PEMBUATAN APLIKASI NOTES MENGGUNAKAN ALGORITMA KRIPTOGRAFI POLYALPHABETIC SUBSTITUTION CIPHER KOMBINASI KODE ASCII DAN OPERASI XOR BERBASIS ANDROID

Rizqi Sukma Kharisma[1)],**Muhammad Aziz Fatchu Rachman**[2)]

[1,2)] Fakultas Ilmu Komputer Universitas AMIKOM Yogyakarta
Jl Ringroad Utara, Condongcatur, Depok, Sleman, Yogyakarta Indonesia 55283
Email : sukma@amikom.ac.id [1)] ,muhammad.rachman@students.amikom.ac.id [2)]

Abstract

Di era digital ini, teknologi berbasis android berkembang begitu cepat. Maka dari itu faktor keamanan sangat berperan penting, sehingga seluruh aplikasi berbasis mobile butuh keamanan. Saat ini menyimpan catatan singkat baik bersifat umum dan pribadi tidak membutuhkan buku dan pena lagi. Kita dapat menyimpannya di smartphone karena hampir semua masyarakat memilikinya. Kerahasiaan informasi catatan tersebut tentunya tidak ingin diketahui dan dicuri oleh orang lain. Maka dari itu dibutuhkannya suatu sistem keamanan yang dapat menjaga informasi tersebut yaitu aplikasi note menggunakan kriptografi. Dengan menggunakan kriptografi ini, informasi yang kita simpan dapat dienkripsi dan dideskripsi dengan suatu kunci yang kita inputkan sehingga hanya kita saja yang tahu isi dari informasi tersebut.

Keywords – *Polyalphabetic Substitution Cipher, Notes, ASCII, XOR.*

1. Pendahuluan

1.1 Latar Belakang

Dalam beberapa dekade terakhir terjadi perkembangan teknologi secara pesat dan masif sehingga berpengaruh pada kebutuhan hidup manusia. Salah satu teknologi paling berpengaruh yang hampir tidak pernah lepas dari setiap kegiatan kita dan selalu dibawa kemana pun yaitu *smartphone*. *Smartphone* merupakan kombinasi telepon genggam dengan fungsional dari *personal digital assistant* (PDA) yang memungkinkan pengguna untuk menyimpan dan membalas email, mengelola kontak dan informasi kalender, mengakses internet mengirim dan menerima pesan, bermain *games*, *file* multimedia, fitur GPS dan berbagai fitur lainnya. [1]

Ada berbagai macam *platform* yang digunakan pada *smartphone* diantaranya Android, iOS, dan Windows Phone. Salah satu *smartphone* yang sedang mengalami peningkatan dalam 5 tahun belakangan ini adalah *smartphone* Android. Saat ini terdapat ratusan juta perangkat *smartphone* Android yang beredar di 190 negara lebih di seluruh dunia dan setiap harinya lebih dari satu juta *smartphone* baru berbasis Android diaktifkan. Tidak heran Android menjadi *platform smartphone* paling populer di dunia. [2]

Android merupakan *platform* yang bersifat *open source*, dimana *source code* (kode sumber) pada Android dapat dibaca oleh pengembang untuk mengkostumisasi berbagai fitur aplikasi sesuai kebutuhan penggunanya. para pengembang pun dapat menjual aplikasinya ke salah satu fitur *smartphone* android yaitu Google Play yang membantu para pengembang untuk membangun visibilitas, *brand*, dan keterlibatan seluruh aplikasi pengembang. Dengan adanya fitur Google Play yang mendistribusikan berbagai macam aplikasi Android, tak heran dalam 1 bulan milyaran aplikasi telah *terdownload*. [2]

Melihat dari pertumbuhan *smartphone* berbasis Android ini, penulis melakukan penelitian yaitu membuat aplikasi *Notes* berbasis Android dengan menggunakan kriptografi, dimana kriptografi ini merupakan ilmu dan seni untuk menjaga keamanan pesan yang nantinya akan menjaga kerahasiaan isi *Note*, dengan melakukan proses enksipsi dan deskripsi data. [3]

1.2 Rumusan Masalah

Berdasarkan latar belakang yang telah dikemukakan, maka permasalahan yang dapat dirumuskan adalah bagaimana membuat aplikasi *Notes* menggunakan algoritma kriptografi Polyalphabetic Substitution Cipher yang dikombinasikan dengan kode ASCII dan operasi XOR berbasis android?

