E-ISSN : 2540 - 8984

JIPI (Jurnal Ilmiah Penelitian dan Pembelajaran Informatika)
Volume 07, Nomor 03, September 2022 : 926–934

PROTOTYPE PENERAPAN HASIL KOMBINASI KRIPTOGRAFI DIFFIE-HELLMAN, MESSAGE-DIGEST 5 DAN RIVEST CHIPER 4 PADA LAYANAN PESAN SINGKAT SMARTPHONE ANDROID

Deden Sukmana[1)], Sugiarti[2)]
[1,2)]Magister Sistem Informasi STMIK LIKMI
Ir. H. Juanda No. 96 Bandung 40132, Jawa Barat, Indonesia
e-mail: dedensukmana98@gmail.com[1)], sugiartirahmat131@gmail.com [2)]

ABSTRAK

Kebutuhan masyarakat dalam saling bertukar informasi sudah tidak dapat dipungkiri lagi. Seiring dengan perkembangan teknologi, masyarakat semakin mudah untuk bertukar informasi. Salah satu contohnya menggunakan layanan pesan singkat (Short Message Service) atau biasa disebut SMS. Layanan ini biasa tersedia pada handphone biasa hingga smartphone, namun sekarang seiring berkembangnya jaman terutama perkembangan teknologi smartphone yang semakin canggih, layanan pesan singkat memiliki beberapa kekurangan yang salah satunya ada pada bagian keamanannya yang masih rendah. Untuk mengatasi masalah tersebut peneliti berencana untuk meningkatkan keamanan pada layanan pesan singkat ini dengan menambahkan algoritma algoritma kriptografi diffie-hellman, message-digest 5, dan rivest chiper 4 pada aplikasi sms berbasis Android. Sehingga, pengguna layanan pesan singkat ini tidak khawatir pesannya akan diketahui oleh oranglain yang tidak berkepentingan. Setelah algoritma kroptografi diffie-hellman, message-digest 5, dan rivest chiper 4 berhasil diimplementasikan pada aplikasi sms android, pesan yang dikirim dan diterima berbentuk chipertext, sehingga orang yang tidak berkepentingan tidak bisa membacanya langsung.

***Kata Kunci**: Android, Implementasi, Kombinasi, Kriptografi, Sms.*

ABSTRACT

The community's need for exchanging information cannot be denied. Along with the development of technology, it is easier for people to exchange information. One example is using a short message service (Short Message Service) or so-called SMS. This service is usually available on ordinary cellphones to smartphones, but now with the development of the era, especially the development of increasingly sophisticated smartphone technology, the short message service has several shortcomings, one of which is the low security section. To solve this problem, the researcher plans to increase the security of this short message service by adding diffie-hellman, message-digest 5, and rivest cipher 4 cryptographic algorithms to the Android-based sms application. So, users of this short message service are not worried that their messages will be known by other unauthorized people. After the diffie-hellman, message-digest 5, and rivest cipher 4 cryptographic algorithms were successfully implemented in the android sms application, messages sent and received were in the form of ciphertext, so that unauthorized people could not read them directly.

***Keywords**: Android, Combination, Cryptography, Implementation, Sms.*

I. PENDAHULUAN

PERKEMBANGAN teknologi semakin maju berdampak pada cara masyarakat dalam berkomunikasi. Dahulu komunikasi jarak jauh masih menggunakan cara yang konvensional, yaitu dengan cara saling mengirim surat, tetapi sekarang komunikasi jarak jauh dapat dilakukan dengan mudah dan cepat yaitu dengan adanya teknologi seperti email, SMS (*Short Message Service*), dan Internet yang merupakan salah satu teknologi telekomunikasi yang paling banyak digunakan. Selain itu, perkembangan ponsel genggam juga semakin maju dengan hadirnya smartphone yang menjalankan sistem operasi Android. Android adalah sistem operasi berbasis Linux untuk perangkat seluler. Android adalah sistem operasi *open source* (gratis). Oleh karena itu, Android menyediakan *platform* terbuka bagi para pengembang untuk membuat aplikasi mereka sendiri untuk dijalankan di perangkat Android [1].

