Pengembangan Aplikasi *Parental Control* Berbasis Android Menggunakan Kriptografi *Vigenere Cipher* pada *Pattern Lock*

Rifqi Ramadhani Muhammad[*1)], Nurdin Bahtiar, S.Si, M.T[*2)]

[*]Departemen Ilmu Komputer / Informatika, Universitas Diponegoro
[1)]rifqi.ramadhani.m@gmail.com, [2)]nurdinbahtiar@gmail.com

Abstrak

Parental Control merupakan aktivitas pengawasan seseorang terhadap anak dalam bermain teknologi smartphone. Di samping itu, perkembangan teknologi khususnya smartphone telah mengalami peningkatan pesat yang dapat dilihat pada penggunaannya secara praktis, karena dapat meningkatkan produktifitas jika digunakan dengan optimal. Sebaliknya, penggunaan smartphone juga dapat mengakibatkan dampak buruk apabila digunakan dengan tidak semestinya. Hal tersebut kerap terjadi secara berlebihan khususnya pada penggunaan smartphone oleh anak. Apabila hal tersebut dibiarkan secara terus menerus dapat berdampak terhadap psikologis dan tentunya akan menganggu perkembangannya. Orang tua sebagai pengawas tumbuh kembang anak perlu melakukan pengendalian penggunaan smartphone sesuai dengan usia anak mereka. Untuk dapat melakukan pengendalian penggunaan smartphone tersebut maka dibangun sebuah aplikasi Parental Control yang menggunakan sistem keamanan Pattern Lock dengan mengimplementasikan algoritma Vigenere Cipher di dalam pembentukan pola Pattern Lock. Vigenere Cipher merupakan algoritma kriptografi yang dapat digunakan untuk mengamankan data atau karakter pola dimana algoritmanya adalah mengenkripsi data karakter di dalam pola Pattern Lock yang telah dikonversi menjadi karakter alfabet, sehingga keamanan dari informasi sistem login tersebut dapat ditingkatkan. Di dalam aplikasi ini pengguna dapat mengunci aplikasi ter-install pada smartphone Android, sehingga apabila aplikasi terkunci dijalankan, pengguna diharuskan memasukkan kunci dengan benar melalui Pattern Lock screen. Pada saat menghubungkan noda pada Pattern Lock, waktu yang dibutuhkan untuk membentuk pola kunci terenkripsi tidak lama. Dengan menghubungkan dua noda paling cepat memerlukan waktu 2 mili detik dan dengan menghubungkan maksimal sembilan noda memerlukan waktu paling lama 38 mili detik.

Kata kunci : *Vigenere Cipher, Pattern Lock, Parental Control, Smartphone Android*

Abstract

Parental Control is a person's supervisory activity towards children in playing smartphone technology. Besides that, the development of technology, especially smartphones has increased rapidly which can be seen in practical use, because it can increase productivity if used optimally. Instead, smartphone use can also cause adverse effects if used improperly. This often happens to excessive, especially in the use of smartphones by children. If this is allowed continuously, it can have an impact on the child's psychological condition and will certainly disrupt the child's development. Parents as supervisors for child development need to control smartphone usage according to their child's age. To be able to control smartphone usage, a Parental Control application is built that uses the Pattern Lock security system by implementing the Vigenere Cipher algorithm in forming Pattern Lock patterns. Vigenere Cipher is a cryptographic algorithm that can be used to

secure data or character patterns where the algorithm is to encrypt characters data in the Pattern Lock pattern that has been converted into alphabetical characters, so that the security of the login system information can be increased. In this application the user can lock the installed application on an Android smartphone, so that when the locked application is executed, the user is required to enter the key correctly through the Pattern Lock screen. When connecting the dots in Pattern Lock, the time needed to form an encrypted key pattern is not long. By connecting two dots, the fastest time takes 2 milli seconds, and by connecting a maximum of nine dots, it takes a maximum of 38 milli seconds.

Keywords : *Vigenere Cipher, Pattern Lock, Parental Control, Android Smartphone*

1 PENDAHULUAN

Dewasa ini, keperawatan anak telah mengalami pergeseran yang sangat mendasar [13]. Beberapa kasus yang sering dijumpai di masyarakat, seperti peristiwa yang dapat menimbulkan trauma pada anak, antara lain cemas, marah, dan lain-lain akibat penggunaan *gadget*. *Gadget* tersebut bukan hanya aplikasi tentang pembelajaran mengenal huruf atau gambar, tetapi terdapat aplikasi hiburan, seperti *video*, *video game*, bahkan sosial media [14]. Pada kenyataannya, anak-anak akan lebih sering menggunakan *gadget*-nya untuk bermain *game* daripada untuk belajar ataupun bemain di luar rumah dengan teman-teman seusianya [8]. Apabila hal tersebut dibiarkan secara terus menerus dapat berdampak terhadap psikologis anak dan tentunya akan mengganggu perkembangan anak. Dan kegiatan tersebut dapat menimbulkan trauma apabila dilakukan tanpa pengawasan. Padahal, perhatian khusus kepada anak sebagai individu yang masih dalam usia perkembangan tentu tidak kalah pentingnya, karena masa kanak-kanak merupakan proses menuju kematangan [13].

Dengan berkembangnya teknologi, proses keperawatan anakpun mengalami perkembangan. Proses tersebut adalah pengawasan penggunaan teknologi khususnya *gadget* terhadap anak. Orang tua diwajibkan mengawasi tumbuh kembang anak sesuai usia anak. Apabila anak dibiarkan bebas menggunakan *gadget* tidak sesuai kebutuhannya, maka akan berdampak terhadap psikologis anak dan tentunya mengganggu perkembangan anak. Selain kebutuhan fisiologis, anak juga individu yang membutuhkan kebutuhan psikologis, sosial dan spiritual. Sedangkan anak dikatakan sejahtera jika anak tidak merasakan gangguan psikologis, seperti rasa cemas, takut maupun lain-lain.

