

## Paper

# Perancangan Aplikasi Pengamanan Pesan Teks Menggunakan Algoritma Kombinasi TTVC Dan OTP Berbasis Android Studio

Author: Ratih Ningtyas, Andi Marwan Elhanafi, Mufida Khairani



SEMINAR NASIONAL TEKNOLOGI INFORMASI & KOMUNIKASI  
**SNASTIKOM KE - 9 TAHUN 2022**

Tema : Peran Tekhnologi dalam Pengembangan Smart System

## Perancangan Aplikasi Pengamanan Pesan Teks Menggunakan Algoritma Kombinasi TTVC Dan OTP Berbasis Android Studio

Ratih Ningtyas<sup>1\*</sup>, Andi Marwan Elhanafi<sup>2</sup>, Mufida Khairani<sup>3</sup>

Program Studi Teknik Informatika, Fakultas Teknik dan Komputer Universitas Harapan Medan

<sup>1\*</sup>ratihningtyas328@gmail.com, <sup>2</sup>andimarwanelhanafi@gmail.com, <sup>3</sup>mufida.khairani@gmail.com

### Abstrak

Sistem operasi untuk perangkat mobile semakin berkembang. Android merupakan salah satu sistem operasi mobile yang kini sangat populer dan banyak digunakan orang-orang. Untuk keperluan aspek keamanan, android juga telah menyediakan khusus untuk fungsi-fungsi kriptografi, seperti enkripsi, dekripsi, dan sebagainya. Kurang amannya pengiriman pesan dapat terjadi karena ketika dilakukan pengiriman, pesan yang dikirim berupa pesan asli sehingga apabila dilakukan pengambilan pesan dari jalur pengiriman maka pesan akan dapat diketahui oleh pihak yang tidak berhak. Maka diperlukan sebuah keamanan pada sebuah data pesan. Enkripsi dan dekripsi dapat di gunakan untuk membuat pesan agar tidak dapat dibaca atau dipahami oleh orang lain yang tidak memiliki hak akses. Teknik pengamanan data dan informasi tersebut dikenal dengan nama kriptografi. Penggunaan algoritma *Triple Transposition Vigenere Cipher (TTVC)* pernah dilakukan terhadap keamanan *SMS (Short Message Service)* agar dapat menjaga integritas dan keamanan pada isi pesan dan menutupi celah dari keamanan SMS. Pesan yang dikirimkan akan dienkripsi menggunakan *Triple Transposition Vigenere Cipher* terlebih dahulu supaya isi dalam pesannya dapat dibaca oleh pengirim dan penerima. Berdasarkan hal yang sudah dibahas diatas penulis akan melakukan perancangan Aplikasi Pengamanan Pesan Teks Menggunakan Algoritma Kombinasi *Triple Transposition Vigenere Cipher* dan *One Time Pad* Berbasis Android Studio untuk memberikan keamanan pada pesan dari pihak yang tidak berhak.

**Kata Kunci :** *Android, Enkripsi, Dekripsi, Kriptografi, Triple Transposition Vigenere Cipher, One Time Pad.*

### Abstrack

*Operating systems for mobile devices are growing. Android is a mobile operating system that is now very popular and widely used by people. For the purposes of the security aspect, Android has also provided specifically for cryptographic functions, such as encryption, decryption, and so on. Insecure message delivery can occur because when sending, the message sent is in the form of an original message so that if a message is taken from the delivery line, the message will be known by unauthorized parties. So we need a security on a message data. Encryption and decryption can be used to make messages so that they cannot be read or understood by other people who do not have access rights. The technique of securing data and information is known as cryptography. The use of the Triple Transposition Vigenere Cipher (TTVC) algorithm has been carried out on SMS security (Short Message Service) in order to maintain the integrity and security of the message content and cover gaps in SMS security. The message sent will be encrypted using the Triple Transposition Vigenere Cipher first so that the contents of the message can be read by the sender and recipient. Based on what has been discussed above the author will design a Text Message Security Application Using a Combination Algorithm of Triple Transposition Vigenere Cipher and One Time Pad Based on Android Studio to provide security for messages from unauthorized parties.*