Layanan SMS yang menggunakan aplikasi telepon seluler standar masih banyak digunakan di berbagai kalangan masyarakat dan belum memberikan cara yang aman untuk bertukar informasi. Pesan yang dikirim melalui aplikasi ponsel tetap berupa teks terbuka yang tidak dilindungi dengan benar. Selain itu, pengiriman SMS tidak sampai ke penerima secara langsung, tetapi pengiriman SMS harus dilakukan melalui *Short Message Service Center* (SMSC), yang mencatat komunikasi antara pengirim dan penerima. Operator dapat mengambil informasi dan membaca SMS dengan SMSC [2]. Sehingga, bisa dikatakan layanan SMS ini kurang memerhatikan privasi. Padahal pada era teknologi informasi saat ini privasi merupakan hal yang sangat penting. Seperti dalam berkomunikasi, privasi

E-ISSN : 2540 - 8984

JIPI (Jurnal Ilmiah Penelitian dan Pembelajaran Informatika)
Volume 07, Nomor 03, September 2022 : 926–934

dibutuhkan agar pada saat setiap individu berkomunikasi satu sama lain tidak merasa khawatir komunikasi mereka diketahui oleh pihak ketiga atau pihak yang tidak berkepentingan dan privasi tersebut patut dihargai karena privasi melekat pada setiap individu [13].

Kriptografi adalah ilmu yang mempelajari teknik matematika yang berkaitan dengan aspek keamanan informasi, seperti tingkat kepercayaan, integritas data, otentikasi entitas, dan otentikasi keaslian data. Pesan memiliki nilai estetika tersendiri dalam seni dan budaya, karena seni didefinisikan oleh fakta sejarah bahwa setiap orang memiliki cara sendiri untuk melindungi data. Selain keamanan data, keamanan juga membutuhkan teknologi dan seni. Keandalan keamanan tergantung pada bagaimana setiap individu memahami arti dari data. Banyak orang sekarang ini menggeluti bidang enkripsi karena mempelajari teknik enkripsi memungkinkan mereka untuk memelihara komputernya tanpa mengeluarkan banyak modal dibandingkan dengan menyewa atau membeli software khusus untuk keamanan data. [3]

Banyak penelitian yang telah mengimplementasikan berbagai macam algoritma kriptografi untuk menambah keamanan pada layanan pesan singkat Android. Diantaranya penelitian yang dilakukan oleh [4] yang mengimplementasikan algoritma kriptografi AES pada aplikasi SMS berbasis Android sebagai sistem keamanan pesan dan hasil dari penelitian ini menyatakan bahwa algoritma kriptografi AES dapat diimplementasikan pada aplikasi SMS berbasis Android. Penelitian lain yang dilakukan oleh [5] yaitu mengimplementasikan algoritma kriptografi RSA untuk pengamanan data pengiriman SMS berbasis Android. [6] juga menyatakan bahwa algoritma kriptografi DES dapat digunakan untuk mengirim pesan SMS yang bersifat rahasia dengan mengenkripsi terlebih dahulu pesan tersebut sebelum pesan itu dikirim.

Dari latar belakang dan beberapa penelitian terkait diatas maka dalam penelitian ini, peneliti bermaksud menerapkan kombinasi algoritma kriptografi *Diffie-Hellman*, *Message-Diggest 5* dan *Rivest Chiper 4* pada layanan pesan singkat Android yang merupakan hasil penelitian yang dilakukan oleh [7] dengan harapan dapat membantu menambah keamanan pada pesan singkat yang dikirim guna meningkatkan privasi penggunanya.

II. METODE PENELITIAN

Siklus hidup pengembangan sistem yang digunakan dalam penelitian ini adalah metode air terjun atau biasa dikenal dengan metode waterfall, nama model ini sebenarnya "Linear Sequential Model" yang menggambarkan suatu pendekatan yang sistematis dan sekuensial (berurutan) [8]. Beberapa langkah model waterfall yang digunakan dalam penelitian ini yaitu:

1. Analisis kebutuhan, menganalisis kebutuhan-kebutuhan yang diperlukan dalam membuat aplikasi layanan pesan singkat yang mengimplementasikan kombinasi algoritma kriptografi pada *smartphone* Android.
2. Perancangan sistem, mulai dari perancangan masukan (*input*) dan keluaran (*output*), hingga perancangan antarmuka (*user interface*).
3. Pengkodean dan testing, membuat dan menguji aplikasi layanan pesan singkat.