1.3 Tujuan

Tujuan dari penelitian ini dimaksudkan untuk membuat aplikasi *Note* berbasis android dengan kerahasian isi *Note* lebih terjaga karena data atau informasi yang dibuat akan dienkripsi dengan algoritma kriptografi Polyalphabetic Substitution Cipher yang dikombinasikan dengan kode ASCII dan operasi XOR.

1.4 Tinjauan Pustaka

Dalam implementasi, berikut beberapa acuan yang penulis gunakan :

Ari (2016), dalam papernya yang berjudul "*Implementasi Teknik Steganografi Dengan Kriptografi Kunci Private AES Untuk Keamanan File Gambar Berbasis Android"* membahas tentang penerapan teknik steganografi yang merupakan seni penyembunyian informasi kedalam media gambar dengan algoritma kriptografi AES untuk melindungi hak cipta dari suatu *file* gambar. Persamaan dengan penelitian yang saya lakukan yaitu sama-sama aplikasi enkripsi berbasis android. Sedangkan perbedaannya yaitu implementasi yang saya terapkan tidak pada *file* gambar, melainkan pada aplikasi *Notes*. Dan juga algoritma yang saya gunakan yaitu algoritma Polyalphabetic Substitution Cipher yang dikombinasikan dengan kode ASCII dan operasi XOR. [4]

Aedhoh (2016), dalam papernya yang berjudul "*Perancangan Aplikasi Diary Menggunakan Algoritma Kriptografi RC6 Berbasis Android*" membahas tentang implementasi algoritma kriptografi RC6 untuk mengenkripsi dan mendeskripsi data yang tersimpan di diary agar tidak dapat dibaca dan disalahgunakan oleh orang lain. Persamaan dengan penelitian yang saya lakukan yaitu sama-sama aplikasi enkripsi berbasis android. Sedangkan perbedaannya yaitu implementasi yang saya terapkan tidak pada aplikasi *Diary*, melainkan pada aplikasi *Notes*. Dan juga algoritma yang saya gunakan yaitu algoritma Polyalphabetic Substitution Cipher yang dikombinasikan dengan kode ASCII dan operasi XOR. [5]

Upik (2016), dalam jurnalnya yang berjudul "*Perancangan Aplikasi Kriptografi Berlapis Menggunakan Algoritma Caesar, Transposisi, Vigenere, Dan Blok Cipher Berbasis Mobile*" membahas tentang implementasi 4 algoritma kriptografi klasik untuk proses enkripsi dan deskripsi . Persamaan dengan penelitian yang saya lakukan yaitu sama-sama aplikasi enkripsi berbasis android. Sedangkan perbedaannya yaitu implementasi yang saya terapkan tidak pada aplikasi sederhana yang hanya melakukan proses enkripsi dan deskripsi pada textbox yang disediakan melainkan pada aplikasi *Notes*. Dan juga algoritma yang saya gunakan yaitu algoritma Polyalphabetic Substitution Cipher yang dikombinasikan dengan kode ASCII dan operasi XOR. [6]

1.4.1 Android

Android adalah sebuah sistem operasi untuk perangkat *mobile* berbasis linux yang mencakup sistem operasi, *middleware* dan aplikasi. Android menyediakan *platform* terbuka bagi para pengembang untuk menciptakan aplikasi mereka. Android memiliki *platform* yang sangat lengkap baik itu sistem operasinya, aplikasi, dan *tool* pengembangnya, serta dukungan yang sangat tinggi dari komunitas *Open Source* di dunia. [7]

