Implementasi Algoritma Vigenere Cipher Dan Atbash Cipher Untuk Keamanan Teks Pada Aplikasi Catatan Berbasis Android

Muhammad Iqbal Afandi[1], Nurhayati[2]
[1]Jurusan Teknik Informatika, Fakultas Teknik dan Imu Komputer
[2]Dosen Jurusan Teknik Informatika Universitas Potensi Utama
[1,2]Universitas Potensi Utama, Jl.K.L. Yos Sudarso Km. 6,5 No 3A Tanjung Mulia Medan
E-mail: [1]muhammadiqbalafandi30@gmail.com, [2]izzkyir@yahoo.com

Abstrak

Teknologi smartphone berbasis android berkembang begitu cepat. Saat ini banyak pengguna yang memanfaatkan aplikasi catatan smartphone android untuk menyimpan catatan baik bersifat umum atau pribadi. Maka dari itu faktor keamanan data sangat berperan penting dalam pengembangan aplikasi smartphone berbasis android. Dengan menggunakan kombinasi algoritma kriptografi, keamanan data dapat lebih terjamin dari serangan-serangan yang dapat membahayakan isi data yang tersimpan. Kombinasi algoritma yang digunakan yaitu algoritma Vigenere Cipher dan algoritma Atbash Cipher. Algoritma Vigenere Cipher adalah metode menyandikan teks abjad dengan menggunakan deretan sandi caesar berdasarkan huruf-huruf pada kata kunci. Algoritma Atbash Cipher adalah cipher substitusi sederhana dengan cara membalikkan abjad sehingga setiap huruf dipetakan ke huruf di posisi yang sama kebalikan dari abjad. Kombinasi algoritma kriptografi ini nantinya digunakan untuk fitur enkripsi teks pada aplikasi catatan yang penulis buat, dengan menggunakan algoritma kriptografi ini teks catatan yang disimpan dapat dienkripsi dan didekripsi dengan suatu kunci yang inputkan sehingga hanya pemilik saja yang tahu isi dari informasi tersebut.

Kata Kunci : Vigenere Cipher, Atbash Cipher, Catatan, Android.

Abstract

Android-based smartphone technology is growing so fast. Currently, many users take advantage of the android smartphone note application to keep notes either public or private. Therefore, the data security factor plays an important role in the development of Android-based smartphone applications. By using a combination of cryptographic algorithms, data security can be more guaranteed from attacks that can harm the contents of stored data. The combination of algorithms used is the Vigenere Cipher algorithm and the Atbash Cipher algorithm. The Vigenere Cipher algorithm is a method of encoding the text of the alphabet by using a series of caesarean codes based on the letters in the keywords. The Atbash Cipher algorithm is a simple substitution cipher by reversing the alphabet so that each letter is mapped to a letter in the same position as the opposite of the alphabet. This combination of cryptographic algorithms will later be used for the text encryption feature of the note application that the author created, using this cryptographic algorithm the stored text of the notes can be encrypted and decrypted with a key that is input so that only the owner knows the contents of the information.

Keywords: Cryptography, Vigenere Cipher, Atbash Cipher, Notes, Android.

1. PENDAHULUAN

Keamanan pesan teks adalah suatu cara untuk melindungi pesan teks dari ancaman, baik dalam bentuk kesengajaan maupun tidak disengaja. Kemajuan teknologi informasi yang sangat pesat membuat permasalahan keamanan sering bermunculan terutama dalam keamanan teks.

Dengan adanya keterangan di atas maka dibutuhkan sebuah cara untuk mengatasi keamanan teks tersebut, salah satu cara pengamanan teks dalam dunia teknologi komputer dan jaringan adalah metode kriptografi. Kriptografi bertujuan untuk menyamarkan data atau informasi yang dikomunikasikan. Kriptografi terbagi atas dua yaitu, kriptografi klasik dan kriptografi *modern*.

Namun pada kasus ini keamanan teks yang akan dibahas adalah keamanan teks pada aplikasi catatan android *smartphone*. Penulis memilih sistem operasi android dikarenakan android *smartphone* banyak digunakan pada saat ini.