III. HASIL DAN PEMBAHASAN

Pada tahapan ini terbagi menjadi tiga bagian yaitu perancangan, implementasi dan pengujian.

A. Perancangan

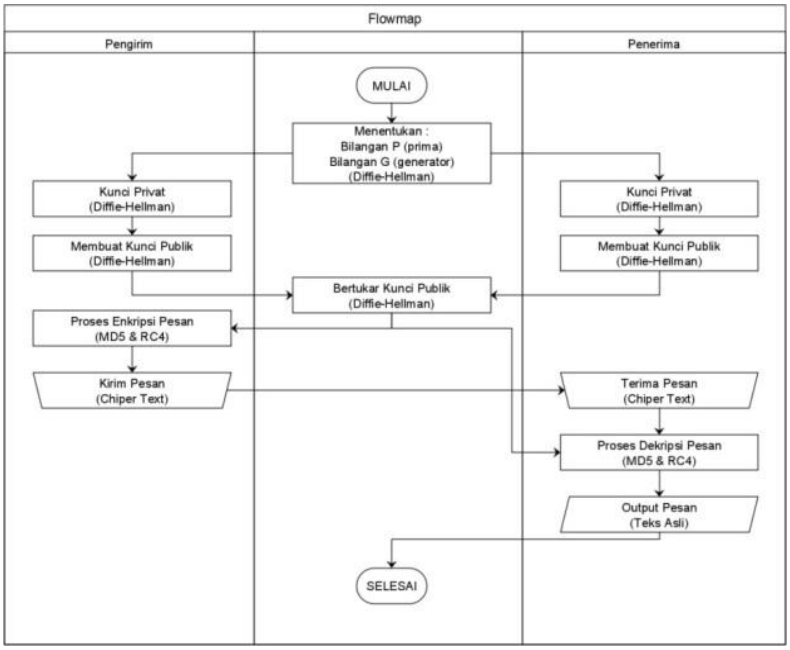
Dalam tahapan perancangan peneliti menggunakan Diagram alir yang mendefinisikan pemetaan aliran informasi kedalam struktur program yang digunakan untuk memungkinkan pengguna lebih memahami sistem yang dikembangkan [10] dan *Unified Modelling Language* yang merupakan salah satu standar bahasa yang paling banyak digunakan di industri untuk mendefinisikan persyaratan, melakukan analisis dan desain, dan menggambarkan arsitektur pemrograman berorientasi objek [9].

1) Diagram Alir Sistem

Dari hasil penelitian yang dilakukan oleh [7] dengan penelitian mengkombinasikan algoritma kriptografi *Diffie-hellman*, *Message-Diggest* 5 dan *Rivest Chiper* 4 yang peneliti akan implementasikan pada aplikasi Layanan Pesan Singkat (SMS) berbasis Android maka dihasilkan diagram alir (*flowmap*) sebagai berikut:

E-ISSN : 2540 - 8984

JIPI (Jurnal Ilmiah Penelitian dan Pembelajaran Informatika)
Volume 07, Nomor 03, September 2022 : 926–934