1.4.2 Notes

Notes atau buku catatan adalah buku yang ukurannya lebih kecil daripada buku tulis, untuk mencatat hal yang dianggap penting yang biasanya berisikan berbagai hal seperti kegiatan sehari, hasil karya tulis, informasi penting, dan lain sebagainya. [8]

1.4.3 Kriptografi

Kroptografi bersala dari bahasa Yunani, menurut bahasa Kriptografi terbagi menjadi dua yaitu *kripto* dan *graphia*. Kripto berarti *secret* (rahasia) dan graphia berarti *writing* (tulisan). Menurut terminologinya, Kriptografi adalah ilmu dan seni untuk menjaga keamanan pesan ketika dikirim dari suatu tempat ketempat lain. [3]

Algoritma kriptografi terbagi menjadi dibagi menjadi tiga bagian berdasarkan dari kunci yang digunakan yaitu Algoritma Simetri,

Algoritma Asimetri dan Fungsi Hash. Algoritma Simetri adalah algoritma klasik karena menggunakan kunci yang sama untuk proses Enkripsi dan Dekripsinya. Algortima Simetri memakai kunci simetri diantaranya *Data Encryption Standart* (DES), *International Data Encryption Algorithm* (IDEA), *Advenced Encryption Standart* (AES), *One Time Pad* (OPT) RC2, RC3, RC4, RC5,dan RC6 dan lain sebagainya. [3]

1.4.4 Polyalphabetic Substitution Cipher

Sistem cipher substitusi adalah sebuah algoritma enkripsi dan dekripsi yang mensubstitusi unit-unit sebuah *text* dengan unit-unit lain berdasarkan aturan tertentu. Unit-unit ini bisa saja sebuah huruf, sepasang huruf, sebuah kata, dan sebagainya.

Pada penelitian ini kode abjad majemuk atau polyalphabetic substitution cipher yang digunakan yaitu kode Vigenere Blok angka. Kode Vigenere dipublikasikan oleh diplomat (sekaligus seorang kriptologis) Perancis Blaise de Vigenere pada abad 16, tahun 1586. Algoritma ini baru dikenal luas 200 tahun kemudian dan dinamakan kode Vigenere.[9]

Cipher abjad-majemuk ini dibuat dari sejumlah cipher abjad-tunggal, masing-masing dengan kunci yang berbeda. Kebanyakan cipher abjad-majemuk adalah cipher substitusi periodic yang didasarkan pada periode m.

Contoh

P : KRIPTOGRAFI
K: LAMPIONLAMP
C: VRUEBCTCARX

Perhitungan :

(K + L) mod 26 = (10 + 11) mod 26 = 21 = V

(R + A) mod 26 = (17 + 0) mod 26 = 17 = R

Dst.

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

Tabel 1. Konversi Huruf ke Angka

1.4.5 ASCII

ASCII *(American Standard Code for Information Interchange)* atau kode Standar Amerika untuk Pertukaran Informasi. Merupakan suatu standar internasional dalam kode huruf dan lumeri seperti Hex dan Unicode tetapi ASCII lebih bersifat universal, contohnya 124 adalah untuk karakter "|". Biasanya digunakan oleh komputer dan alat komunikasi lain untuk menunjukkan teks. Dalam kriptografi, kode ASCII ini merupakan urutan bit yang akan mewakili teks asli yang kemudian dienkripsi untuk mendapatkan teks kode dalam bentuk urutan bit.ASCII memerlukan 8 bit untuk mendapatkan satu karakter dan blok kode mempunyai 64 bit untuk satu blok.[9]

Karakter control pada ASCII dibedakan menjadi 5 kelompok sesuai dengan penggunaan yaitu berturut-turut meliputi *logical communication*, *Device control*, *Information separator*, *Code extention*, dan *physical communication*. Kode ASCII ini banyak dijumpai pada *keyboard* komputer atau instrumen-instrumen digital.