Pengguna sering memanfaatkan aplikasi catatan yang ada di android *smartphone* untuk menyimpan catatan yang sifatnya umum atau pribadi. Aplikasi yang penulis buat nantinya memiliki fitur enkripsi teks. Demi meningkatkan keamanan data penulis menggunakan kombinasi algoritma untuk menjaga keamanan data agar lebih terjamin dari serangan-serangan yang dapat membahayakan isi data yang tersimpan, terutama data dalam bentuk teks. Maka atas dasar ini penulis memilih judul penelitihan Implementasi Algoritma *Vigenere Cipher* dan *Atbash Cipher* untuk Keamanan Teks pada Aplikasi Catatan Berbasis Android.

Berdasarkan penelitian yang dilakukan Yusfrizal, Y. (2019). Untuk melindungi dan menjaga rahasia data untuk menghindari orang yang tidak berhak mendapatkan informasi ini, yaitu menggunakan metode kriptografi. Metode kriptografi memiliki teknik dan metode mereka sendiri. Salah satu metode kriptografi yang dapat digunakan adalah metode Reverse Cipher. untuk mencapai tingkat keamanan yang lebih tinggi, metode dikombinasikan dengan metode RSA yang menggunakan kunci publik dan memiliki keamanan yang tinggi[1].

Berdasarkan penelitian yang dilakukan Rizqi Sukma Kharisma dan Muhammad Aziz Fatchu Rachman (2017), membahas tentang penerapan teknik kriptografi pada aplikasi *notes*. Persamaan dengan penelitian yang saya lakukan yaitu sama-sama aplikasi enkripsi catatan (*notes*) berbasis android. Sedangkan perbedaannya yaitu algoritma, algoritma yang saya gunakan yaitu algoritma *Vigenere Cipher* dan *Atbash Cipher*[2].

2. METODE PENELITIHAN

2.1. Pengertian Catatan (*Notes*)

Notes atau buku catatan adalah buku yang ukurannya lebih kecil dari pada buku tulis, untuk mencatat hal yang dianggap penting yang biasanya berisikan berbagai hal seperti kegiatan sehari, hasil karya tulis, informasi penting, dan lain sebagainya[2].

2.2. Pengertian Algoritma

Algoritma adalah spesifikasi urutan langkah untuk melakukan pekerjaan tertentu. Pertimbangan dalam pemilihan algoritma adalah pertama algoritma haruslah benar. Pertimbangan kedua yang harus diperhatikan adalah kita harus mengetahui seberapa baik hasil yang dicapai oleh algoritma tersebut. Ketiga adalah efisiensi algoritma. Efisiensi algoritma dapat ditinjau dari 2 hal yaitu efisiensi waktu dan memori[3].

2.3. Pengertian *Atbash Cipher*

Sandi *Atbash* adalah *cipher* substitusi sederhana dengan cara membalikkan alfabet sehingga setiap huruf dipetakan ke huruf di posisi yang sama kebalikan dari abjad. Pelaksanaan pertama kali *Atbash Cipher* dilakukan pada abjad Ibrani dan referensi perjanjian lama untuk itu *Atbash Cipher* juga telah dikaitkan dengan berbagai bentuk mistisisme. Di zaman *modern*, ini disebut sebagai kode alfabet terbalik, *translator Atbash* ini (termasuk *Encoder Atbash* dan *Decoder Atbash*) dapat membantu mengenkripsi dan dekripsi kode pesan. Sandi *Atbash* digunakan bangsa Yahudi konon sejak sekitar 600 SM. Sandi *Atbash* mengganti alfabet *Hebrew* dengan korespondensi kebalikannya Jika diterapkan pada alfabet latin maka akan berupa:

Pi : A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
Ci : Z Y X W V U T S R Q P O N M L K J I H G F E D C B A.

Maka dari penerapan pada alfabet berikut menghasilkan rumus:

$E(x) = D(x) = (-x \bmod m) + 1$
Keterangan:
E (x): Proses Enkripsi
D (x): Proses Dekripsi
x: *Plaintext* atau *Ciphertext*
m: Jumlah Alfabet dari A-Z
Pada model penyandian ini, huruf "A" pada *plaintext* diubah menjadi huruf "Z" pada *ciphertext*, huruf "B" akan disandikan dengan huruf "Y", dan seterusnya[3].