**Keywords:** *Android, Encryption, Decryption, Cryptography, Triple Transposition Vigenere Cipher, One Time Pad.*

## 1. PENDAHULUAN

Pada era zaman sekarang ini berbagai macam teknologi yang semakin canggih salah satunya teknologi di bidang informasi. Teknologi dapat kita jumpai dalam kehidupan sehari-hari dimana teknologi memberikan kemudahan untuk melakukan pertukaran informasi. Jaringan komputer dan internet telah mengalami perkembangan yang sangat pesat. Salah satunya adalah telepon seluler (ponsel) dengan banyak fitur dan juga memiliki sistem yang sama dengan komputer. Berbagai perangkat lunak untuk mengembangkan aplikasi ponsel pun bermunculan, diantaranya yang cukup dikenal luas adalah android. Salah satu fasilitas yang disediakan ponsel adalah untuk melakukan pengiriman pesan singkat melalui *Short Message Service* [1]. Pesan merupakan komunikasi pengiriman surat secara elektronik yang terhubung melalui jaringan yang saling terkoneksi. Namun terkadang

internet memiliki kelemahan yaitu dari sisi keamanan. Keamanan data pada android menjadi faktor yang penting dan perlu mendapat perhatian khusus, karena di zaman sekarang yang semakin maju, semakin banyak pula penyadapan dan penyalahgunaan informasi pada android untuk keuntungan pribadi ataupun untuk tujuan-tujuan yang tidak baik [2]. Kurang amannya pengiriman pesan dapat terjadi karena ketika dilakukan pengiriman, pesan yang dikirim berupa pesan asli sehingga apabila dilakukan pengambilan pesan dari jalur pengiriman maka pesan akan dapat diketahui oleh pihak yang tidak berhak. Maka diperlukan sebuah keamanan pada sebuah data pesan. Keamanan merupakan sebuah tindakan untuk menjaga kerahasiaan pada sebuah data pesan dari berbagai macam gangguan dan ancaman. Enkripsi dan dekripsi dapat di gunakan untuk membuat pesan agar tidak dapat dibaca atau dipahami oleh orang lain yang tidak memiliki hak akses. Dengan memanfaatkan kriptografi pesan yang hendak dikirimkan akan dilakukan enkripsi pesan terlebih dahulu sehingga pesan yang dikirim bukan merupakan pesan asli melainkan pesan yang sudah dienkripsi yang menjadikan kerahasiaan pesan tetap terjaga. Pesan asli dapat di terima dan dibaca oleh penerima setelah pesan tersebut diterjemahkan (dekripsi) menggunakan kunci rahasia [3].

Penggunaan algoritma *Triple Transposition Vigenere Cipher (TTVC)* pernah dilakukan terhadap keamanan SMS (*Short Message Service*) agar dapat menjaga integritas dan keamanan pada isi pesan dan menutupi celah dari keamanan SMS. Pesan yang dikirimkan akan dienkripsi menggunakan *Triple Transposition Vigenere Cipher* terlebih dahulu supaya isi dalam pesannya dapat dibaca oleh pengirim dan penerima. Sedangkan penggunaan algoritma *One Time Pad (OTP)* dikatakan sempurna dan aman karena didalam penggunaannya barisan pada bilangan diacak sebagai kunci enkripsi dan panjang kunci tersebut sama dengan pesan yang akan dienkripsi dan tidak ada perulangan kunci sebagaimana yang telah diterapkan pada *Vegenere Cipher*. Android studio adalah IDE (*Integrated Development Environment*) resmi untuk pengembangan aplikasi Android dan bersifat open source atau gratis. Peluncuran Android Studio ini diumumkan oleh Google pada 16 mei 2013 pada event Google I/O Conference untuk tahun 2013. Sejak saat itu, Android Studio menggantikan Eclipse sebagai IDE resmi untuk mengembangkan aplikasi Android [4]. Java adalah bahasa pemrograman yang biasa digunakan untuk mengembangkan bagian back-end dari software [5].

Berdasarkan hal yang sudah dibahas diatas penulis akan melakukan perancangan Aplikasi Pengamanan Pesan Teks Menggunakan Algoritma Kombinasi *Triple Transposition Vigenere Cipher* dan *One Time Pad* Berbasis Android Studio untuk memberikan keamanan pada pesan dari pihak yang tidak berhak.

