil *meeting* masih ditulis pada sebuah *notepad* atau *sticky notes* pada komputer, atau pada kertas *notes* yang di tempelkan pada sebuah komputer, atau bahkan pada buku tulis lalu disimpan pada tempat-tempat tertentu agar isi dari buku tersebut tidak dibaca oleh orang lain. Tentu hal ini merupakan peluang bagi orang-orang yang tidak berhak misalnya *hacker* untuk mengambil atau mengubah informasi pemilik data dengan membuka *notepad* atau bahkan kertas catatan yang berisi data atau informasi perusahaan tersebut terselip lalu hilang. Tentu hal tersebut akan sangat merugikan bagi pemilik data dan perusahaan. Akibatnya saat informasi atau data dibutuhkan oleh *manager* atau *owner* perusahaan, penyampaian informasi atau data tersebut menjadi kurang tepat.

Oleh sebab itu masalah keamanan suatu data merupakan aspek penting dari suatu sistem informasi. Jika data tersebut bersifat penting maka data tersebut harus diberikan keamanan khusus agar orang yang tidak bertanggung jawab tidak dapat mengerti mengenai data tersebut. Mengimplementasikan sebuah teknik kriptografi ini dapat mengamankan isi catatan dengan proses enkripsi dan dekripsi data. Proses enkripsi ini nantinya akan mengubah susunan tulisan atau bahkan merubah karakter huruf secara acak sehingga tulisan tidak dapat dibaca tanpa kunci tertentu untuk mengembalikan *text* asli dari tulisan tersebut.

Berdasarkan permasalahan diatas, penulis membuat Aplikasi *Notes* dengan menggunakan Algoritma Enkripsi RC4 (*Rivest Code* 4) untuk mengamankan isi catatan yang berisikan informasi atau data perusahaan yang penting. Selain itu aplikasi ini juga dirancang dengan fitur dimana karyawan PT Internusa Food bisa mengirimkan atau men-*send file* catatan tersebut melalui *handphone* kepada *manager* atau *owner* yang dikategorikan sebagai si pemilik catatan tersebut. Salah satu algoritma kunci simetris

yang berbentuk *stream cipher* membuat RC4 mampu memproses unit atau *input* data pada satu saat. Dan memiliki kecepatan operasi yang lebih tinggi dibandingkan algoritma lainnya menjadikan algoritma RC4 ini dapat diimplementasikan pada sistem *real-time*. Untuk itu dengan algoritma kriptografi RC4 (*Rivest Code* 4) yang diimplementasikan pada aplikasi *notes* ini berbasis android diharapkan kerahasiaan isi catatan tetap aman.

2. ANALISA KEBUTUHAN SISTEM

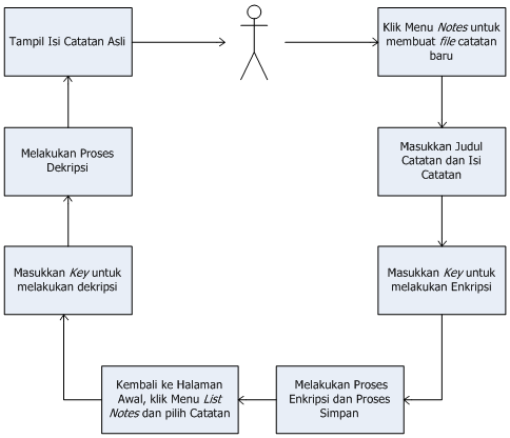
2.1. Masalah

Pencatatan informasi berupa data perusahaan lainnya yang masih manual berupa tulisan dikertas *sticky notes* yang ditempelkan pada komputer di PT Internusa Food saat ini dirasa masih kurang optimal, hal ini dikarenakan kurangnya keamanan dari sebuah catatan tersebut. Akibatnya bisa saja kertas *sticky notes* tersebut hilang atau bahkan bisa dibaca orang yang tidak bertanggung jawab. Dengan begitu saat informasi atau data dibutuhkan, penyampaian informasi atau data tersebut jadi kurang tepat.

Dengan adanya permasalahan tersebut maka dibutuhkan sebuah wadah penyimpanan catatan tersebut yang bisa digunakan oleh pegawai PT Internusa Food secara *mobile* yang nantinya saat data yang dibutuhkan tersimpan dalam satu tempat dan juga dapat diakses oleh *manager* atau *owner* perusahaan yang dikategorikan juga sebagai si pemilik catatan. Dengan demikian diharapkan isi catatan tidak bisa dilihat orang lain sehingga isi catatan menjadi aman dan bisa memudahkan pegawai karna dapat dilihat dari *smartphone* pegawai.