2.4. Pengertian Kriptografi

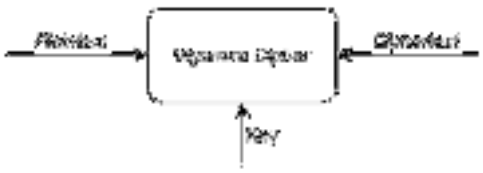
Kriptografi (*cryptography*) berasal dari Bahasa Yunani, yaitu *cryptos* dan *graphia* yang berarti 'penulisan rahasia'. Kriptografi adalah ilmu ataupun seni yang mempelajari bagaimana membuat suatu pesan yang dikirim oleh pengirim dapat disampaikan kepada penerima dengan aman. Kriptografi merupakan bagian dari suatu cabang ilmu matematika yang disebut kriptologi (*cryptology*). Kriptografi bertujuan menjaga kerahasian informasi yang terkandung dalam data sehingga informasi tersebut tidak dapat diketahui oleh pihak yang tidak sah. Perancang algoritma kriptografi disebut *kriptografer*. [3] Enkripsi mengubah informasi atau data menjadi bentuk yang hampir tidak dikenali seperti informasi awal menggunakan algoritma tertentu[4].

2.5. Pengertian *Vigenere Cipher*

Vigenere Cipher termasuk dalam cipher abjad majemuk (*polyalphabetic substitution cipher*) yang dipublikasikan oleh diplomat (sekaligus seorang *kriptologis*) Perancis, *Blaise de Vigenere* pada abad 16 (tahun 1586). *Vigenere Cipher* adalah metode menyandikan teks alfabet dengan menggunakan deretan sandi *caesar* berdasarkan huruf-huruf pada kata kunci. *Vigenere Cipher* merupakan bagian dari algoritma kriptografi klasik yang sangat dikenal karena menggunakan rumus matematika, selain itu *Vigenere Cipher* juga dapat menggunakan tabel *Vigenere* untuk melakukan enkripsi *plaintext* ataupun dekripsi *ciphertext*. Tabel *Vigenere* ini digunakan untuk memperoleh *ciphertext* berdasarkan kunci yang sudah ditentukan. Jika panjang kunci lebih pendek dari *plaintext* maka maka kunci akan diulang penggunaannya secara periodik[4].

2.6. Proses Enkripsi *Vigenere Cipher*

Proses enkripsi menggunakan *Vigenere Cipher* membutuhkan 1 buah kunci untuk dapat menghasilkan *ciphertext*. Kunci yang digunakan merupakan sebuah kata atau susunan dari beberapa huruf. Kemudian dari kunci yang sudah ditentukan akan dikonversikan menggunakan tabel konversi sehingga menjadi bentuk desimal. Selain mengkonversi kunci yang digunakan, *Vigenere Cipher* juga harus mengkonversi *plaintext* (Pi) menggunakan tabel konversi agar menjadi bentuk desimal, kemudian *ciphertext* (Ci) akan diperoleh dengan mengenkripsi *plaintext* dengan persamaan:
$Ci = (Pi + Ki) \bmod 26$
Ci merupakan *ciphertext* dari pergeseran karakter yang terdapat pada *plaintext*. Pi merupakan *plaintext*. Ki merupakan kunci yang digunakan. [4]

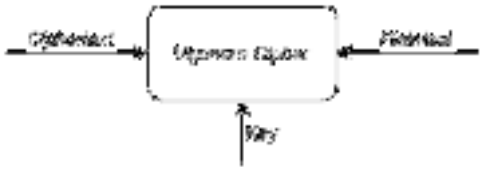


Gambar 1. Proses Enkripsi *Vigenere Cipher*

2.7. Proses Dekripsi *Vigenere Cipher*

Proses dekripsi menggunakan *Vigenere Cipher* membutuhkan 1 buah kunci untuk dapat menghasilkan *plaintext*. Kunci yang digunakan merupakan kunci yang sama dengan kunci yang digunakan pada proses enkripsi. Selain mengkonversi kunci yang digunakan, *Vigenere Cipher* juga

harus mengkonversi *ciphertext* (Ci) menggunakan tabel konversi yang juga menghasilkan bilangan desimal, kemudian *plaintext* (Pi) akan diperoleh dengan mendekripsi *plaintext* dengan persamaan:
Pi = (Ci – Ki+26) mod 26
Pi merupakan *plaintext* dari pergeseran karakter yang terdapat pada *ciphertext*. Ci merupakan pergeseran karakter pada *ciphertext*. Ki merupakan kunci berupa hasil konversi tabel berupa bilangan desimal dari pergeseran karakter yang terdapat pada kunci yang digunakan[5].