Pada teknologi *gadget*, *gadget* sendiri dapat digunakan sebagai alat pengawasan terhadap penggunaan *gadget* oleh anak, yaitu membatasi penggunaan aplikasi pada *gadget smartphone*. Pada penelitian sebelumnya dilakukan studi mengenai implementasi algoritma kriptografi dalam suatu teknologi perangkat *mobile*, dalam hal ini yaitu platform Android. Penerapan kriptografi dalam *mobile platform* telah cukup banyak digunakan berkaitan dengan aspek keamanan, aspek inilah yang sangat diperlukan dalam aktivitas *mobile* tersebut [5].

Kriptografi adalah ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan, integritas data, serta otentikasi. Ilmu sandi (kriptografi) sendiri telah ada sejak lama.

Tercatat dalam sejarah bahwa Julius Caesar, seorang kaisar Romawi menggunakan penyandian untuk menyampaikan pesan rahasia saat perang [6].

Penggunaan kriptografi pada sistem keamanaan aplikasi android yang akan diimplementasikan pada tugas akhir ini adalah metode *Vigenere Cipher*. Dalam tugas akhir ini metode *Vigenere Cipher* akan digunakan sebagai enkriptor sandi pada aplikasi android yang akan dihasilkan. *Vigenere Cipher* sendiri sebenarnya merupakan pengembangan dari sandi Caesar. Pada sandi Caesar, setiap huruf pada teks digantikan dengan huruf lain yang memiliki perbedaan tertentu pada urutan alfabet. Misalnya pada sandi Caesar dengan geseran 3, A menjadi D, B menjadi E dan seterusnya. Sandi *Vigenere* terdiri dari beberapa sandi Caesar dengan nilai geseran yang berbeda.

Kriptografi merupakan metode yang banyak dikembangkan dan digunakan dalam pembuatan aplikasi. Metode kriptografi yang banyak digunakan adalah *Blockcipher* dan *Vigenere Cipher*. *Vigenere Cipher* pernah digunakan untuk membuat sistem keamanan data pelanggan dengan menggunakan teknik enkripsi [2]. Pengembangan sistem menggunakan metode *Vigenere Cipher* dapat membuat suatu pesan rahasia tidak mudah dibaca langsung bagi orang lain. Pengirim pesan teks asli berupa suatu kalimat yang dienkripsi oleh kriptosistem untuk mengacak pesan aslinya dengan memberikan kunci menjadi *cipher*text dan dapat dikembalikan ke pesan aslinya atau didekripsikan [4]. Penggunaan kriptografi pada pesan sms, pada penerapannya teks sms akan di tukar dengan karakter yang bersesuaian dengan kunci yang di-*input*-kan *user*, karakter *plaintext* akan diproses dengan karakter dari kunci dengan indeks yang sama untuk menghasilkan karakter baru. Dalam hal ini karakter baru yang mungkin muncul adalah sebanyak 26 karakter dalam tabel ASCII sehingga diharapkan lebih aman daripada metode *vigenere* asli dan untuk membacanya *user* harus meng-*input*-kan kunci yang sama dengan kunci yang digunakan untuk proses enkripsi agar pesan kembali ke bentuk semula [7].

Berkenaan dengan data yaitu pesan atau karakter dan informasi yang dapat disimpan pada *gadget* khususnya *smartphone*, *smartphone* saat ini juga digunakan untuk mengakses surat dan terhubung ke media sosial, itu diperlukan untuk memastikan keamanan data dan informasi yang disimpan di ponsel [1]. Bahkan pada media *offline*, seperti keamaan *smartphone* sendiri dapat menggunakan sistem keamanan seperti *lock screen* dan *pattern lock* atau yang lainnya. *Pattern Lock* adalah salah satu mekanisme perlindungan *login* dalam sistem Android untuk membuka kunci layar. Dengan menghubungkan 4-9 titik dalam *grid* 3x3, pengguna dapat mengatur pola buka kunci yang setara dengan kata sandi atau PIN (Sun, Wang, & Zheng, 2014). Dengan menggunakan layar *pattern lock*, data kunci yang didapat dari pembentukan pola *pattern lock* dapat digunakan sebagai data yang dapat diolah menjadi karakter lain. Pada dasarnya pembentukan pola *pattern lock* Android hanya menggunakan karakter 1-9 sesuai titik *pattern lock*.

Dengan menggunakan Kriptografi *Vigenere Cipher* data karakter pada nilai titik *pattern lock* dapat dienkripsikan menjadi nilai atau karakter baru. Meskipun hasil enkripsi *Vigenere Cipher* dapat dipecahkan dengan dengan teknik *brute force attack*, tetapi memerlukan waktu lama untuk memecahkan susunan karakter yang

telah terenkripsi. Untuk meningkatkan keamanan atau hasil enkripsi yang lebih kuat maka harus dibentuk sisipan kunci yang lebih panjang di dalam perhitungan enkripsi pada algoritm *Vigenere Cipher*. Untuk dapat meningkatkan keamanan sistem *login* pada *pattern lock*, dalam tugas akhir ini penulis melakukan pembangunan aplikasi pada sistem keamanan aplikasi ter-*install* di dalam *smartphone*, yaitu dengan menggabungkan nilai titik *pattern lock* terhadap algoritma *Vigenere Cipher*. Nilai titik tersebut diubah menjadi karakter alfabet kemudian dilakukan enkripsi karakter menggunakan *Vigenere Cipher*, sehingga sistem keamanan *login* pada *pattern lock* dapat ditingkatkan. Disamping penggunaan *pattern lock* sebagai sistem keamanan *login*, aplikasi ini membantu orang tua dalam mengawasi kegiatan anak dalam menggunakan *smartphone*, yaitu dengan mengunci aplikasi ter-*install* yang dalam penggunaannya melalui verifikasi *pattern lock.*

Berdasarkan latar belakang masalah yang telah dijelaskan maka dapat disusun suatu rumusan masalah yakni bagaimana membuat suatu aplikasi yang dapat mengunci aplikasi android dengan menggunakan metode *Vigenere Cipher* sebagai *Parental Control* untuk membatasi penggunaan aplikasi yang tidak sesuai usia anak.