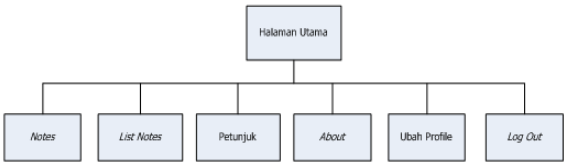
2.2. Solusi Penelitian

Dari permasalahan diatas, maka dibuatlah sebuah aplikasi *notes* yang dapat dijalankan pada semua jenis *smartphone* dan sekaligus dapat mengamankan isi catatan tersebut menjadi teks yang tidak bisa dibaca oleh pihak yang tidak berhak. Dengan begitu diharapkan isi *notes* terjaga kerahasiaannya. Kemudian aplikasi bisa mengembalikan isi catatan tersebut menjadi seperti semula tanpa mengalami perubahan. Dalam proses menyimpan catatan dan membuka kembali isi catatan dibutuhkan kunci yang sama yang dimasukkan saat pengguna menyimpan catatan tersebut sehingga orang lain yang tidak mengetahui kunci tersebut tidak dapat membaca isi dari catatan. Berikut Gambar 1 merupakan alur proses aplikasi yang akan dibuat.



Gambar 1. Alur Proses Aplikasi

Berdasarkan analisa kebutuhan maka dibuat rancangan Aplikasi Catatan dengan algoritma Kriptografi RC4 (*Rivest Code* 4) PT Internusa Food yang akan diimplementasikan. Dengan tujuan struktur dari tampilan menu ini akan mempermudah dalam pembuatan aplikasi. Berikut ini gambaran tampilan menu yang akan dibuat pada Gambar 2.



Gambar 2. Tampilan Menu Aplikasi

2.3. Spesifikasi Database

Pada aplikasi *notes* (catatan) ini, membutuhkan database yang terdiri dari tb*notes* dan tb*user*. Database yang digunakan bersifat dinamis yang artinya bisa melakukan penambahan data, pengubahan data dan penghapusan data tanpa mengubah program. Dan *file* database diberi nama db*notes*.

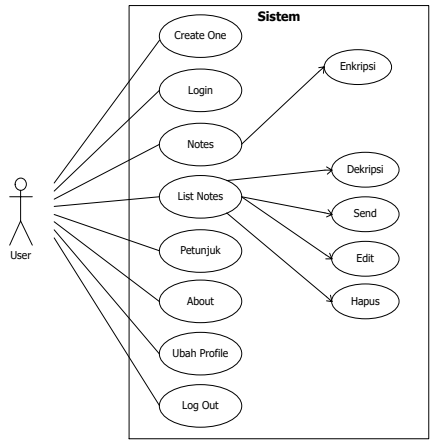
Nama *Field*	Tipe Data	Ukuran *Field*	Keterangan
Idcatatan	Varchar	10	Id Catatan
judulcatatan	Text		Judul Catatan
catatan	Text		Isi Catatan
created_at	Timestamp		Tanggal Catatan
email	Varchar	20	*Email User*
statusdata	Varchar	10	Status Catatan
keyrc4	Varchar	20	kunci/*Key*

Tabel 1. Tabel Tb*notes*

Nama *Field*	Tipe Data	Ukuran *Field*	Keterangan
Email	Varchar	20	*Email User*
Telepon	Varchar	20	Telepon *User*
Username	Varchar	50	*Username User*
Password	Varchar	50	*Password User*
Status	Varchar	10	Status *User*

Tabel 2. Tabel Tb*user*

Untuk *use case* diagram aplikasi dapat dilihat pada Gambar 3 sebagai berikut:



Gambar 3. Diagram *Use Case* Aplikasi

2.4. Metode Penelitian

Penelitian ini menggunakan pendekatan umum *Waterfall* yang dibuat sebagai berikut:

a. Analisa, Tahap dimana dilakukan proses pengumpulan data, identifikasi masalah, dan analisis kebutuhan sistem hingga aktifitas pendefinisian sistem. Tahap ini bertujuan untuk menemukan solusi yang didapat dari aktivitas-aktivitas tersebut.