1.4.6 XOR

Secara singkat, operasi XOR akan mengembalikan nilai 1 jika jumlah operand bernilai satu ganjil, jika tidak maka akan mengembalikan hasil 0. Operasi ini memberikan cara pengkombinasian dua *bit-string* dengan panjang yang sama.[9]

A	B	A XOR B
0	0	0
0	1	1
1	0	1
1	1	0

Tabel 2. Operasi XOR

2. Pembahasan

2.1 Analisis Kebutuhan Fungsional

Kebutuhan fungsional adalah jenis kebutuhan yang menjelaskan fungsi-fungsi yang nantinya dapat dilakukan sistem. Adapun kebutuhan fungsional aplikasi *Notes* Kriptograsi Polyalphabetic substitution cipher kombinasi dengan kode ASCII dan operasi XOR ini adalah sebagai berikut :

1. Sistem dapat melakukan Registrasi Akun baru.
2. Sistem dapat melakukan *Login User*.
3. Sistem dapat membuat *Note* berupa *text*.

4. Sistem dapat melakukan enkripsi *text*.
5. Sistem dapat melakukan deskripsi *text*.
6. Sistem dapat menampilkan daftar *Note* yang tersimpan.
7. Sistem dapat membaca *Note* yang ditampilkan.
8. Sistem dapat melakukan *edit* dan *delete Note*.

2.2 Analisis Kebutuhan Non-Fungsional

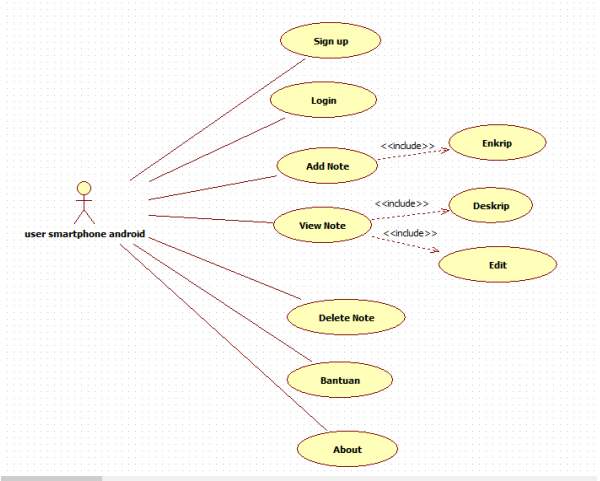
Kebutuhan Non Fungsional adalah jenis kebutuhan yang menjelaskan tentang kebutuhan diluar sistem seperti kebutuhan Operasional, *Performance*, Keamanan, Politik dan Budaya. Adapun kebutuhan Oprasional Aplikasi *Notes* Kriptograsi Polyalphabetic substitution cipher kombinasi dengan kode ASCII dan operasi XOR ini adalah sebagai berikut :

1. Kebutuhan Perangkat Keras
   Spesifikasi perangkat keras yang digunakan penulis dalam pembuatan Aplikasi *Notes* Kriptograsi Polyalphabetic substitution cipher kombinasi dengan kode ASCII dan operasi XOR ini adalah sebagai berikut :
   1. Processor Intel Core i5-5200U 2,2GHz.
   2. Memory (RAM) dengan Kapasitas 8GB.
   3. Harddisk dengan kapasitas 1TB.
   4. VGA Intel(R) HD Graphics 5500 dan NVIDIA GeForce GT 940M 4GB.
2. Kebutuhan minimal device yang digunakan untuk menjalankan aplikasi adalah:
   1. *Smartphone* android atau *emulator* dengan versi minimal 4.4 (*KitKat*).
   2. Memory (RAM) dengan Kapasitas 512MB.
3. Perangkat lunak yang digunakan dalam pembuatan Aplikasi Notes Kriptografi Polyalphabetic substitution cipher kombinasi dengan kode ASCII dan operasi XOR ini adalah sebagai berikut :
   1. Sistem operasi Windows 8.1 Entreprise 64Bit.
   2. Android Studio.
   3. Android *Software Development Kit* (SDK).
   4. Android *Development Tools* (ADT).