Tujuan yang dicapai dari Tugas Akhir ini adalah menghasilkan aplikasi *Parental Control* berbasis Android menggunakan algoritma *Vigenere Cipher* untuk membatasi penggunaan aplikasi yang tidak sesuai dengan usia anak.

2 TINJAUAN PUSTAKA

2.1. KRIPTOGRAFI

Kriptografi adalah ilmu dan seni untuk menjaga kerahasiaan pesan dengan cara menyandikannya ke dalam bentuk yang tidak dapat dimengerti lagi maknanya. Dalam ilmu kriptografi, terdapat dua buah proses yaitu melakukan enkripsi dan dekripsi. Pesan yang akan dienkripsi disebut sebagai *plaintext*. Disebut demikian karena informasi ini dengan mudah dapat dibaca dan dipahami oleh siapa saja. Algoritma yang dipakai untuk mengenkripsi dan mendekripsi sebuah *plaintext* melibatkan penggunaan suatu bentuk kunci. Pesan *plaintext* yang telah dienkripsi dikenal sebagai *ciphertext* [9].

Dalam kriptografi terdapat istilah sebagai berikut [9]:

1. Pesan, *Plaintext* dan *Ciphertext*

   Pesan adalah data atau informasi yang dapat dibaca dan dimengerti maknanya. Nama lain untuk pesan adalah atau teks jelas.

2. Pengirim dan Penerima

   Komunikasi data melibatkan pertukaran pesan antara dua entitas. Pengirim adalah entitas yang mengirim pesan kepada entitas lainnya. Penerima adalah entitas yang menerima pesan.

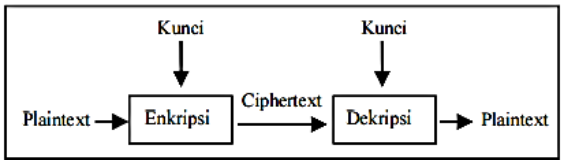
3. Enkripsi dan dekripsi

   Proses menyandikan *plaintext* menjadi *ciphertext* disebut enkripsi atau *enciphering* (nama standar menurut ISO 7498-2). Sedangkan proses mengembalikan *ciphertext* menjadi *plaintext* semula disebut dekripsi atau *deciphering* (nama standar menurut ISO 7498-2).

4. *Cipher* dan kunci

   Algoritma kriptogarfi disebut juga *cipher*, yaitu aturan untuk enkripsi dan dekripsi atau fungsi matematika yang digunakan untuk enkripsi dan dekripsi. Beberapa *cipher* memerlukan algoritma yang berbeda untuk enkripsi dan dekripsi.

Proses enkripsi dan dekripsi *cipher* dapat dilihat pada Gambar 1.



Gambar 1 Skema Enkripsi dan Dekripsi Menggunakan Kunci [9]

2.2. *VIGENERE CIPHER*

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 digunakann untuk memperoleh *ciphertext* berdasarkan kunci yang sudah ditentukan [10].

2.2.1. Proses Enkripsi *Vigenere Cipher*

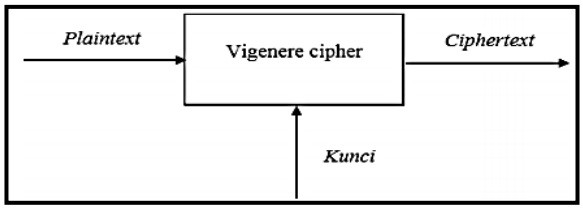
Proses enkripsi menggunakan *Vigenere cipher* membutuhkan 1 buah kunci untuk dapat menghasilkan *ciphertext*. Kunci yang digunakan merupakan sebuah kata atau susunan dari beberapa huruf.

Persamaan enkripsi *plaintext* dapat dilihat pada persamaan 1 dan dapat dijelaskan sebagai berikut:

$$Ci = (Pi + Kr) \bmod 26 \qquad (1)$$

Ci = *ciphertext* dari pergeseran karakter yang terdapat pada *plaintext*.
Pi = pergeseran karakter pada *plaintext*.
Kr = kunci berupa hasil konversi tabel berbentuk bilangan desimal dari pergeseran karakter yang terdapat pada kunci yang digunakan.

Gambaran proses enkripsi *Vigenere Cipher* dapat dilihat pada Gambar 2.



Gambar 2 Proses Enkripsi *Vigenere Cipher* [10]

2.2.2. Proses Dekripsi *Vigenere Cipher*

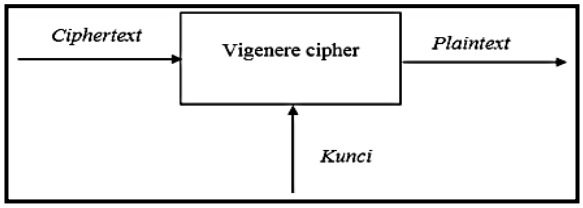
Proses dekripsi menggunakan *Vigenere cipher* membutuhkan satu buah kunci untuk dapat menghasilkan *plaintext*. Kunci yang digunakan merupakan sebuah kata atau susunan dari beberapa huruf.

Persamaan enkripsi *plaintext* dapat dilihat pada persamaan 2 dan dapat dijelaskan sebagai berikut:

$$Pi = ((Ci - Kr) + 26) \bmod 26 \qquad (2)$$

Pi = *plaintext* dari pergeseran karakter yang terdapat pada *ciphertext*.
Ci = pergeseran karakter pada *ciphertext*.
Kr = kunci berupa hasil konversi tabel berbentuk bilangan desimal dari pergeseran karakter yang terdapat pada kunci yang digunakan.