## 2. METODE PENELITIAN

### 2.1 Kriptografi

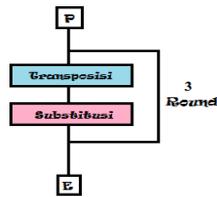
Kriptografi berasal dari bahasa Yunani : "*Cryptos*" artinya "*secret*" (rahasia). Sedangkan "*graphein*" artinya "*writing*" (tulisan). Jadi kriptografi berarti "*secret writing*" (tulisan rahasia). Ada beberapa definisi kriptografi yang telah dikemukakan di dalam berbagai literatur. Definisi yang dipakai di buku-buku yang lama (sebelum tahun 1908-an) menyatakan bahwa kriptografi adalah ilmu dan seni untk menjaga kerahasiaan pesan dengan cara menyandikannya kedalam bentuk yang tidak dapat dimengerti lagi maknanya [6]. kriptografi pada awalnya dijabarkan sebagai ilmu mempelajari bagaimana menyembunyikan pesan. Namun pada pengertian modern kriptografi adalah ilmu yang bersandarkan pada teknik matematika untuk berurusan dengan keamanan informasi seperti kerahasiaan, keutuhan data dan otentikasi entitas. Jadi pengertian kriptografi modern adalah tidak saja berurusan hanya dengan penyembunyian pesan namun lebih pada sekumpulan teknik yang menyediakan keamanan informasi [7].

### 2.2 Algoritma Kriptografi Klasik

Algoritma kriptografi yang termasuk ke dalam jenis kriptografi klasik ini digunakan pada masa sebelum berlakunya komputarisasi dengan komputer, algoritma kriptografi ini rata-rata masih menggunakan kunci *simetris* dan menyandikan pesan dengan teknik *substitusi* atau *transposisi* [8]. Cipher Substitusi adalah pada teknik ini, setiap huruf pada *plaintext* akan digantikan dengan huruf lain berdasarkan suatu cara atau rumus tertentu. Cipher tranposisi adalah mengubah susunan huruf pada *plainteks* sehingga urutannya berubah. *Plainteks* yang dirubah susunan hurufnya seperti ini merupakan *cipherteksnya* [9].

### 2.3 Triple Transposition Vigenere Cipher

*Triple Transposition Vigenere Cipher* adalah metode enkripsi dengan cara mengulang teknik *Vigenere Cipher* yang setiap *plainteksnya* dilakukan transposisi terlebih dahulu sebanyak tiga kali dengan menggunakan kunci yang tiap kuncinya harus berbeda satu dengan yang lainnya.



**Gambar 1** Triple Transposition Vigenere Cipher

Proses yang terjadi pada *Triple Transposition Vigenere Cipher* terbagi menjadi dua bagian. Metode transposisi dapat disimbolkan dengan T dan metode substitusi menggunakan vigenere yang disimbolkan dengan E serta kunci untuk melakukan vigenere K. Secara matematis metode *Triple Transposition Vigenere Cipher* ini dapat dituliskan sebagai:

$$\text{Proses enkripsi: } C = S_3(T_3(S_2(T_2(S_1(T_1(P)))))) \quad (1)$$

Bila dijabarkan, cipherteks diperoleh dengan mentransposisikan plainteks, kemudian hasilnya disubstitusi menggunakan kunci pertama, lalu ditransposisikan kembali, lalu disubstitusi dengan menggunakan kunci yang berbeda dari kunci pertama, disebut saja kunci kedua, setelah itu dilakukan transposisi lagi yang kemudian diakhiri dengan proses substitusi menggunakan kunci ketiga.

Proses dekripsi dapat dilakukan dengan arah sebaliknya. Bila dirumuskan maka akan terlihat sebagai berikut:

$$\text{Proses dekripsi: } P = T_1'(S_1'(T_2'(S_2'(T_3'(S_3'(C)))))) \quad (2)$$

Maksud T' disini adalah transposisi kebalikkannya dan S' adalah substitusi kebalikkannya.