Gambar 2. Proses Dekripsi *Vigenere Cipher*

3. HASIL DAN PEMBAHASAN

3.1. *Vigenere Cipher*

Tabel 1. *Vigenere Cipher* Dalam Bentuk Angka

!	“	#	$	%	&	‘	(	)	*	+	,	-	.	/	0	1	2	3	4
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
5	6	7	8	9	:	;	<	=	>	?	@	A	B	C	D	E	F	G	H
20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39
I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	[	\
40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59
]	^	_	`	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p
60	61	62	63	64	65	66	67	68	69	70	71	72	73	74	75	76	77	78	79
q	r	s	t	u	v	w	x	y	z	{	|	}	~						
80	81	82	83	84	85	86	87	88	89	90	91	92	93						

Dari tabel diatas bisa dilihat bawah terdapat angka desimal mulai dari 0 sampai 93, nantinya angka-angka tersebut akan dijumlahkan untuk keperluan mengenkripsi dan dekripsi pada algoritma *Vigenere Cipher*.

1. Enkripsi
Sebelumnya diketahui rumus enkripsinya Ci = (Pi + Ki) *mod* 26, diubah menjadi
Ci = (Pi + Ki) *mod* 94
Keterangan :
Pi diganti dengan nilai desimal karakter yang akan dienkripsi.
Ki diganti dengan nilai desimal kunci dan *modulus* 26 diganti dengan *modulus* 94 dimana angka 94 merupakan jumlah seluruh karakter.

2. Dekripsi
Sebelumnya diketahui rumus dekripsinya Pi = (Ci – Ki + 26) *modulus* 26, diubah menjadi
Pi = (Ci – Ki + 94) *mod* 94
Keterangan :
Ci diganti dengan nilai desimal karakter yang akan didekripsi.
Ki diganti dengan nilai desimal kunci dan *modulus* 26 diganti dengan *modulus* 94 dimana angka 94 merupakan jumlah seluruh karakter.

3.2. *Atbash Cipher*

Tabel 2. *Atbash Cipher* Dalam Bentuk Angka

!	“	#	$	%	&	‘	(	)	*	+	,	-	.	/	0	1	2	3	4
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
5	6	7	8	9	:	;	<	=	>	?	@	A	B	C	D	E	F	G	H
21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40
I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	[	\
41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60
]	^	_	`	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p
61	62	63	64	65	66	67	68	69	70	71	72	73	74	75	76	77	78	79	80
q	r	s	t	u	v	w	x	y	z	{	|	}	~						
81	82	83	84	85	86	87	88	89	90	91	92	93	94						

Dari tabel diatas bisa dilihat bawah terdapat angka desimal mulai dari 1 sampai 94, nantinya angka-angka tersebut akan dijumlahkan untuk keperluan mengenkripsi dan dekripsi pada algoritma *Atbash Cipher*.

Pada *Atbash Cipher* rumus enkripsi dan dekripsi sama yaitu :
E(x) = D(x) = (-x *mod* m) + 1
Keterangan :
x diganti dengan nilai desimal karakter yang akan dienkripsi atau didekripsi dan m pada rumus *Atbash Cipher* diganti dengan angka 94, dimana angka 94 merupakan jumlah seluruh karakter.

3.3. Perhitungan Algoritma

Plaintext: SerBuBerlin
Kunci: PizzapPizap

1. Enkripsi
Plaintext dan kunci diubah kedalam nilai desimal berdasarkan Tabel 2 maka didapat nilai desimal *plaintext* dan kunci:
Plaintext: 50 68 81 33 84 33 68 81 75 72 77

kunci*:* 47 72 89 89 64 79 47 72 89 64 79
diketahui rumus algoritma: *Vigenere Cipher* Ci = (Pi + Ki) *modulus* 94.