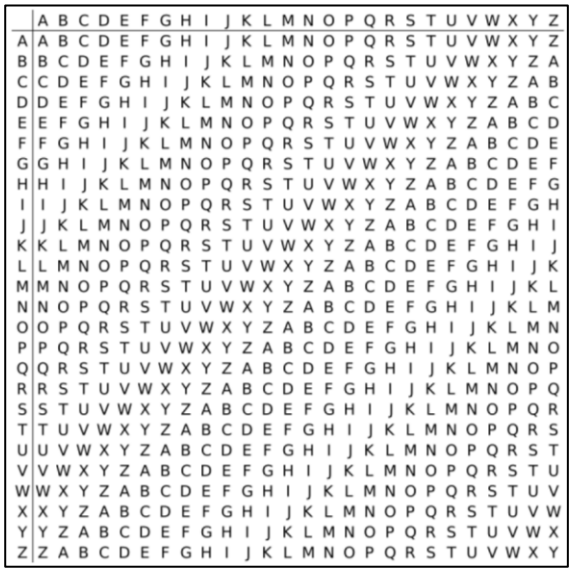
Gambaran proses enkripsi *Vigenere Cipher* dapat dilihat pada Gambar 3.



Gambar 3 Proses Dekripsi *Vigenere Cipher* [10]

Vigenere cipher pada dasarnya memiliki karakteristik yang terletak pada cara membentuk tabel atau cara menghasilkan kuncinya, sedangkan enkripsi dan dekripsi tidak berbeda dengan *vigenere cipher* standar. Berdasarkan langkah pembentukan enkripsi, huruf pada kunci akan dikonversi menjadi sebuah nilai, misalnya A = 0, B = 1, sampai dengan Z = 25. Setelah itu prosesnya sama seperti pada

Caesar *cipher* dimana setiap huruf pada plainteks akan digeser sejauh nilai kunci yang posisinya bersesuaian. Pergeseran huruf-huruf ini bisa dipetakan dalam bentuk tabel 26x26 yang memetakan antara huruf pada plainteks dengan huruf pada kunci seperti yang di-perlihatkan pada Gambar 4 [3]:



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

Gambar 4 Tabel Pemetaan *Vigenere Cipher* [3]

2.3. *PARENTAL CONTROL*

Parental control adalah layanan bantu orang tua yang bersangkutan mengontrol anak-anak mereka mengakses melalui *web* ataupun dari perangkat selular lainnya [11]. Salah satu yang dapat dilakukan oleh orang tua untuk mengawasi anaknya adalah dengan mengontrol aktivitas anak dalam bermain *gadget*. Pengawasan ini adalah bentuk pengendalian sosial.

Pengendalian sosial dapat dilakukan oleh individu terhadap individu, individu terhadap suatu kelompok sosial, maupun dilakukan oleh suatu kelompok terhadap kelompok lainnya, atau suatu kelompok terhadap individu. Itu semua merupakan proses pengendalian sosial yang dapat terjadi dalam kehidupan sehari-hari, meskipun sering kali manusia tidak menyadari.

2.4. APLIKASI *PARENTAL CONTROL*

Aplikasi *Parental Control* merupakan alat bantu orang tua yang membatasi kegiatan pada anak, dimana aplikasi *Parental Control* umum digunakan pada pengaksesan situs internet dan *control* siaran televisi [11]. Dengan adanya fitur *parental control*, orang tua dapat memanfaatkan fitur pembatasan penggunaan aplikasi. Jenis aplikasi yang dibatasi penggunaannya adalah aplikasi browser, sosial media, *tools*, berita, majalah, dan hiburan.

Aplikasi hiburan yang dibatasi adalah aplikasi yang memiliki *content rating* pada usia di atas usia anak. *Content rating* tersebut juga dapat dilihat di dalam aplikasi PlayStore. *Content rating* sendiri sangat penting agar dapat membantu pengguna, khususnya orang tua untuk mengidentifikasi kemungkinan konten yang tidak pantas dalam aplikasi.

2.5. *PATTERN LOCK*

Andorid *Pattern* merupakan bentuk keamanan yang terdapat di dalam telepon selular bersistem operasi Android. Android *Pattern* akan mengunci sistem selama *user* tidak memberikan pola yang tepat seperti yang sudah disimpan pada sistem sebelumnya. Pola merupakan representasi dari *password*, dan dibuat dengan menghubungkan sembilan titik yang ada.

Pada tahapan awal, user haruslah membuat pola yang akan dijadikan sebagai pola kunci. Pola tersebut merupakan penghubungan dari titik dengan maksimal sembilan buah titik. Tidak ada satupun titik yang dihubungkan dua kali ataupun lebih.

Selanjutnya, setelah pola utama tersimpan, setiap kali user akan menggunakan telepon seluler tersebut, *user* harus memasukkan pola yang dibuatnya tersebut. Kesalahan dalam memasukkan pola akan menyebabkan user tidak dapat

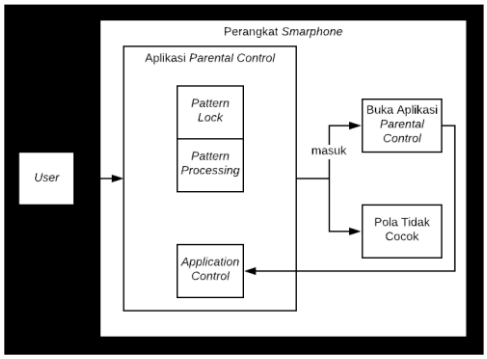
mengakses fitur-fitur yang ada dalam telepon selular tersebut.

3 METODE PENELITIAN

3.1. *Requirement*

Aplikasi *Parental Control* berbasis Android menggunakan Kriptografi *Vigenere Cipher* pada *Pattern Lock* ini membutuhkan perangkat *smartphone* Android dengan sistem operasi diatas versi Android Oreo atau dengan API Level 27 keatas dan memerlukan halaman *pattern lock* sebagai *system login view*. Dalam *pattern lock* ini akan dilakukan enkripsi pola kunci yang dimasukkan *user*.

Dalam pembangunan Aplikasi *Parental Control* digunakan *platform* Android sebagai dasar pembangunan aplikasinya. Ada tiga komponen penting dalam aplikasi Android yakni *View*, *Model*, *Control*. Aplikasi ini akan berhubungan dengan aplikasi ter-*install* pada *smartphone* Android untuk dapat mengakses informasi kerja aplikasi ter-*install*. Arsitektur Aplikasi *Parental Control* dapat dilihat pada Gambar 5.