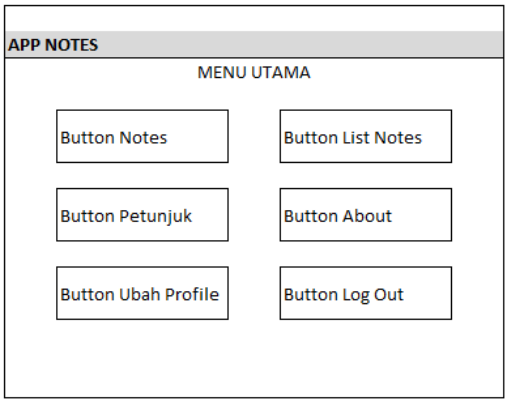
b. Perancangan Sistem, Data yang diperoleh kemudian dipelajari dan dianalisa untuk mengetahui cara kerja algoritma kriptografi yang dibuat. Membuat desain rancangan layar sistem sesuai analisa yang dilakukan, membuat *Flowchart*, database dan lain-lain.

c. Implementasi, Mengimplentasikan rancangan sistem yang sudah dibuat berdasarkan hasil analisa. Dituangkan dalam kode-kode dengan menggunakan bahasa pemograman. Pada penerapan ke dalam program akan digunakan bahasa pemrograman *Java Mobile* (Android) dengan database *MySQL*.

d. Pengujian Sistem, Pada tahapan ini peneliti memeriksa kembali dari tahapan analisa dan desain dalam pengerjaan aplikasi kemudian akan dilakukan pengujian hasil desain sistem tersebut. Termasuk dalam memperbaiki kesalahan yang tidak ditemukan pada langkah sebelumnya.

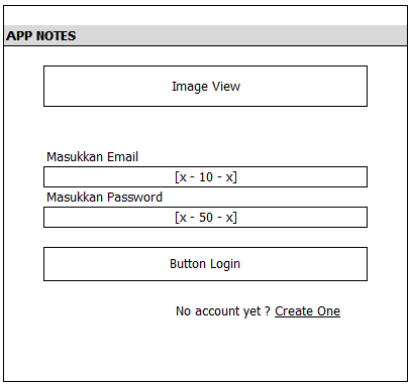
2.5. Rancangan Aplikasi

Rancangan halaman utama ini merupakan tampilan yang akan muncul pada saat aplikasi dijalankan.



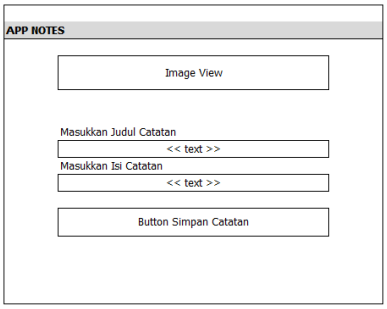
Gambar 4. Rancangan Halaman Utama

Pada rancangan ini menampilkan *form* untuk melakukan *login* pengguna. Pada rancangan layar *form login* ini terdapat juga tombol *Create One* yang digunakan untuk *user* yang belum mempunyai akun atau belum terdaftar.



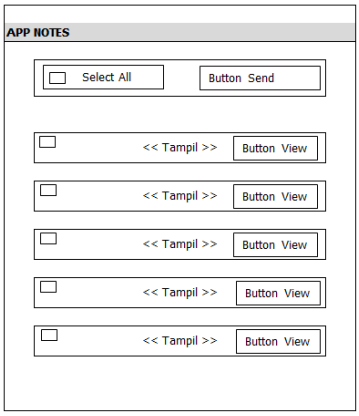
Gambar 5. Rancangan *Login*

Pada rancangan ini muncul ketika pengguna hendak membuat catatan baru dengan mengklik tombol *Notes* pada halaman utama.



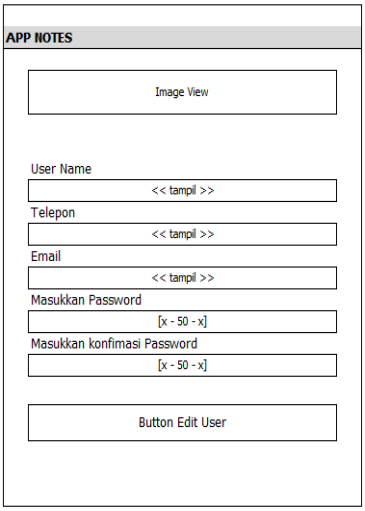
Gambar 6. Rancangan *Notes*

Pada rancangan menu *list notes* ini menampilkan *form* untuk melihat daftar catatan yang sudah dibuat pengguna dan tersimpan dalam database.