Proses perhitungan enkripsi *Vigenere Cipher*:
Ci = (50 + 47) modulus 94 = 3
Ci = (68 + 72) modulus 94 = 46
Ci = (81 + 89) modulus 94 = 76
Ci = (33 + 89) modulus 94 = 28
Ci = (84 + 64) modulus 94 = 54
Ci = (33 + 79) modulus 94 = 18
Ci = (68 + 47) modulus 94 = 21
Ci = (81 + 72) modulus 94 = 59
Ci = (75 + 89) modulus 94 = 70
Ci = (72 + 89) modulus 94 = 67
Ci = (77 + 64) modulus 94 = 47

Dari perhitungan diatas didapat hasil nilai desimal enkripsi *Vigenere Ciphertext*: 3 46 76 28 54 18 21 59 70 67 47, dan jika diubah ke karakter berdasarkan Tabel 2 menjadi $Om=W36\gdP

Selanjutnya yaitu mengenkripsi menggunakan algoritma *Atbash Cipher*. Pertama ubah nilai karakter yang didapat dari hasil enkripsi *Vigenere Ciphertext* kedalam nilai desimal *Atbash Cipher,* berdasarkan Tabel 3 didapat nilai desimal *Atbash Cipher* dari karakter $Om=W36\gdP :
4 47 77 29 55 19 22 60 71 68 48 diketahui rumus algoritma: *Atbash Cipher* E(x) = ((-x *modulus* 94) + 1).

Proses perhitungan enkripsi *Atbash Cipher*:
E(x) = (-4 modulus 94) + 1 = 91
E(x) = (-47 mod 94) + 1 = 48
E(x) = (-77 modulus 94) + 1 = 18
E(x) = (-29 modulus 94) + 1 = 66
E(x) = (-55 modulus 94) + 1 = 40
E(x) = (-19 modulus 94) + 1 = 76
E(x) = (-22 modulus 94) + 1 = 73
E(x) = (-60 modulus 94) + 1 = 35
E(x) = (-71 modulus 94) + 1 = 24
E(x) = (-68 modulus 94) + 1 = 27
E(x) = (-48 modulus 94) + 1 = 47

dari perhitungan diatas maka didapat nilai desimal *Atbash Ciphertext:* 91 48 18 66 40 76 73 35 24 27 47 dan jika diubah ke karakter berdasarkan Tabel 3 menjadi {P2bHliC8;O

2. Dekripsi
Untuk melakukan dekripsi ubah terlebih dahulu
Ciphertext: {P2bHliC8;O
kedalam nilai desimal *Atbash Cipher* berdasarkan Tabel 3 *Ciphertext:* 91 48 18 66 40 76 73 35 24 27 47. Untuk mendekripsi terlebih dahulu menggunakan algoritma *Atbash Cipher,* diketahui rumus dekripsinya D(x) = ((-x *modulus* 94) + 1).

Proses perhitungan dekripsi *Atbash Cipher*:
D(x) = ((-91 modulus 94) + 1) = 4
D(x) = ((-48 modulus 94) + 1) = 47
D(x) = ((-18 modulus 94) + 1) = 77
D(x) = ((-66 modulus 94) + 1) = 29
D(x) = ((-40 modulus 94) + 1) = 55
D(x) = ((-76 modulus 94) + 1) = 19

D(x) = ((-73 modulus 94) + 1) = 22
D(x) = ((-35 modulus 94) + 1) = 60
D(x) = ((-24 modulus 94) + 1) = 71
D(x) = ((-27 modulus 94) + 1) = 68
D(x) = ((-47 modulus 94) + 1) = 48

dari perhitungan diatas maka didapat nilai desimal *Atbash Plaintext:*
4 47 77 29 55 19 22 60 71 43 63. dan jika diubah ke karakter berdasarkan Tabel 3 menjadi $Om=W36\gdP

Selanjutnya yaitu mendekripsi nilai desimal *Atbash Plaintext* yang didapatkan menggunakan algoritma *Vigenere Cipher*, pertama ubah nilai karakter yang didapat dari hasil enkripsi *Atbash Cipher* teks kedalam nilai desimal *Vigenere Cipher,* berdasarkan Tabel 2 didapat nilai desimal *Vigenere Cipher* dari karakter $Om=W36\gdP :
3 46 76 28 54 18 21 59 70 67 47

diketahui rumus algoritma: *Vigenere Cipher* Pi = (Ci – Ki + 94) *modulus* 94. Karena *Vigenere Cipher* membutuhkan kunci menggunakan kunci yang sama dengan kunci yang sebelumnya digunakan untuk melakukan enkripsi
Kunci: 47 72 89 89 64 79 47 72 89 64 79