Gambar 1. Diagram Alur Sistem

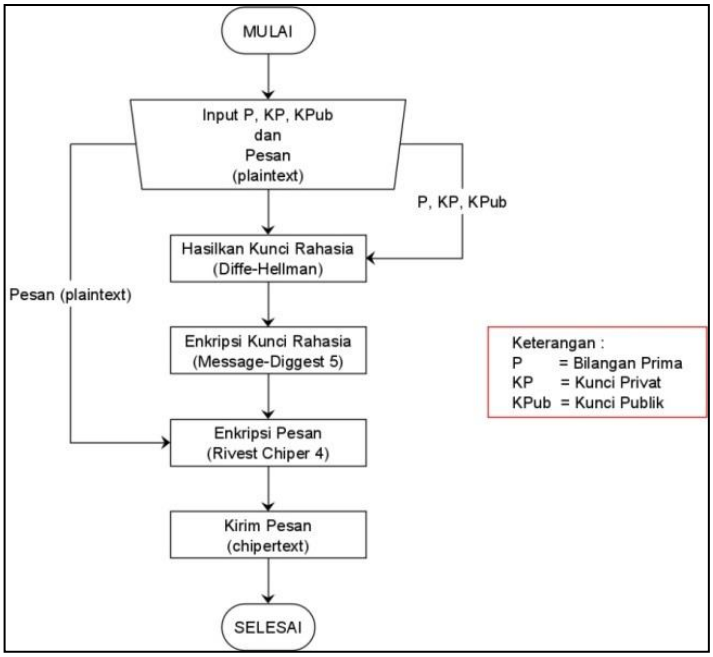
Dari diagram alur pada gambar 1 tersebut, pengirim dan penerima harus menentukan terlebih dahulu bilangan prima (P) dan bilangan generator (G) dengan ketentuan bilangan generator harus kurang dari bilangan prima (bilangan P dan G bersifat publik), kemudian pengirim dan penerima menentukan kunci privat masing-masing (kunci privat bersifat rahasia), selanjutnya pengirim dan penerima membuat kunci publik masing-masing dengan menghitung bilangan P, G dan kunci privat masing-masing (kunci publik bersifat publik).setelah kunci publik berhasil dibuat, pengirim dan penerima saling bertukar kunci publik. Pengirim menggunakan kunci publik penerima untuk mengenkripsi pesan menjadi chipertext sebelum pesan itu dikirim dan penerima menerima pesan dalam bentuk chipertext yang harus didekripsi terlebih dahulu menggunakan kunci publik pengirim untuk menghasilkan atau melihat pesan asli dari pengirim.

2) Diagram Alir Enkripsi Pesan

Diagram alir enkripsi pesan pada gambar 2, pengirim menginputkan bilangan prima, kunci privat (pengirim), kunci publik (yang telah ditukar dengan penerima), dan pesan (*plaintext* / teks asli). Kemudian P, KP dan KPub akan dihitung untuk menghasilkan kunci rahasia menggunakan algoritma Diffie-Hellman. Setelah kunci rahasia dihasilkan, kunci tersebut dienkripsi kembali menggunakan algoritma Message-Digest 5 dan digunakan sebagai kunci untuk mengenkripsi pesan (*plaintext*) menjadi *chipertext*, kemudian pesan (*chipertext*) tesebut dikirim.

E-ISSN : 2540 - 8984

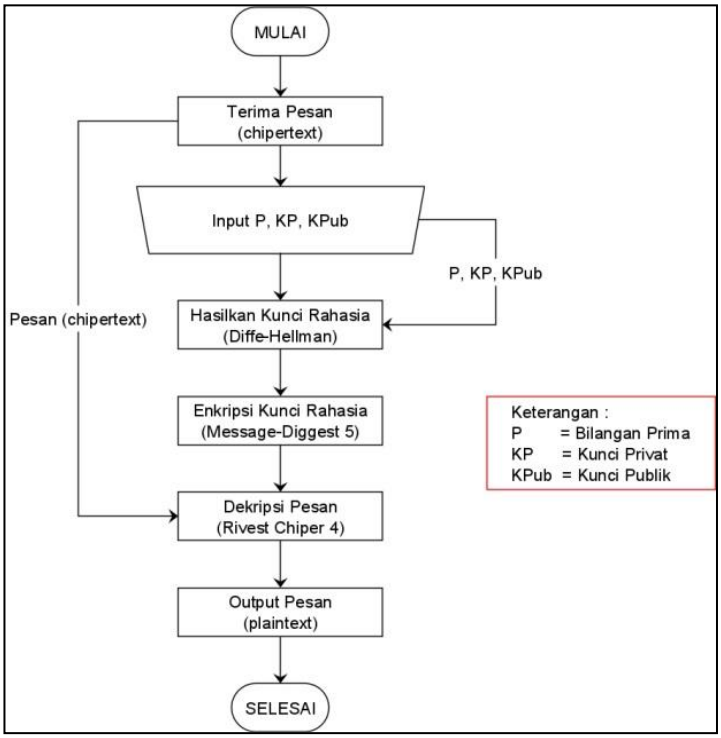
JIPI (Jurnal Ilmiah Penelitian dan Pembelajaran Informatika)
Volume 07, Nomor 03, September 2022 : 926–934