Gambar 7. Rancangan *List Notes*

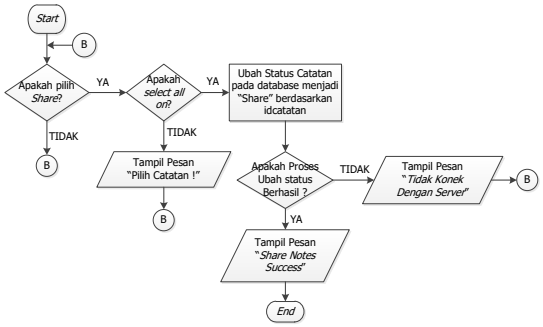
Rancangan layar *Form* ubah *profile* ini merupakan tampilan yang akan muncul setelah pengguna mengklik menu Ubah *Profile*. Rancangan ini digunakan untuk mengubah atau mengganti data pengguna.



Gambar 8. Rancangan Ubah *Profile*

2.6. Flowchart Button Send

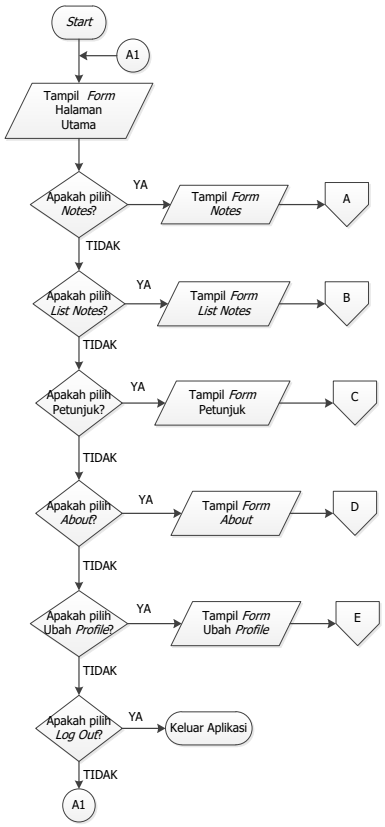
Flowchart dibawah ini menggambarkan proses dari *button Send* catatan yang berlangsung pada *Form List Notes. Button* ini berfungsi untuk mengirim *file* catatan dari akun karyawan ke *manager* sebagai orang yang berhak menerimanya.



Gambar 9. *Flowchart Button Send*

2.7. Flowchart Home Aplikasi

Flowchart form halaman utama merupakan alur proses menu pada aplikasi. *Flowchart* ini yang akan digunakan pada saat pengguna membuka aplikasi.



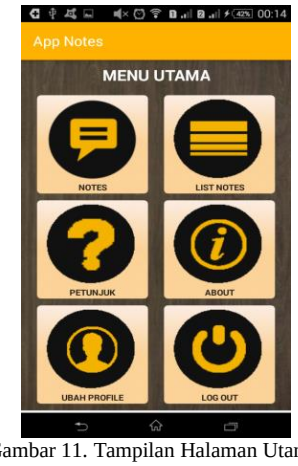
Gambar 10. *Flowchart Home* Aplikasi

3. URAIAN

3.1. Implementasi Aplikasi

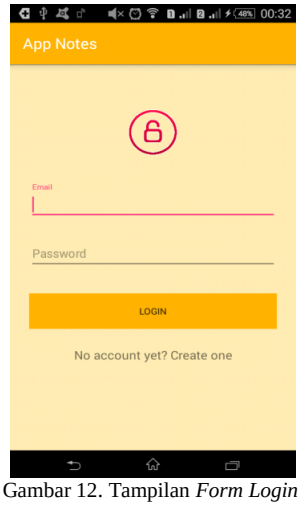
Untuk memastikan keberhasilan jalannya aplikasi ini, perlu dilakukan pengujian untuk aplikasi yang dibuat. Jika tidak diuji terlebih dahulu bisa saja aplikasi tersebut gagal digunakan. Pengujian tersebut untuk mengetahui *performance*, hasil enkripsi dan hasil dekripsi *notes* dengan RC4 serta memastikan semua fitur berjalan dengan baik. Untuk halaman

utama pada aplikasi memiliki tampilan sebagai berikut.