## 2.4 One Time Pad

Algoritma ini ditemukan pada tahun 1917 oleh Mayor Joseph Mauborgne dan Gilbert Vernam. Cipher ini termasuk ke dalam kelompok algoritma kriptografi simetri. *One Time Pad* berisi deretan karakter kunci yang dibangkitkan secara acak dan setiap kunci hanya bisa dipakai sekali pakai. Pemilihan kunci harus secara acak agar tidak bisa diproduksi ulang dan membuat lawan tidak mudah memecahkannya. Panjang stream karakter kunci sama dengan panjang pesan [10].

$$\text{Proses enkripsi : } C_i = (P_i + K_i) \bmod n \quad (1)$$

Dimana:

$C_i$  = Ciphertext;

$P_i$  = Plaintext;

$K_i$  = Kunci;

$$\text{Proses dekripsi : } P_i = (C_i - K_i) \bmod n \quad (2)$$

Sistem *One Time Pad* tidak dapat dipecahkan karena beberapa alasan:

1. Barisan kunci acak + teks asli yang tidak acak = teks kode yang seluruhnya acak.
2. Mendekripsi teks kode dengan beberapa kunci berbeda dapat menghasilkan teks asli yang bermakna sehingga kriptanalis tidak punya cara untuk menentukan teks asli mana yang benar.

## 3. HASIL DAN PEMBAHASAN

### 3.1 Perhitungan Metode Triple Transposition Vigenere Cipher

#### 3.1.1 Enkripsi

Terdapat sebuah *plaintext* dibawah dengan jumlah sebanyak 13 karakter.

Plaintext : **Ratih Ningtyas**

1. Transposisi pertama ( $T_1$ ) dengan kunci 2 :

**Tabel 1.** Transposisi Pertama ( $T_1$ ) dengan kunci 2

R	a
t	i
h	N
i	n
g	t
y	a
s	

Hasil  $T_1$  : R t h i g y s a i N n t a

Substitusi pertama ( $S_1$ ) dengan kunci = Rahasia

$S_1 = (T_1) + (K)$

**Tabel 2.** Substitusi pertama ( $S_1$ ) dengan kunci = Rahasia

<b>T<sub>1</sub></b>	R	t	h	i	g	y	s	a	i	N	n	t	a
<b>K</b>	R	a	h	a	s	i	a	R	a	h	a	s	i
<b>H</b>	\$	U	P	J	Z	b	T	3	J	6	O	g	J

Hasil = \$ U P J Z b T 3 J 6 O g J

2. Transposisi kedua ( $T_2$ ) dengan kunci 3 :

Plaintext : = \$ U P J Z b T 3 J 6 O g J

**Tabel 3.** Transposisi Kedua ( $T_2$ ) dengan kunci 3

\$	U	P
J	Z	b
T	3	J
6	O	g
J		

Hasil  $T_2$  = \$ J T 6 J U Z 3 O P b J g

Substitusi kedua ( $S_2$ ) dengan kunci = Penting

$S_2 = (T_2) + (K)$

**Tabel 4.** Substitusi Kedua ( $S_2$ ) dengan kunci = Penting

<b>T<sub>2</sub></b>	\$	J	T	6	J	U	Z	3	O	P	B	J	g
<b>K</b>	P	e	n	t	i	n	g	P	e	n	t	i	n
<b>H</b>	t	/	B	*	3	C	A	ETX	4	>	V	3	U

Hasil = t / B \* 3 C A ETX 4 > V 3 U

3. Transposisi ketiga ( $T_3$ ) dengan kunci 4 :

Plaintext : t / B \* 3 C A ETX 4 > V 3 U

**Tabel 5.** Transposisi Ketiga ( $T_3$ ) dengan kunci 4

t	/	B	*
3	C	A	ETX
4	>	V	3
U			

Hasil = t 3 4 U / C > B A V \* ETX 3

Substitusi ketiga ( $S_3$ ) dengan kunci = Biasa

**Tabel 6.** Substitusi ketiga ( $S_3$ ) dengan kunci = Biasa

<b>T<sub>3</sub></b>	t	3	4	U	/	C	>	B	A	V	*	ETX	3
<b>K</b>	B	i	a	s	a	B	i	a	s	a	B	i	a
<b>H</b>	6	FS	NAK	H	DLE	ENQ	'	#	4	7	1	1	DC4

Jadi hasil enkripsinya adalah = 6 FS NAK H DLE ENQ ' # 4 7 1 1 DC4

**3.1.2 Dekripsi**

Maksud  $T'$  disini adalah tranposisi kebalikkannya dan  $S'$  adalah susbtitusi kebalikkannya.