Gambar 2. Diagram Alur Enkripsi Pesan

3) Diagram Alir Deskripsi Pesan

Pesan yang dikirim melalui aplikasi akan diterima dalam bentuk *chipertext*, sehingga penerima perlu mendekripsi pesan tersebut, penerima menginputkan bilangan prima, kunci privat (penerima) dan kunci publik (yang telah ditukar dengan pengirim) untuk dihitung dan menghasilkan kunci rahasia menggunakan algoritma *Diffie-Hellman*.Setelah kunci rahasia dihasilkan, kunci tersebut dienkripsi kembali menggunakan algoritma *Message-Diggest* 5 dan digunakan untuk mendekripsi pesan (*chipertext*) menjadi pesan dalam bentuk teks asli (*plaintext*) menggunakan algoritma *Rivest Chiper* 4. Untuk diagram alirnya dapat dilihat pada gambar 3.



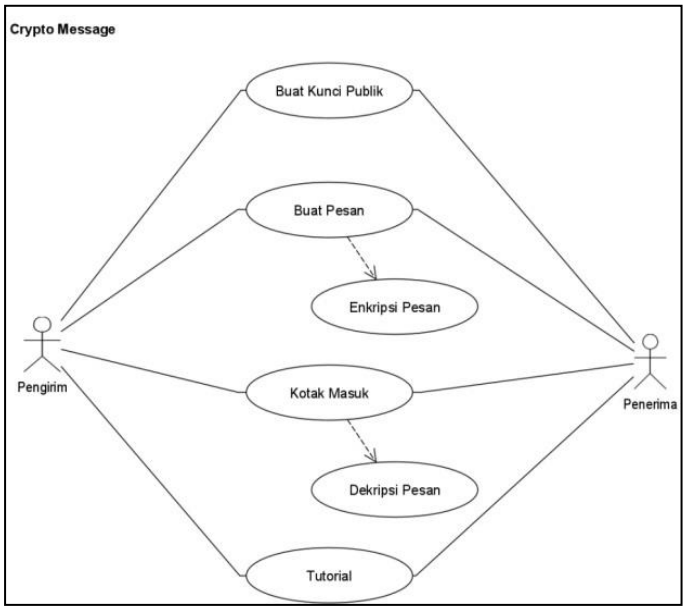
Gambar 3. Diagram Alur Dekripsi Pesan

E-ISSN : 2540 - 8984

JIPI (Jurnal Ilmiah Penelitian dan Pembelajaran Informatika)
Volume 07, Nomor 03, September 2022 : 926–934

4) Use Case Diagram

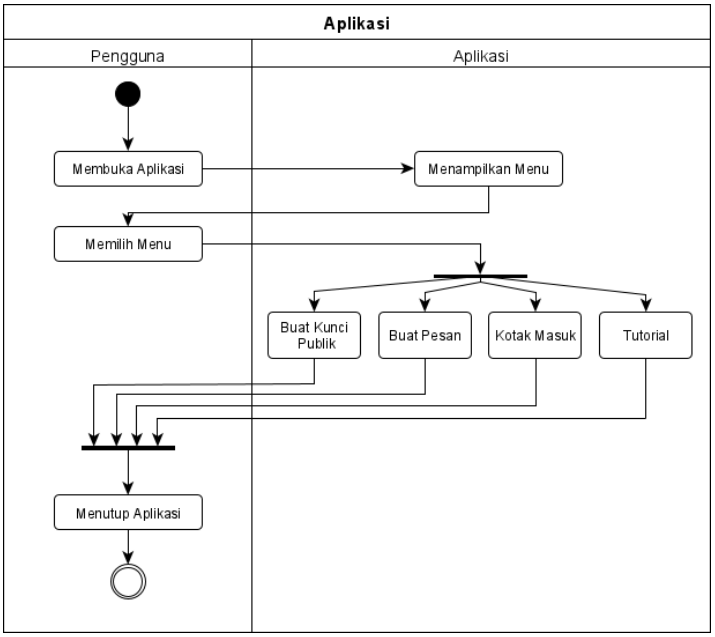
Use case diagram merupakan model perilaku dari sistem yang dibuat. *Use case* bekerja dengan menjelaskan interaksi umum antara pengguna sistem dan sistem itu sendiri melalui cerita tentang bagaimana sistem digunakan [9] Gambar 4 menujukkan use case dari sistem yang akan dibangun.