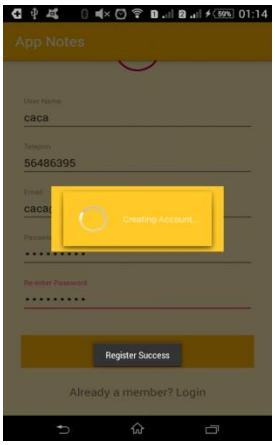
Gambar 11. Tampilan Halaman Utama

Berikut Gambar 12 tampilan *form login* aplikasi, data yang digunakan pengguna adalah *email* dan *password* yang terdaftar pada aplikasi.



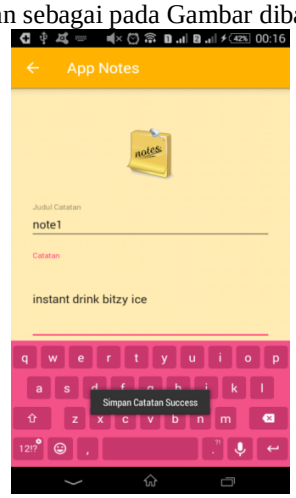
Gambar 12. Tampilan *Form Login*

Jika pengguna belum mempunyai akun, maka pengguna dapat membuat akun baru untuk bisa membuka aplikasi ini. Pengguna bisa membuat akun baru dengan mengklik tombol *Create One* yang terdapat pada tampilan *Login* pada langkah kedua. Pada tampilan berikut ini pengguna diminta untuk mengisi data pengguna seperti *Username*, Telepon, *Email* dan *Password* akun. Jika pembuatan akun pengguna berhasil akan muncul pesan *"Register Success"* seperti pada Gambar dibawah ini.



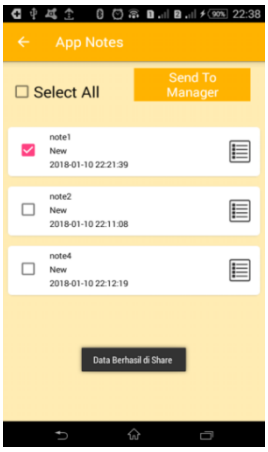
Gambar 13. Tampilan Sukses Register

Langkah selanjutnya adalah membuat *file* catatan baru dengan mengklik tombol *Notes* pada Halaman Utama. Pada tampilan ini pengguna dapat memasukkan judul dan isi catatan yang akan disimpan. Selanjutnya akan diminta memasukkan sebuah kata kunci untuk proses penyimpanan catatan. Dan setelah berhasil memasukkan kata kunci dan proses menyimpan catatan berhasil maka akan muncul tampilan sebagai pada Gambar dibawah ini.



Gambar 14. Tampilan Simpan Catatan

Jika pengguna hendak mengirimkan *file* catatan kepada akun *manager* yang terdaftar pada aplikasi dapat dilihat pada Gambar 15 dibawah ini. Pada tampilan ini pengguna diharuskan untuk mencentang atau memberi tanda pada kotak *select* di tiap *file* catatan yang akan dikirimkan dan dilanjutkan dengan menekan tombol *Send To Manager*.



Gambar 15. Tampilan *Send Notes* Berhasil

Untuk tampilan hasil penyimpanan *file* catatan dari database program yang digunakan. Tampilan dapat dilihat pada Gambar 16 dimana isi catatan yang tampil berupa teks yang telah terenkripsi pada *field* catatan.

judulcatatan	catatan	created_at	email	statusdata
note2	fqmnh	2018-01-07 15:04:58	kaka@gmail.com	New
note3	`rfhk}kwz	2018-01-07 15:22:35	kaka@gmail.com	Share
note4	higc`%f}hqi	2018-01-07 15:22:35	kaka@gmail.com	Share
note5	`wclj}ntq	2018-01-07 15:06:26	kaka@gmail.com	New
note1	hmjh pb`	2018-01-07 15:49:27	lala@gmail.com	New
note2	wwfg|%giglq	2018-01-07 15:49:49	lala@gmail.com	New

Gambar 16. Tampilan Layar Database

Melakukan pengujian proses enkripsi *notes*, Tabel 4 dibawah ini akan menampilkan isi catatan yang telah di lakukan proses enkripsi kemudian dilakukan proses dekripsi yaitu mengembalikan *ciphertext* pada tabel enkripsi diatas menjadi *plaintext* kembali atau menjadi teks asli kembali. Pengujian ini dilakukan untuk membuktikan bahwa hasil dari pengujian enkripsi *notes* telah berhasil dan dapat dikembalikan menjadi teks asli dengan menggunakan kunci/*key* yang sama saat proses simpan *notes*.