Proses perhitungan dekripsi *Vigenere Cipher*:
Pi = (3 – 47 + 94) modulus 94 = 50
Pi = (46 – 72 + 94) modulus 94 = 68
Pi = (76 – 89 + 94) modulus 94 = 81
Pi = (28 – 89 + 94) modulus 94 = 33
Pi = (54 – 64 + 94) modulus 94 = 84
Pi = (18 – 79 + 94) modulus 94 = 33
Pi = (21 – 47 + 94) modulus 94 = 68
Pi = (59 – 72 + 94) modulus 94 = 81
Pi = (70 – 89 + 94) modulus 94 = 75
Pi = (67 – 89 + 94) modulus 94 = 72
Pi = (47– 64 + 94) modulus 94 = 77

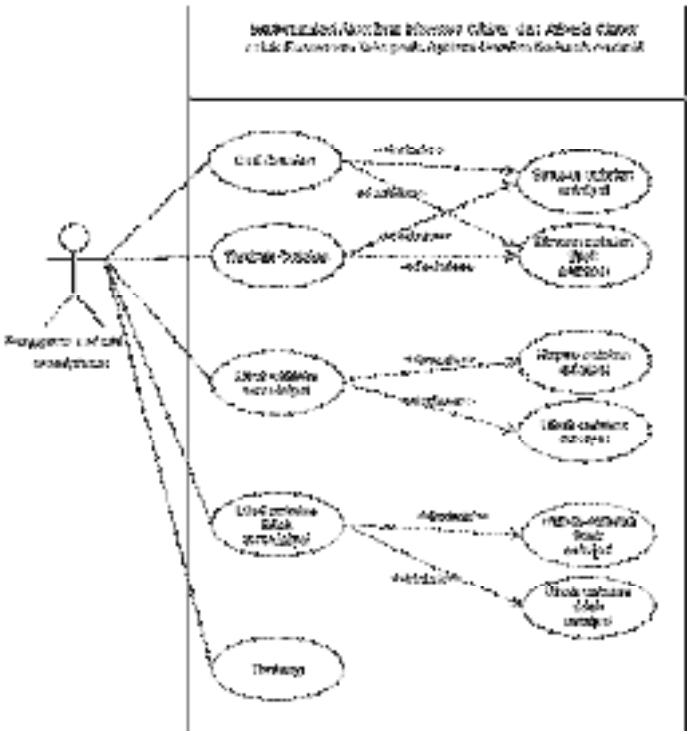
dari perhitungan diatas maka didapat nilai desimal *Vigenere Plaintext:* 50 68 81 33 84 33 68 81 75 72 77.
Terakhir ubah berdasarkan nilai desimal pada Tabel 2 maka didapat:
Plaintext: SerBuBerlin

3.4. Desain Sistem

Adapun tahapan-tahapan dalam mendesain sistem menggunakan *Unified Modeling Language* (UML) antara lain yaitu *Use Case Diagram*, dan *Activity Diagram*.

1. *Use Case Diagram*

Use case diagram adalah *use case diagram* yang digunakan untuk menggambarkan secara ringkas siapa yang menggunakan sistem dan apa saja yang bisa dilakukannya.



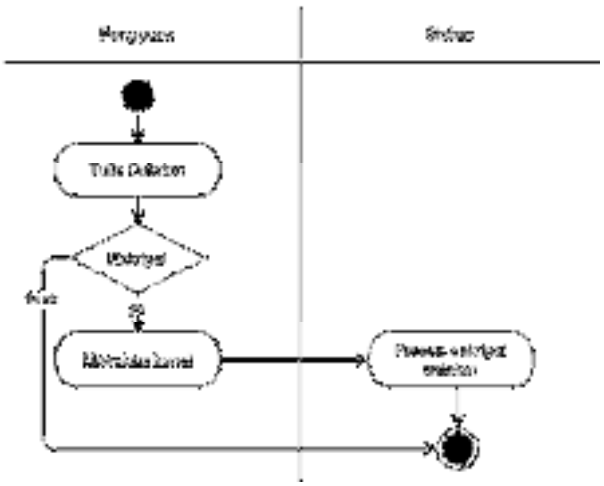
Gambar 3. *Use Case Diagram*

2. *Activity Diagram*

Activity diagram adalah diagram yang menggambarkan *workflow* (aliran kerja). Perlu diperhatikan *Activity diagram* adalah aktivitas yang dapat dilakukan oleh sistem.