Gambar 4. *Use case* Diagram

5) Activity Diagram

Activity diagram adalah diagram yang menggambarkan alur kerja atau aktivitas dari suatu sistem yang berada di dalam perangkat lunak [9]. Gambar 5 menunjukan *activity diagram* dari sistem yang akan dibangun secara garis besar.



Gambar 5. *Activity* Diagram

B. Implementasi

Aplikasi ini dinamai *Crypto Message*, dimana aplikasi ini didesain khusus untuk mengenkripsi dan dekripsi pesan singkat menggunakan algoritma kriptografi *Diffie-Hellman*, *Message-Diggest* 5 dan *Rivest Chiper* 4 pada

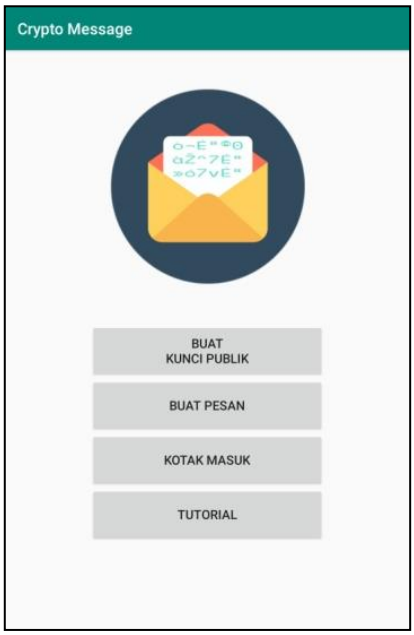
E-ISSN : 2540 - 8984

JIPI (Jurnal Ilmiah Penelitian dan Pembelajaran Informatika)
Volume 07, Nomor 03, September 2022 : 926–934

smartphone Android. Berikut merupakan hasil implementasi berdasarkan rancangan yang telah dijelaskan sebelumnya.

Antarmuka Utama

Antarmuka utama merupakan antarmuka yang menampilkan menu utama pada saat aplikasi dibuka. Menu utama tersebut diantaranya menu buat kunci publik, buat pesan, kotak masuk, dan menu tutorial. Gambar 6 menunujukan antarmuka utama aplikasi.



Gambar 6. Antarmuka utama

Antarmuka Kunci Publik

Antarmuka ini ditujukan untuk membuat kunci publik yang akan ditukar antara pengirim dan penerima. Antarmuka dapat dilihat pada gambar 7.

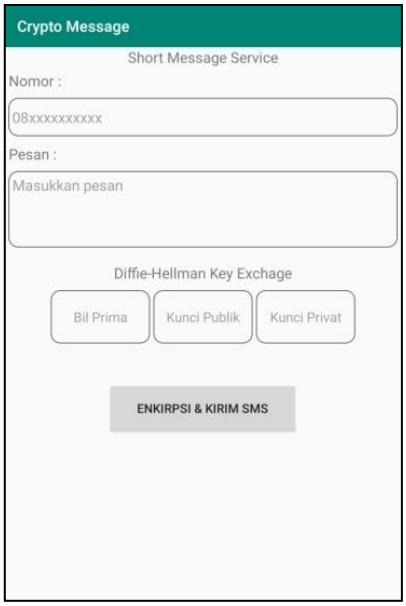
Gambar 7. Antarmuka buat kunci publik

Antarmuka Buat Pesan

Antarmuka buat pesan dapat dilihat pada gambar 8, antarmuka ini digunakan untuk membuat dan mengenkripsi pesan kemudian pesan tersebut dikirimkan ke SMSC (*Short Message Service Center*).