Diketahui sebuah ciphertext dibawah dengan jumlah sebanyak 13 karakter.

Ciphertext : 6 FS NAK H DLE ENQ ' # 4 7 1 1 DC4

1. Substitusi kebalikan ketiga ( $S_3'$ ) dengan kunci = Biasa

$$S_3' = (C) - (K)$$

**Tabel 7.** Substitusi kebalikan ketiga ( $S_3'$ ) dengan kunci = Biasa

<b>T<sub>3'</sub></b>	6	FS	NAK	H	DLE	ENQ	'	#	4	7	1	1	DC4
<b>K</b>	B	i	a	s	a	B	i	a	s	a	B	i	a
<b>H</b>	t	3	4	U	/	C	>	B	A	V	*	ETX	3

Hasil = t 3 4 U / C > B A V \* ETX 3

Transposisi kebalikan ketiga ( $T_3'$ ) dengan kunci 4 :

**Tabel 8.** Transposisi kebalikan ketiga ( $T_3'$ ) dengan kunci 4

t	/	A	3
3	C	V	
4	>	*	
U	B	ETX	

Hasil  $T_3'$  = t / A 3 3 C V 4 > \* U B ETX

2. Substitusi kebalikan ketiga ( $S_2'$ ) dengan kunci = Penting

$$S_2' = (C) - (K)$$

Ciphertext : t / A 3 3 C V 4 > \* U B ETX

**Tabel 9.** Substitusi kebalikan kedua ( $S_2'$ ) dengan kunci = Penting

<b>T<sub>2'</sub></b>	t	/	A	3	3	C	V	4	>	*	U	B	ETX
<b>K</b>	P	e	n	t	i	n	g	P	e	n	t	i	n
<b>H</b>	\$	J	T	6	J	U	Z	3	O	P	b	J	g

Hasil = \$ J T 6 J U Z 3 O P b J g

**Tabel 10.** Transposisi kebalikan kedua ( $T_2'$ ) dengan kunci 3

\$	U	b
J	Z	J
T	3	g
6	O	
J	P	

Hasil  $T_2'$  = \$ U b J Z J T 3 g 6 O J P

3. Substitusi kebalikan pertama ( $S_1'$ ) dengan kunci = Rahasia

$$S_2' = (C) - (K)$$

Ciphertext : \$ U b J Z J T 3 g 6 O J P

**Tabel 11.** Substitusi kebalikan kedua ( $S_2'$ ) dengan kunci = Rahasia

<b>T<sub>1</sub>'</b>	\$	U	b	J	Z	J	T	3	g	6	O	J	P
<b>K</b>	R	a	h	a	s	i	a	R	a	h	a	s	i
<b>H</b>	R	t	h	i	g	y	s	a	i	N	n	t	a

Hasil = R t h i g y s a i N n t a

**Tabel 12.** Transposisi kebalikan kedua ( $T_1'$ ) dengan kunci 3

R	a
t	i
h	N
i	n
g	t
y	a
s	

Hasil  $T_1'$  = R a t i h N i n g t y a s

### 3.2 Perhitungan Metode One Time Pad

#### 3.2.1 Enkripsi

Plaintext : Ratih Ningtyas

Kunci : Rahasia

**Tabel 13.** Enkripsi *One Time Pad*

Plaintext	Kunci	(P+K) mod128	Cipher	Hasil Akhir
R = 82	R = 82	164/128= 36	\$	\$ B \ J [ 7 J @ H \ Z T \
a = 97	a = 97	194/128= 66	B	
t = 116	h = 104	220/128= 92	\	
i = 105	a = 97	202/128= 74	J	
h = 104	s = 115	219/128= 91	[	
N = 78	i = 105	183/128= 55	7	
i = 105	a = 97	202/128= 74	J	
n = 110	R = 82	192/128= 64	@	
g = 103	a = 97	200/128= 72	H	
t = 116	h = 104	220/128= 92	\	
y = 121	a = 97	218/128= 90	Z	
a = 97	s = 115	212/128= 84	T	
s = 115	i = 105	220/128= 92	\	

#### 3.2.2 Dekripsi

Setelah melakukan proses *enkripsi* pesan teks dalam *One Time Pad*, *ciphertext* yang diperoleh adalah \$ B \ J [ 7 J @ H \ Z T \.