Isi Notes Asli		Kunci
Judul	**Isi Catatan**	
note1	*instant drink bitzy ice*	1234
note2	*lollipops*	56789
note3	*parago chewy and milk*	10121416
note4	*soya cereal*	8905478
note5	*cucu stick biscuits*	64439992
note6	*vanelo layer cakes*	65645789
note7	*coffee hard candy*	65645789

Tabel 3. Tabel *Text Notes* Asli

Isi Notes Enkripsi		Kunci	Dekripsi Notes	
Judul	**Isi Catatan**		**Judul**	**Isi Catatan**
note1	| xftiw5kqlij*ez{ws(bgi	1234	*note1*	*instant drink bitzy ice*
note2	noldlvhrv	56789	*note2*	*lollipops*
note3	an}lvf+`fozz$f|g/d`ie	10121416	*note3*	*parago chewy and milk*
note4	uk c dozfgd	8905478	*note4*	*soya cereal*
note5	oqsz.y|jil.nj q~f}	64439992	*note5*	*cucu stick biscuits*
note6	vc`lj~&bjwf{}apce{	65645789	*note6*	*vanelo layer cakes*
note7	k `nbf%jaxh'o`kz	65645789	*note7*	*coffee hard candy*

Tabel 4. Tabel Hasil Uji Coba

4. AKHIR

Adapun kesimpulan yang diperoleh setelah melewati tahap perancangan, pembuatan, serangkaian uji coba dan analisa program aplikasi *Notes* ini, kesimpulan yang didapat adalah sebagai berikut:

a. Dengan mengimplementasikan Algoritma RC4 (*Rivest Code* 4) pada proses enkripsi dan dekripsi pada database berjalan dengan baik sehingga isi catatan tidak terbaca oleh pihak luar.
b. Aplikasi ini memiliki fitur pengamanan informasi ganda yaitu *login user* dan enkripsi isi *notes* sehingga dapat merahasiakan isi *notes* lebih baik.
c. Semakin panjang kunci atau *key* maka semakin kuat keamanan enkripsi datanya.

Dengan adanya keterbatasan aplikasi ini, ada beberapa saran yang perlu dipertimbangkan guna pengembangan aplikasi lebih lanjut antara lain:

a. Dapat difokuskan penggunaan metode kriptografi dengan kombinasi algoritma yang lain guna meningkatkan keamanan data.
b. Dapat ditambahkan fitur *search* atau cari catatan dari judul catatan guna mempermudah *user* dalam melakukan pencarian catatan yang diperlukan si pengguna.
c. Dapat ditambahan untuk karakter masukkan kunci/*key* tidak hanya berupa angka saja tetapi dapat berupa karakter huruf.

5. DAFTAR PUSTAKA

[1] Menezes, Oorcshot, dan Vanstone, 1996, *Hanbook Of Applied Cryptography*, Florida, CRC Press.
[2] Saefudin dan Syamsudin, 2017, Aplikasi Enkripsi Pesan Teks Dengan Metode AES Pada Ponsel Berbasis Android, Serang, Universitas Serang Raya.
[3] Schneier, Bruce, 1996, *Applied Cryptography, Second Edition*, New Jersey, John Wiley & Sons, Inc.
[4] Saragih, Uli S., 2017, Implementasi Enkripsi Dan Dekripsi Metode RC4 Untuk Pengamanan Data Sistem Informasi, Lampung, Universitas Lampung.
[5] D. P. Nasional, 2008, Kamus Besar Bahasa Indonesia Pusat Bahasa, Jakarta, Gramedia Pustaka Utama.
[6] Piansyah, E., 2008, Implementasi Algoritma Dasar RC4 *Stream Cipher* Dan Pengacakan *Plaintext* Dengan Teknik *Dynamic Blocking* Pada Aplikasi

Sistem Informasi Kegiatan Skripsi Di Dep. Teknik Elektro, Depok, Universitas Indonesia.
[7] Kurniawan, Yusuf, 2004, Kriptografi Keamanan Internet Dan Jaringan Komunikasi, Bandung, Informatika Bandung.
[8] Douglas, R. Stinson, 2006, *Cryptography: Theory And Practice*, Florida, CRC Press.