Gambar 5 Arsitektur Aplikasi *Parental Control*

3.2. Deskripsi Umum Perangkat Lunak

Aplikasi *Parental Control* adalah sebuah aplikasi yang menyediakan fasilitas bagi orang tua untuk membatasi penggunaan *smartphone* terhadap anak dengan cara mengunci aplikasi tertentu pada aplikasi ter-*install*. Untuk dapat menjalankan aplikasi terkunci, pengguna *smartphone* harus memasukkan pola kunci yang benar melalui *pattern lock*. Pengguna aplikasi adalah orang tua, dimana orang tua dalam menggunakan aplikasi ini dapat mengelola aplikasi ter-*install* dan dapat melakukan ubah pola kunci pada menu aplikasi.

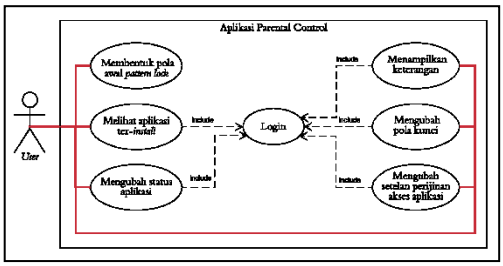
3.3. Analisis Kebutuhan Sistem

Terdapat tujuh *Use Case* dalam pengembangan Aplikasi *Parental Control* seperti diuraikan pada Tabel 1.

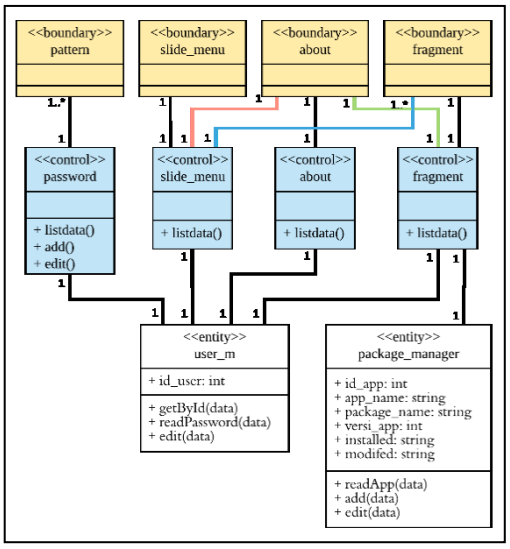
Tabel 1 Definisi *Use Case*

No	Kode *Use Case*	Nama *Use Case*
1.	Membentuk pola awal *pattern lock*	*User* dapat melihat tampilan *pattern lock* yang digunakan untuk membentuk pola awal kunci.
2.	M*elakukan Login*	*User* dapat *login* menggunakan sandi *pattern lock.*
3.	Menampilkan aplikasi ter-*install*	*User* dapat menampilkan aplikasi ter-*install*.
4.	Mengubah status aplikasi	*User* dapat mengubah status aplikasi yang akan dikunci atau tidak dikunci.
5.	Mengubah pengaturan *permit drawing over app* dan *usage access permission*	*User* dapat mengubah pengaturan pada penggunaan fitur penguncian aplikasi dalam
6.	Mengubah pola kunci tersimpan	*User* dapat mengubah pola *pattern lock* tersimpan yang telah dibentuk.
7.	Menampilkan keterangan aplikasi *Parental Control*	*User* dapat melihat keterangan Aplikasi *Parental Control*

Diagram *use case* menjelaskan apa yang dilakukan oleh sistem dan siapa yang berinteraksi dengan sistem. Diagram *use case* pada Aplikasi *Parental Control* dapat dilihat pada Gambar 6, sedangkan pemodelan *class diagram* Aplikasi *Parental Control* disajikan pada Gambar 7.



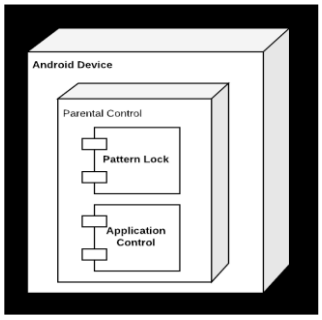
Gambar 6 *Use Case Diagram*



Gambar 7 Pemodelan *Class Diagram*

3.4. *Deployment Diagram*

Deployment Diagram berisikan perangkat yang digunakan pada aplikasi. Terdapat komponen yang diperlukan dalam menjalankan Aplikasi *Parental Control* yaitu Android Device dan Aplikasi *Parental Control* yang membutuhkan *Pattern Lock* dan *Application Control*. Komponen *Pattern Lock* dan *Application Control* berhubungan langsung dengan *User* melalui Aplikasi *Parental Control*. Perhitungan algoritma *Vigenere Cipher* disimpan di dalam komponen *Pattern Lock*. Deployment Diagram Aplikasi dapat dilihat pada Gambar 8.



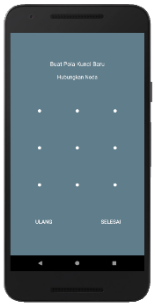
Gambar 8 *Deployment Diagram*

4 HASIL DAN PEMBAHASAN

Bagian ini menjelaskan mengenai kebutuhan perangkat lunak yang akan dibangun pada uraian *Implementation* (Implementasi) dan *Testing* (Pengujian). Aplikasi *Parental Control* dibangun menggunakan Bahasa pemrograman Java melalui IDE Android Studio.

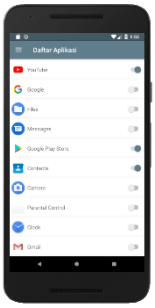
4.1. Implementasi Antarmuka

Implementasi antarmuka Aplikasi *Parental Control* disajikan pada Gambar 9 sampai 11.