2.3 Perancangan UML

2.3.1 *Use Case* Diagram

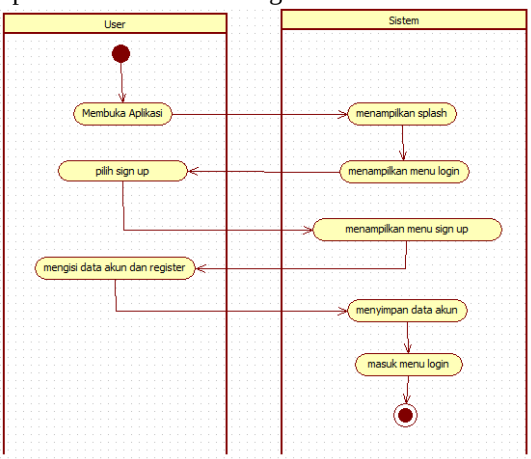
Use case diagram menjelaskan apa yang dilakukan oleh sistem yang akan dibangun dan siapa yang berinteraksi dengan sistem. Adapun *Use case* Diagram Aplikasi *Notes* Kriptograsi Polyalphabetic substitution cipher kombinasi dengan kode ASCII dan operasi XOR adalah sebagai berikut.



Gambar 1. *Use Case* Diagram

2.3.2 *Activity* Diagram

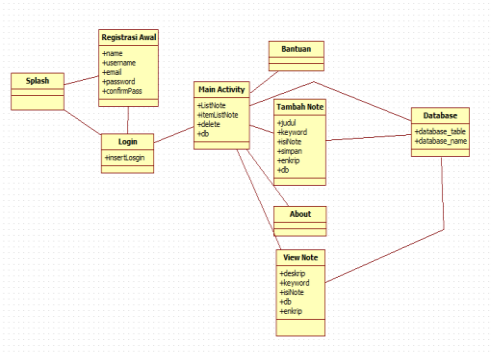
Activity diagram menggambarkan berbagai alir aktifitas dalam sistem yang sedang dirancang, dan bagaimana mereka berakhir. Adapun *Activity* Diagram Aplikasi *Notes* Kriptograsi Polyalphabetic substitution cipher kombinasi dengan kode ASCII dan operasi XOR adalah sebagai berikut.



Gambar 2. *Activity* Diagram Menu *Sign Up*

2.3.3 *Class* Diagram

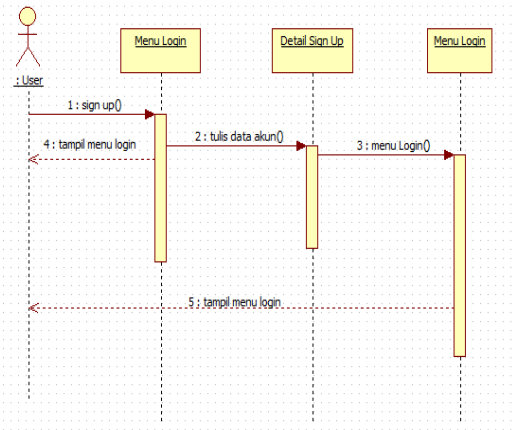
Class diagram mendiskripsikan jenis-jenis objek dalam sistem dan berbagai macam hubungan statis yang terjadi. Adapun *Class* Diagram Aplikasi *Notes* Kriptograsi Polyalphabetic substitution cipher kombinasi dengan kode ASCII dan operasi XOR adalah sebagai berikut.