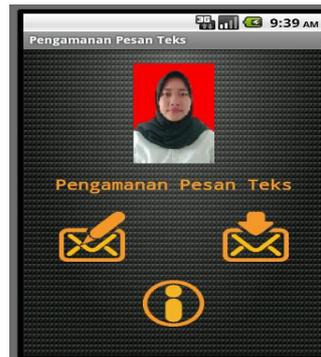
**Tabel 14.** Dekripsi *One Time Pad*

Ciphertext	Kunci	(C-K) mod256	Plaintext	Hasil Akhir
\$ = 36	R = 82	-46/128= 82	R	R a t i h N i n g t y a s
B = 66	a = 97	-31/128= 97	a	
\ = 92	h = 104	-12/128= 116	t	
J = 74	a = 97	-23/128= 105	i	
[ = 91	s = 115	-24/128= 104	h	
7 = 55	i = 105	-50/128= 78	N	
J = 74	a = 97	-23/128= 105	i	
@ = 64	R = 82	-18/128= 110	n	
H = 72	a = 97	-25/128= 103	g	

$\backslash = 92$	$h = 104$	$-12/128 = 116$	t
$Z = 90$	$a = 97$	$-7/128 = 121$	y
$T = 84$	$s = 115$	$-31/128 = 97$	a
$\backslash = 92$	$i = 105$	$-13/128 = 115$	s

### 3.3 Halaman Home

Setelah berhasil log in maka pertama yang muncul adalah Form beranda. Form beranda akan menampilkan menu yang dapat kita pilih. Terdapat menu seperti Mengirim Pesan, Menerima Pesan, dan Tentang.



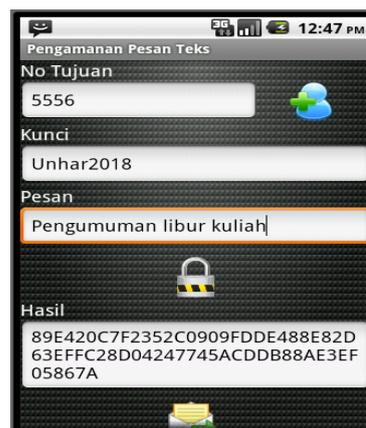
Gambar 2 Tampilan Menu Utama

### 3.4 Tampilan Form Pesan Keluar

Pengujian enkripsi menggunakan sistem yang dibangun terhadap contoh tersebut akan menghasilkan *ciphertext*, *cipherkey*. Pada tahap ini, penulis melakukan pengujian *form* enkripsi dengan menginputkan contoh sebagai berikut :

1. Masukkan nomor tujuannya adalah 5556
2. Pesan yang akan dienkripsi adalah Pengumuman libur kuliah dimana jumlah pesan adalah 23 kata
3. Kunci yang digunakan adalah Unhar2018

Setelah contoh tersebut diinputkan ke dalam *form* enkripsi kemudian menekan tombol kunci maka akan dihasilkan *output*.



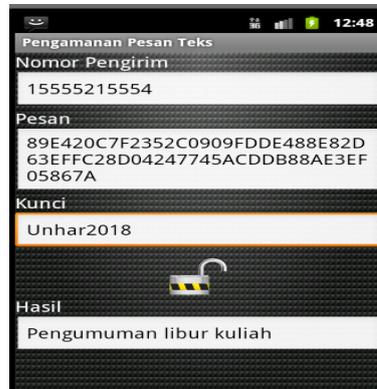
Gambar 3 Tampilan Proses Enkripsi dan Hasilnya

### 3.5 Tampilan Form Pesan Keluar

Pengujian dekripsi menggunakan sistem yang dibangun terhadap contoh tersebut akan menghasilkan *cipherkey*, *ciphertext*. Pada tahap ini, penulis melakukan pengujian *form* dekripsi dengan meninputkan contoh sebagai berikut:

1. Kunci yang digunakan adalah Teknik Informatika 2018.

Setelah contoh tersebut diinputkan ke dalam *form* dekripsi kemudian menekan tombol kunci maka akan dihasilkan output.