Gambar 9 Antarmuka Membentuk Pola Awal *Pattern Lock*

Gambar 10 Antarmuka Mengubah Pola Kunci Tersimpan



Gambar 11 Antarmuka Mengubah Status Aplikasi

4.2. Pengujian

Pengujian Aplikasi *Parental Control* berbasis Android dilakukan dengan metode *blackbox,* yaitu melakukan pengujian fungsionalitas dari perangkat lunak untuk menemukan kesalahan pada *requirement* dengan mengabaikan mekanisme internal atau komponen dari program.

Berdasarkan hasil uji yang telah disajikan sebelumnya, dapat dilihat bahwa semua pengujian pada Aplikasi *Parental Control* berbasis Android dapat diterima. Pada saat pengujian, Aplikasi *Parental Control* dapat berjalan sesuai yang diharapkan.

Tabel 2 Percobaan Pembentukan Dua Noda Pola Kunci

No	Noda *pattern lock*	*Plaintext*	*Ciphertext*	Lama Eksekusi (mili detik)
1.	1, 2	ABCDEFGHIJ	ACEGIFHJLN	3
2.	2, 3	FGHIJKLMNO	FHJLNKMOQS	4
3.	3, 4	KLMNOPQRST	KMOQSPRTVX	6
4.	4, 5	PQRSTUVWXY	PRTVXUWYAC	10
5.	5, 6	UVWXYZABCD	UWYACZBDFH	9
6.	6, 7	ZABCDEFGHI	ZBDFHEGIKM	8
7.	7, 8	EFGHIJKLMN	EGIKMJLNPR	12
8.	8, 9	JKLMNOPQRS	JLNPROQSUW	3
9.	9, 2	OPQRSFGHIJ	OQSUWFHJLN	3
10.	1, 4	ABCDEPQRST	ACEGIPRTVX	6
11.	2, 5	FGHIJUVWXY	FHJLNUWYAC	5
12.	3, 6	KLMNOZABCD	KMOQSZBDFH	8
13.	4, 7	PQRSTEFGHI	PRTVXEGIKM	12
14.	5, 8	UVWXYJKLMN	UWYACJLNPR	3
15.	6, 9	ZABCDOPQRS	ZBDFHOQSUW	10
16.	7, 4	EFGHIPQRST	EGIKMPRTVX	7
17.	8, 5	JKLMNUVWXY	JLNPRUWYAC	6
18.	9, 6	OPQRSZABCD	OQSUWZBDFH	7
19.	1, 5	ABCDEUVWXY	ACEGIUWYAC	2
20.	2, 6	FGHIJZABCD	FHJLNZBDFH	5
21.	3, 4	KLMNOPQRST	KMOQSPRTVX	11
22.	4, 8	PQRSTJKLMN	PRTVXJLNPR	14
23.	5, 9	UVWXYOPQRS	UWYACOQSUW	4
24.	6, 7	ZABCDEFGHI	ZBDFHEGIKM	5
25.	7, 5	EFGHIUVWXY	EGIKMUWYAC	8
26.	8, 6	JKLMNZABCD	JLNPRZBDFH	8
27.	9, 4	OPQRSPQRST	OQSUWPRTVX	5
28.	1, 8	ABCDEJKLMN	ACEGIJLNPR	10
29.	3, 8	KLMNOJKLMN	KMOQSJLNPR	13
30.	7, 2	EFGHIFGHIJ	EGIKMFHJLN	6

Tabel 3 Percobaan Pembentukan Sembilan Noda Pola Kunci

No	Noda *pattern lock*	*Plaintext*	*Ciphertext*	Lama Eksekusi (mili detik)
1.	1, 2, 3, 4, 5, 6, 7, 8, 9	ABCDEFGHIJKLMNOPQRSTUVWXYZABCDEFGHIJKLMNOPQRS	ACEGIFHJLNKMOQSPRTVXUWYACZBDFHEGIKMJLNPROQSUW	20
2.	4, 5, 6, 7, 8, 9, 1, 2, 3	PQRSTUVWXYZABCDEFGHIJKLMNOPQRSABCDEFGHIJKLMNO	PRTVXUWYACZBDFHEGIKMJLNPROQSUWACEGIFHJLNKMOQS	38
3.	7, 8, 9, 5, 1, 2, 3, 4, 6	EFGHIJKLMNOPQRSUVWXYABCDEFGHIJKLMNOPQRSTZABCD	EGIKMJLNPROQSUWUWYACACEGIFHJLNKMOQSPRTVXZBDFH	17
4.	1, 2, 3, 5, 7, 8, 9, 4, 6	ABCDEFGHIJKLMNOUVWXYEFGHIJKLMNOPQRSPQRSTZABCD	ACEGIFHJLNKMOQSUWYACEGIKMJLNPROQSUWPRTVXZBDFH	30