Gambar 3. *Class* Diagram

2.3.4 *Sequence* Diagram

Sequence diagram digunakan untuk menggambarkan interaksi antara objek dalam dan sekitar sistem (termasuk pengguna,*display*, dan sebagainya) berupa *messege* yang digambarkan terhadap waktu. Adapun *Sequence* Diagram Aplikasi *Notes* Kriptograsi Polyalphabetic substitution cipher kombinasi dengan kode ASCII dan operasi XOR adalah sebagai berikut.



Gambar 4. *Sequence* Diagram Menu *Sign Up*

2.4 Tampilan Aplikasi

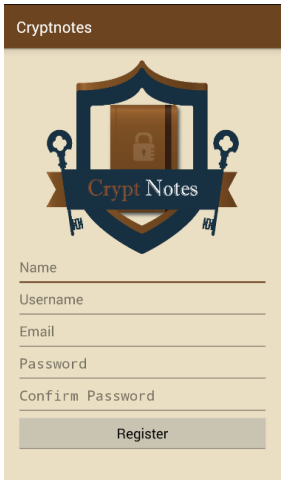
2.4.1 *Splash Screen*

Splash Screen adalah tampilan awal saat membuka aplikasi sebelum memasuki menu *Login*. *Splash Screen* hanya muncul dalam beberapa detik. Tampilan *Splash Screen* aplikasi *Note* ini adalah sebagai berikut.

Gambar 5. *Splash Screen*

2.4.2 Menu *Sign Up*

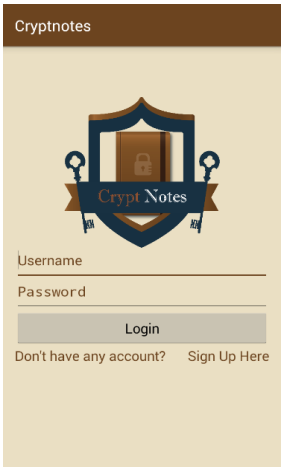
Antar muka Menu *Sign Up* untuk mendaftarkan data *user* yang nantinya akan digunakan untuk login adalah sebagai berikut.



Gambar 6. Antar Muka Menu *Sign Up*

2.4.3 Menu *Login*

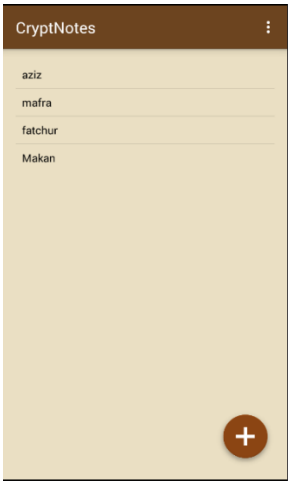
Antar muka Menu *Login* sebagai pengamana sebelum masuk pada menu utama dari aplikasi ini adalah sebagai berikut.



Gambar 7. Antar Muka Menu *Login*

2.4.4 Menu Utama

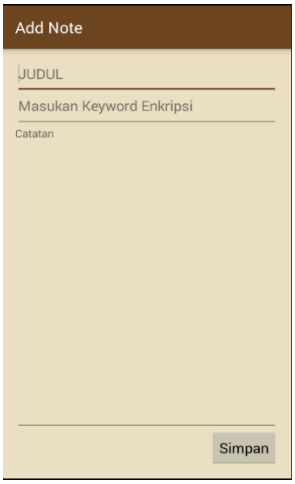
Menu utama dalam aplikasi ini yang menjadi pusat aktifitas dari pengguna memiliki tampilan antar muka sebagai berikut.



Gambar 7. Antar Muka Menu Utama

2.4.5 Menu Tambah *Note* dan *Edit Note*

Menu Tambah *Note* dan *Edit Note* berfungsi untuk menuliskan *Note* baru dan memperbaharui *Note* yang tersimpan , dengan tampilan antar muka sebagai berikut.