**Gambar 4** Tampilan Proses Dekripsi dan Hasilnya

#### 4. KESIMPULAN

Berdasarkan penelitian yang dilakukan oleh penulis, melalui analisa yang dilakukan maka diambil kesimpulan beberapa hal sebagai berikut :

1. Aplikasi enkripsi dan dekripsi dengan menggunakan algoritma Triple Transposition Vigenere Cipher dan One Time Pad dapat digunakan untuk mengamankan pesan teks. Karena proses enkripsi dan dekripsi pada algoritma Vigenere Cipher dilakukan sebanyak 3 kali teknik transposisi dan 3 kali teknik substitusi sehingga menghasilkan ciphertext yang sulit untuk dibaca.
2. Kunci enkripsi dan dekripsi hanya akan diberikan kepada pengguna yang berhak menerima pesan saja.
3. Pesan hanya bisa terkirim dan dibaca maksimal 72 kata. Karena emulator punya kemampuan kapasitas dalam pemrosesan perhitungan, dimana emulator menggunakan virtual memori.

#### DAFTAR PUSTAKA

- [1] S. Sari, "Perancangan Aplikasi Pengamanan Pesan Teks Menggunakan Algoritma One Time Pad Berbasis Android," *KAKIFIKOM (Kumpulan Artik. Karya Ilm. Fak. Ilmu Komputer)*, vol. 01, pp. 23–26, 2020, doi: 10.54367/kakifikom.v1i1.623.
- [2] A. M. Elhanafi, "Analisis Dan Penerapan Algoritma Substitusi, Encoding Triple Base64 Dan Vigenere Cipher Untuk Keamanan Login Pada Website," *Tesis*, pp. 1–69, 2014.
- [3] S. Sutrisno, P. Studi, T. Informatika, F. I. Komputer, U. Dian, and N. Semarang, "RANCANG BANGUN APLIKASI PESAN MENGGUNAKAN ALGORITMA VIGENERE The way to make and apply Vigenere Cipher and One Time Pad has been formulated in this".
- [4] J. Andi, "Pembangunan Aplikasi Child Tracker Berbasis Assisted – Global Positioning System ( A-GPS ) Dengan Platform Android," *J. Ilm. Komput. dan Inform.*, vol. 1, no. 1, pp. 1–8, 2015.
- [5] Sadikin Rifki, *Kriptografi Untuk Keamanan Jaringan Dan Implementasinya Dalam Bahasa Java*. Yogyakarta: C.V.Andi OFFSET, 2012.
- [6] J. Rekursif, D. Fitria, and B. Susilo, "E-Learning Kriptografi Dengan Virtual Class Berbasis Multimedia," *J. Rekrusif*, vol. 2, no. 1, pp. 10–18, 2014.
- [7] D. Abdullah and Surnihayati, "Pengamanan Email Menggunakan Metode Vigenere Chiper," *JISAMAR (Journal Inf. Syst. Applied, Manag. Account. Res.)*, vol. 1, no. November, pp. 1–9, 2017.
- [8] M. K. Harahap, "Analisis Perbandingan Algoritma Kriptografi Klasik Vigenere Cipher Dan One Time Pad," *InfoTekJar (Jurnal Nas. Inform. dan Teknol. Jaringan)*, vol. 1, no. 1, pp. 61–64, 2016, doi: 10.30743/infotekjar.v1i1.43.
- [9] M. L. Caroline, "Metode Enkripsi baru : Triple Transposition Vigenere Cipher," *J. Inf. Technol.*, vol. 1, no. 1, pp. 22–28, 2018.

- [10] M. A. Jauhari, "UNIVERSITAS SUMATERA UTARA Poliklinik UNIVERSITAS SUMATERA UTARA," *J. Pembang. Wil. Kota*, vol. 1, no. 3, pp. 82–91, 2018.