No	Noda *pattern lock*	*Plaintext*	*Ciphertext*	Lama Eksekusi (mili detik)
5.	4, 5, 6, 1, 2, 3, 7, 8, 9	PQRSTUVWXYZABCDAB CDEFGHIJKLMNOEFGHIJ KLMNOPQRS	PRTVXUWYACZBDFHAC EGIFHJLNKMOQSEGIKMJ LNPROQSUW	24
6.	7, 8, 9, 4, 5, 6, 1, 2, 3	EFGHIJKLMNOPQRSPQRS TUVWXYZABCDABCDEF GHIJKLMNO	EGIKMJLNPROQSUWPRT VXUWYACZBDFHACEGIF HJLNKMOQS	23
7.	1, 2, 3, 6, 5, 4, 7, 8, 9	ABCDEFGHIJKLMNOZAB CDUVWXYPQRSTEFGHIJ KLMNOPQRS	ACEGIFHJLNKMOQSZBDF HUWYACPRTVXEGIKMJL NPROQSUW	19
8.	4, 5, 6, 9, 8, 7, 1, 2, 3	PQRSTUVWXYZABCDOP QRSJKLMNEFGHIABCDEF GHIJKLMNO	PRTVXUWYACZBDFHOQ SUWJLNPREGIKMACEGIF HJLNKMOQS	17
9.	7, 8, 9, 6, 3, 2, 1, 4, 5	EFGHIJKLMNOPQRSZABC DKLMNOFGHIJABCDEPQ RSTUVWXY	EGIKMJLNPROQSUWZBD FHKMOQSFHJLNACEGIPR TVXUWYAC	30
10.	1, 2, 3, 6, 9, 8, 7, 4, 5	ABCDEFGHIJKLMNOZAB CDOPQRSJKLMNEFGHIPQ RSTUVWXY	ACEGIFHJLNKMOQSZBDF HOQSUWJLNPREGIKMPR TVXUWYAC	14
11.	4, 5, 6, 3, 2, 1, 7, 8, 9	PQRSTUVWXYZABCDKL MNOFGHIJABCDEEFGHIJ KLMNOPQRS	PRTVXUWYACZBDFHKM OQSFHJLNACEGIEGIKMJ LNPROQSUW	16
12.	7, 8, 9, 6, 5, 4, 1, 2, 3	EFGHIJKLMNOPQRSZABC DUVWXYPQRSTABCDEF GHIJKLMNO	EGIKMJLNPROQSUWZBD FHUWYACPRTVXACEGIF HJLNKMOQS	20
13.	1, 2, 3, 6, 9, 8, 7, 5, 4	ABCDEFGHIJKLMNOZAB CDOPQRSJKLMNEFGHIU VWXYPQRST	ACEGIFHJLNKMOQSZBDF HOQSUWJLNPREGIKMUW YACPRTVX	16
14.	4, 5, 6, 3, 2, 1, 9, 8, 7	PQRSTUVWXYZABCDKL MNOFGHIJABCDEOPQRSJ KLMNEFGHI	PRTVXUWYACZBDFHKM OQSFHJLNACEGIOQSUWJ LNPREGIKM	25
15.	7, 8, 9, 6, 5, 4, 3, 2, 1	EFGHIJKLMNOPQRSZABC DUVWXYPQRSTKLMNOF GHIJABCDE	EGIKMJLNPROQSUWZBD FHUWYACPRTVXKMOQS FHJLNACEGI	19
16.	1, 2, 3, 4, 5, 6, 9, 8, 7	ABCDEFGHIJKLMNOPQRS TUVWXYZABCDOPQRSJK LMNEFGHI	ACEGIFHJLNKMOQSPRTV XUWYACZBDFHOQSUWJ LNPREGIKM	14
17.	4, 5, 6, 7, 8, 9, 3, 2, 1	PQRSTUVWXYZABCDEFG HIJKLMNOPQRSKLMNOF GHIJABCDE	PRTVXUWYACZBDFHEGI KMJLNPROQSUWKMOQS FHJLNACEGI	16
18.	7, 8, 9, 5, 1, 2, 3, 6, 4	EFGHIJKLMNOPQRSUVW XYABCDEFGHIJKLMNOZ ABCDPQRST	EGIKMJLNPROQSUWUWY ACACEGIFHJLNKMOQSZ BDFHPRTVX	19
19.	1, 2, 3, 6, 7, 8, 9, 4, 5	ABCDEFGHIJKLMNOZAB CDEFGHIJKLMNOPQRSPQ RSTUVWXY	ACEGIFHJLNKMOQSZBDF HEGIKMJLNPROQSUWPR TVXUWYAC	34
20.	4, 5, 6, 9, 1, 2, 3, 7, 8	PQRSTUVWXYZABCDOP QRSABCDEFGHIJKLMNO EFGHIJKLMN	PRTVXUWYACZBDFHOQ SUWACEGIFHJLNKMOQS EGIKMJLNPR	27
21.	7, 8, 9, 6, 3, 4, 5, 1, 2	EFGHIJKLMNOPQRSZABC DKLMNOPQRSTUVWXYA BCDEFGHIJ	EGIKMJLNPROQSUWZBD FHKMOQSPRTVXUWYAC ACEGIFHJLN	17
22.	1, 2, 3, 4, 7, 8, 9, 6, 5	ABCDEFGHIJKLMNOPQRS TEFGHIJKLMNOPQRSZAB CDUVWXY	ACEGIFHJLNKMOQSPRTV XEGIKMJLNPROQSUWZB DFHUWYAC	26
23.	4, 5, 6, 7, 1, 2, 3, 9, 8	PQRSTUVWXYZABCDEFG HIABCDEFGHIJKLMNOOP QRSJKLMN	PRTVXUWYACZBDFHEGI KMACEGIFHJLNKMOQSO QSUWJLNPR	21
24.	7, 8, 9, 5, 1, 4, 6, 3, 2	EFGHIJKLMNOPQRSUVW XYABCDEPQRSTZABCDK LMNOFGHIJ	EGIKMJLNPROQSUWUWY ACACEGIPRTVXZBDFHK MOQSFHJLN	19
25.	1, 2, 3, 6, 5, 4, 9, 8, 7	ABCDEFGHIJKLMNOZAB CDUVWXYPQRSTOPQRSJ KLMNEFGHI	ACEGIFHJLNKMOQSZBDF HUWYACPRTVXOQSUWJ LNPREGIKM	19
26.	4, 5, 6, 9, 8, 7, 3, 2, 1	PQRSTUVWXYZABCDOP QRSJKLMNEFGHIKLMNO FGHIJABCDE	PRTVXUWYACZBDFHOQ SUWJLNPREGIKMKMOQS FHJLNACEGI	15
27.	7, 8, 9, 6, 3, 2, 1, 5, 4	EFGHIJKLMNOPQRSZABC DKLMNOFGHIJABCDEUV WXYPQRST	EGIKMJLNPROQSUWZBD FHKMOQSFHJLNACEGIU WYACPRTVX	20
28.	1, 2, 3, 6, 7, 4, 5, 9, 8	ABCDEFGHIJKLMNOZAB CDEFGHIPQRSTUVWXYO PQRSJKLMN	ACEGIFHJLNKMOQSZBDF HEGIKMPRTVXUWYACO QSUWJLNPR	22