E-ISSN : 2540 - 8984

JIPI (Jurnal Ilmiah Penelitian dan Pembelajaran Informatika)
Volume 07, Nomor 03, September 2022 : 926–934



Gambar 8. Antarmuka buat pesan

Antarmuka Rincian Pesan

Gambar 9 menujukan antarmuka dari rincian pesan, dan terdapat opsi untuk mendekripsi pesan jika pesan yang diterima dalam bentuk *chipertext*.

Gambar 9. Antarmuka rincian pesan

C. Pengujian

Dalam tahapan pengujian peneliti menggunakan metode Pengujian *black-box* yang memverifikasi hasil eksekusi aplikasi berdasarkan input (data pengujian) yang diberikan dan mengonfirmasi bahwa fungsi aplikasi memenuhi persyaratan. [11] Pengujian *black-box* adalah pengujian yang berfokus pada kesesuaian dengan antarmuka pengguna, pengujian fungsional, dan aliran fungsional yang dibutuhkan oleh pengguna dalam aplikasi atau antarmuka. Pengujian *black-box* tidak menguji terhadap kode sumber program. [12] Berikut merupakan hasil pengujian dari aplikasi *Crypto Message*.

E-ISSN : 2540 - 8984

JIPI (Jurnal Ilmiah Penelitian dan Pembelajaran Informatika)
Volume 07, Nomor 03, September 2022 : 926–934

TABEL I
DATA PENGUJIAN *BLACK-BOX*

No	Data uji	Skenario Uji	Hasil diharapkan
1	Menu Utama	Memilih menu “Buat Kunci Publik”	Menampilkan tampilan pembuatan kunci publik
		Memilih menu “Buat Pesan”	Menampilkan tampilan pembuatan pesan
		Memilih menu “Kotak masuk”	Menampilkan daftar pesan yang diterima
		Melihat detail pesan dan halam dekripsi pesan	Menampilkan detail pesan dan input untuk mendekripsi pesan
		Memilih menu “tutorial”	Menampilkan halaman panduan singkat
2	Buat Kunci Publik	Mengisi semua kolom input dan menekan tombol “buat kunci publik”	Kunci publik dibuat dan ditampilkan
		Mengkosongkan salah satu kolom input dan menekan tombol “buat kunci publik”	Menampilkan peringatan kolom kosong harus diisi
3	Buat Pesan	Mengisi semua kolom input dan menekan tombol “enkrispsi & kirim sms”	Pesan dalam bentuk *plaintext* dienkripsi kemudian dikirim dalam bentuk *chipertext*
		Mengkosongkan salah satu kolom input dan menekan tombol “enkripsi & kirim sms”	Menampilkan peringatan kolom kosong harus diisi
4	Kotak Masuk	Memilih salah satu dari daftar pesan yang diterima	Menampilkan detail pesan dan form untuk dekripsi pesan
		Mengkosongkan salah satu kolom input pada detail pesan dan menekan tombol “dekripsi pesan”	Menampilkan peringatan kolom kosong harus diisi
5	Detail Pesan	Mengisi kolom input dekripsi pesan dan menekan tombol “dekripsi pesan”	Jika kunci sesuai maka pesan akan di dekripsi menjadi *plaintext*, jika kunci tidak sesuai pesan akan dienkripsi menjadi *chipertext*

TABEL II
HASIL PENGUJIAN *BLACK-BOX*

No	Data uji	Skenario Uji	Hasil
1	Menu Utama	Memilih menu “Buat Kunci Publik”	Valid
		Memilih menu “Buat Pesan”	Valid
		Memilih menu “Kotak masuk”	Valid
		Melihat detail pesan dan halam dekripsi pesan	Valid
		Memilih menu “tutorial”	Valid
2	Buat Kunci Publik	Mengisi semua kolom input dan menekan tombol “buat kunci publik”	Valid
		Mengkosongkan salah satu kolom input dan menekan tombol “buat kunci publik”	Valid
3	Buat Pesan	Mengisi semua kolom input dan menekan tombol “enkrispsi & kirim sms”	Valid
		Mengkosongkan salah satu kolom input dan menekan tombol “enkripsi & kirim sms”	Valid
4	Kotak Masuk	Memilih salah satu dari daftar pesan yang diterima	Valid
		Mengkosongkan salah satu kolom input pada detail pesan dan menekan tombol “dekripsi pesan”	Valid
5	Detail Pesan	Mengisi kolom input dekripsi pesan dan menekan tombol “dekripsi pesan”	Valid