a. *Activity diagram* Enkripsi Catatan

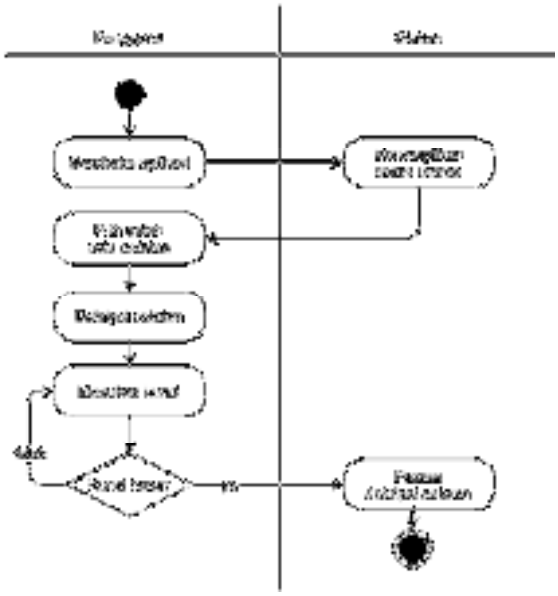
Setelah pengguna menulis catatan penulis memiliki dua opsi, apakah catatan dienkripsi atau tidak, jika dienkripsi pengguna diminta masukan kunci.



Gambar 4. *Activity Diagram* Enkripsi Catatan

b. *Activity Diagram* Dekripsi Catatan

Pengguna memilih catatan yang ingin didekripsi, lalu sistem akan meminta pengguna untuk memasukan kunci, kunci yang digunakan harus sama dengan kunci enkripsi.



Gambar 5. *Activity Diagram* Dekripsi Catatan

3.5. Tampilan Aplikasi

Berikut ini adalah tampilan hasil dari program Implementasi Algoritma *Vigenere Cipher* dan *Atbash Cipher* untuk Keamanan Teks pada Aplikasi Catatan Berbasis Android.

1. Tampilan menu utama

Tampilan menu utama ini pertama kali pengguna lihat, dan di halaman menu utama ini juga akan ditampilkan daftar catatan yang sudah disimpan.

Gambar 6. Tampilan menu utama

2. Masukan Kunci Enkripsi Catatan

Setelah mengikuti proses sebelumnya pengguna akan ditampilkan *form* untuk menambahkan kunci untuk keperluan enkripsi teks catatan, penulis dapat mengimpor kunci yang sudah ada atau menggunakan kunci acak yang sudah disediakan oleh aplikasi atau juga dapat menulis kuncinya sendiri.

Gambar 7. Masukan Kunci Enkripsi Catatan

3. Lihat Catatan

Catatan telah berhasil disimpan pada proses sebelumnya, selanjutnya untuk melihat catatan yang tersimpan, dan klik salah satu catatan lebih tepatnya catatan yang sebelumnya dibuat, lalu akan diarahkan ke *form detail* catatan, seperti yang dilihat isi catatan yang ditampilkan isi catatan yang terenkripsi, untuk mengembalikan ke teks asli penulis dapat menggunakan fitur dekripsi catatan dengan mengklik ikon garis tiga di sudut kanan atas.

Gambar 8. Lihat Catatan

Dialog untuk mengimpor kunci catatan akan muncul ketika ingin meng dekripsi catatan, pesan dialog untuk impor kunci tidak hanya muncul ketika meng dekripsi catatan, tetapi juga muncul ketika fitur ubah catatan dan hapus catatan di klik. Impor kunci dengan kunci yang sebelumnya berhasil diekspor, jika benar kunci yang diimpor, catatan akan didekripsi seperti yang lihat pada gambar dibawah, teks catatan kembali ke teks asli.