No	Noda *pattern lock*	*Plaintext*	*Ciphertext*	Lama Eksekusi (mili detik)
29.	4, 5, 6, 9, 1, 7, 8, 3, 2	PQRSTUVWXYZABCDOP QRSABCDEEFGHIJKLMN KLMNOFGHIJ	PRTVXUWYACZBDFHOQ SUWACEGIEGIKMJLNPRK MOQSFHJLN	18
30.	7, 8, 9, 6, 3, 4, 1, 2, 5	EFGHIJKLMNOPQRSZABC DKLMNOPQRSTABCDEFG HIJUVWXY	EGIKMJLNPROQSUWZBD FHKMOQSPRTVXACEGIF HJLNUWYAC	26

Berdasarkan percobaan yang dilakukan pada perhitungan *Vigenere Cipher*, waktu yang diperlukan untuk membentuk enkripsi noda *pattern lock* didapat dalam waktu paling cepat 2 mili detik dan paling lama 38 mili detik, masing-masing adalah dengan membentuk pola dengan 2 noda dan membentuk pola dengan 9 noda.

5 KESIMPULAN

Berdasarkan proses pembuatan Aplikasi *Parental Control* dengan mengimplementasikan algoritma *Vigenere Cipher* dapat disimpulkan bahwa:

1. Kekuatan enkripsi menggunakan algoritma *Vigenere Cipher* terletak pada penggunaan kunci, semakin panjang dan bervariasi sebuah kunci maka hasil enkripsi semakin rumit. Dengan penggunaan kunci ABCDE pada enkripsi pola kunci, masih memiliki peluang untuk dipecahkan karena penggunaan kunci yang berulang.
2. Implementasi algoritma *Vigenere Cipher* pada pembentukan pola kunci membutuhkan waktu paling cepat 2 mili detik dengan menghubungkan dua noda dan membutuhkan waktu paling lama 38 mili detik dengan menghubungkan sembilan noda pada *pattern lock*.

DAFTAR PUSTAKA

[1] Agrawal, A., & Patidar, A. (2014). Smart Authentication for Smart Phones. International Journal of Computer Science and Information Technologies, 4839. Dipetik Mei 20, 2018, dari https://pdfs.semanticscholar.org/a749/beb7854e1e9ccc6c846fc1626d1f8fa94f26.pdf

[2] Arjana, P. H., Rahayu, T. P., Y., & H. (2012). Implemetasi Enkripsi Data Dengan Algoritma Vigenere Cipher. SENTIKA 2012. Dipetik Juni 12, 2017, dari https://fti.uajy.ac.id/sentika/publikasi/makalah/2012/2012-22.pdf

[3] Efrandi, Anawati, & Yupriyanti. (2014, September). Aplikasi Kriptografi Pesan Menggunakan Algoritma Vigenere Cipher. Media Infotama. Dipetik Agustus 12, 2017, dari https://jurnal.unived.ac.id/index.php/jmi/article/download/242/220

[4] Hamdani. (2012). Penerapan Metode Vigenere pada Kriptografi Klasik Untuk Pesan Rahasia. Diambil kembali dari http://e-journals.unmul.ac.id/index.php/JIM/article/viewFile/86/pdf

[5] Inggiantowi, H. (2011). Studi Implementasi Algoritma Block Cipher pada Platform Android. Dipetik Aprill 10, 2017, dari http://informatika.stei.itb.ac.id/~rinaldi.munir/Kriptografi/2010-2011/Makalah1/Makalah1-IF3058 -Sem1-2010-2011-080.pdf

[6] Juanda, J. (2015). Perancangan Aplikasi Pembelajaran Kriptografi Metode Sandi Vigenere.

[7] Noercholis, A., & Asyanto, P. (2014, Februari). Aplikasi Kriptografi Teks pada SMS (Short Message Service) dengan Menggunakan Metode Vigenere Cipher. Jurnal Ilmiah Teknologi Teknologi dan Informasi ASIA. Dipetik Juni 11, 2017, dari https://s3.amazonaws.com/academia.edu.documents/37574223/4._Achmad_Noercholis_1-9.pdf?AWSAccessKeyId=AKIAIWOWYYGZ2Y53UL3A&Expires=1557235652&Signature=5p0kmRgfbIFNwiZ1dGA9Y4MTZUc%3D&response-content-disposition=inline%3B%20filename%3DAPLIKASI_KRIPTOGRAFI_

[8] Nurrachmawati. (2014). Pengaruh Sistem Operasi Mobile Android Pada Anak Usia Dini. Jurnal Elektro.

[9] Pabokory, F. N., Astuti, I. A., & Kridalaksana, A. H. (2015). Implementasi Kriptografi Pengaman Data pada Pesan Teks, Isi File Dokumen, dan File Dokumen Menggunakan Algoritma Advanced Encryption Standard. Informastika Mulawarman. Dipetik Januari 11, 2018, dari http://e-journals.unmul. ac.id/index.php/JIM/article/download/23/pdf

[10] Religia, Y. (2015). Implementasi Algoritma Affine Cipher dan Vigenere Cipher Untuk Keamanan Login Sistem Inventori TB Mintra Jepara.

[11] Subari, P. (2013). Desain dan Implementasi Aplikasi Kontrol Orang Tua Menggunakan GPS Pada Smartphone Android. Jurnal Informatika.

[12] Sun, C., Wang, Y., & Zheng, J. (2014). Dissecting pattern unlock: The effect of pattern. Information Security and Applications. Retrieved Mei 20, 2018

[13] Supartini, Y. (2004). Buku Ajar Konsep Dasar Keperawatan Anak. Jakarta: EGC.

[14] Trinika, Y. (2015). Pengaruh Penggunaan Gadget Terhadap Perkembangan Psikososial Anak Usia Prasekolah (3-6 Tahun) di TK Swasta Kristen Immanuel Tahun Ajaran 2014-2015. Dipetik Mei 28, 2017, dari http:// jurnal.untan.ac.id/index.php/jmkeperawatanFK/article/download/11001/ 10480