Gambar 7. Antar Muka Menu Tambah *Note* dan *Edit Note*

3. Penutup

3.1 Kesimpulan

Setelah melalui tahapan tahapan yang telah dijelaskan pada pembahasan sebelumnya makan dapat ditarik kesimpulan tentang Aplikasi *Cryptnotes* ini adalah:

1. Aplikasi *Cryptnotes* ini menggunakan algoritma kriptografi Polyalphabetic Substitution Cipher yang dikombinasikan dengan kode ASCII dan operasi XOR. Aplikasi ini memiliki fitur pengamanan informasi ganda yaitu *Login Password* dan Enkripsi isi *Note* sehingga penulis dapat merahasiakan isi *Note* lebih baik.
2. Aplikasi dapat berjalan dengan lancar pada sistem operasi Android minimal versi 4.4 (*KitKat*) berdasarkan *usability test* yang telah dilakukan.
3. Setelah melakukan pengujian pada program didapatkan hasil yang memuaskan dimana program berfungsi secara maksimal sesuai rancangan dan kapasitasnya.

3.2 Saran

Berikut beberapa saran yang dapat dipergunakan sebagai pertimbangan untuk pengembangan aplikasi pada penelitian selanjutnya.

1. Aplikasi membutuhkan pengembangan lebih lanjut agar aplikasi lebih sempurna dan terhindar dari berbagai macam *bug* dan *Error*.
2. Pada pengembangan selanjutnya diharapkan dapat menambahkan *fitur-fitur* yang dapat memudahkan pengguan terutama saat membuat dan mengenkripsi

Note yang ditulis serta fitur *backup* data yang terhubung pada *e-mail* pengguna.

Daftar Pustaka

[1] M. Ilyas, dalam *Smartphones*, Intl. Engineering Consortiu, 2006, p. 2.

[2] "Android," [Online]. Available: https://developer.android.com/about/android.html. [Diakses 8 February 2017].

[3] D. Ariyus, Kriptografi : Keamanan Data dan Komunikasi, Yogyakarta: Penerbit Andi, 2006.

[4] A. Muzakir, "Implementasi Teknik Steganografi Dengan Kriptografi Kunci Private AES Untuk Keamanan File Gambar Berbasis Android," dalam *Seminar Nasional Teknologi Informasi dan Multimedia 2016*, Yogyakarta, 2016.

[5] A. S. Assaidi, "Perancangan Aplikasi Diary Menggunakan Algoritma Kriptografi RC6 Berbasis Android," dalam *Seminar Nasional Teknologi Informasi dan Multimedia 2016*, Yogyakarta, 2016.

[6] U. Paranita, "Perancangan Aplikasi Kriptografi Berlapis Menggunakan Algoritma Caesar, Transposisi, Vigenere, Dan Blok Chiper Berbasis Mobile," dalam *Seminar Nasional Teknologi Informasi dan Multimedia 2016*, Yogyakarta, 2016.

[7] N. Safaat, dalam *Pemrograman Aplikasi Mobile Smartphone dan Tablet PC berbasis Android*, Bandung, 2012.

[8] D. P. Nasional, Kamus Besar Bahasa Indonesia Pusat Bahasa, Gramedia Pustaka Utama, 2008.

[9] D. Ariyus, Pengantar Ilmu Kriptografi: Teori Analisis & Implementasi, Yogyakarta: Penerbit Andi, 2008.

Biodata Penulis

Rizqi Sukma Kharisma, memperoleh gelar Sarjana Komputer (S.Kom), Jurusan Teknik Informasi STMIK AMIKOM Yogyakarta, lulus tahun 2009. Memperoleh gelar Magister Komputer (M.Kom) Program Pasca Sarjana Magister Teknik Informatika STMIK AMIKOM Yogyakarta, lulus tahun 2012. Saat ini menjadi Dosen di Universitas AMIKOM Yogyakarta, pada Program Studi Informatika.

Muhammad Aziz Fatchur Rachman, sedang menempuh pendidikan Strata 1 (S1) Program Studi Informatika. Saat ini berstatus Mahasiswa di Universitas AMIKOM Yogyakarta angkatan 2013.