Gambar 9. Catatan Berhasil di Dekripsi

Tabel 3. Hasil Pengujian *Black Box*

No	Fungsi	Output	Hasil
1.	Menu utama menampilkan semua catatan	Semua data yang disimpan berhasil ditampilkan di menu utama	Sesuai
2.	Masukan Kunci catatan dan ekspor kunci catatan	Kunci catatan bisa di *input dan* kunci catatan berhasil di ekspor	Sesuai
3.	Tambah catatan dan simpan catatan	Catatan berhasil disimpan	Sesuai
4.	Lihat Catatan	Catatan yang berhasil disimpan dapat bisa dilihat	Sesuai
5.	Dekripsi catatan	Catatan yang dienkripsi dapat didekripsi	Sesuai
6.	Ubah catatan	Catatan bisa diubah dan berhasil disimpan	Sesuai
7.	Hapus catatan	Catatan berhasil dihapus	Sesuai
8.	Penanganan kesalahan yang mungkin pengguna lakukan	Pengguna menginputkan kunci seluruhnya dengan spasi pesan kesalahan ditampilkan dan pengguna menginputkan kunci yang salah pesan kesalahan ditampilkan	Sesuai

4. KESIMPULAN

Setelah melalui tahapan tahapan yang telah dijelaskan pada pembahasan sebelumnya maka dapat ditarik kesimpulan:

1. Aplikasi enkripsi teks catatan telah mencapai tujuan utama dari sistem yaitu dapat melakukan pengamanan teks catatan menggunakan algoritma *Vigenere Cipher* dan *Atbash Cipher.*
2. Dengan ditambahnya fitur enkripsi teks pada aplikasi catatan, teks catatan dapat lebih terjaga kerahasiaannya, sehingga teks catatan tidak dapat diketahui oleh pihak yang tidak bertanggung jawab.

5. SARAN

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

1. Untuk fitur enkripsi teksnya algoritma *Vigenere Cipher* atau *Atbash Cipher* bukanlah satu-satunya metode yang dapat digunakan, alangkah lebih baik pada penelitian selanjutnya dicoba untuk menggunakan penggabungan algoritma lain yang tentunya lebih modern.
2. Aplikasi membutuhkan pengembangan lebih lanjut agar aplikasi lebih sempurna, penulis berharap pada pengembangan selanjutnya dapat menambahkan fitur-fitur lainnya seperti bisa menyimpan gambar, mensinkronisasikan catatan.

UCAPAN TERIMA KASIH

Penulis mengucapkan terima kasih kepada keluarga penulis dan Universitas Potensi Utama yang telah memberi dukungan terhadap penelitian ini.

DAFTAR PUSTAKA

[1] Yusfrizal, Y. (2019). RANCANG BANGUN APLIKASI KRIPTOGRAFI PADA TEKS MENGGUNAKAN METODE REVERSE CHIPER DAN RSA BERBASIS ANDROID. *JTIK (Jurnal Teknik Informatika Kaputama)*, *3*(2), 29-37.

[2] Kharisma, R. S., & Rachman, M. A. F. (2017). Pembuatan Aplikasi Notes Menggunakan Algoritma Kriptografi Polyalphabetic Substitution Cipher Kombinasi Kode Ascii Dan Operasi Xor Berbasis Android. *Respati*, *12*(2).

[3] Situmorang, B. H., Sinurat, S., & Tampubolon, K. (2018). IMPLEMENTASI ALGORITMA ATBASH UNTUK MENYANDIKAN PESAN TEKS BERBASIS ANDROID. *Pelita Informatika: Informasi dan Informatika*, *7*(2), 394-398.

[4] Permana, A. A. (2018). Penerapan Kriptografi Pada Teks Pesan dengan Menggunakan Metode Vigenere Cipher Berbasis Android. *Jurnal Al-Azhar Indonesia Seri Sains dan Teknologi*, *4*(3), 110-115.

[5] Abdullah, D., & Surnihayati, S. (2017). PENGAMANAN EMAIL MENGGUNAKAN METODE VIGENERE CIPHER. *Journal of Information System, Applied, Management, Accounting and Research*, *1*(1), 1-9.