E-ISSN : 2540 - 8984

JIPI (Jurnal Ilmiah Penelitian dan Pembelajaran Informatika)
Volume 07, Nomor 03, September 2022 : 926–934

IV. KESIMPULAN

Dari hasil penelitian dapat diambil kesimpulan bahwa hasil kombinasi algoritma kriptografi *Diffie-Hellman*, *Message-Diggest 5* dan *Rivest Chiper 4* dari peneliti sebelumnya dapat diterapkan pada aplikasi layanan pesan singkat berbasis Android, dengan menerapkan kriptografi pada aplikasi layanan pesan singkat ini dapat membantu menambah pengamanan terhap pesan tersebut dari orang yang tidak berkepentingan sehingga menambar privasi pada saat berkomunikasi satu sama lain, bahkan SMSC (*Short Message Service Center*) tidak akan dapat membaca pesan tersebut karena pesan akan dienkripsi terlebih dahulu sebelum pesan tersebut dikirim ke SMSC.

Peneliti berharap hasil penelitian ini dapat dikembangkan kembali baik dari segi keilmuan maupun aplikasi hasil dari penelitian.

DAFTAR PUSTAKA

[1] M. H. Masruri, Buku Pintar Android, Jakarta: PT Elex Media Komputindo, 2015.
[2] N. Safaat, Aplikasi Berbasis Android, Bandung: Informatika, 2015.
[3] H. Mukhtar, Kriptografi untuk Keamanan Data, Yogyakarta: DEEPUBLISH, 2018.
[4] J. I. Hanafi and A. Patombongi, "Aplikasi SMS Kriptografi Menggunakan Metode AES Berbasis Android," Jurnal Sistem Informasi Dan Teknik Komputer Catur Sakti, pp. 69-75, 2016.
[5] H. R. Riswanto, K. Safinah, A. N. Muslikah and K. F. Hayati Holle, "Implementasi Teknik Kriptografi Rsa Untuk Pengamanan Data," Jurnal Ilmiah Informatika, 2020.
[6] D. Adhar, "Implementasi Algoritma Des (Data Encryption Standard) Pada Enkripsi Dan Deskripsi Sms Standard) Berbasis Android," Jurnal Teknik Informatika Kaputama (JTIK), 2019.
[7] S. F. Rodiyansyah, T. Wahyuni and D. Sukmana, "Kombinasi Kriptografi Diffie-Hellman, Message-Digest 5 Dan Rivest Chiper 4," Jurnal Ilmiah Intech : Information Technology Journalof UMUS, 2020.
[8] A. A. Wahid, "Analisis Model Waterfall Untuk Pengembangan Sistem Informasi," Metode air terjun atau yang sering disebut metode waterfall, pp. 1-5, 2020.
[9] D. W. Trise Putra and R. Andriani, "Unified Modelling Language (UML) dalam Perancangan Sistem Informasi Permohonan Pembayaran Restitusi SPPD," Jurnal TEKNOIF, pp. 32-39, 2019.
[10] A. Setyawan and J. Wandyatmono, "Sistem Informasi Penggajian Pegawai Kecamatan Geneng Kabupaten Ngawi," Journal Speed, 2009.
[11] V. Febrian, M. R. Ramadhan, M. Faisal and A. Saifudin, "Pengujian pada Aplikasi Penggajian Pegawai dengan menggunakan Metode Blackbox," Jurnal Informatika Universita Pamulang, vol. 5, no. 1, pp. 61-66, 2020.
[12] L. J. Siagian, Otomatisasi Pengujian Perangkat, Yogyakarta: Deepublish, 2018.
[13] I. T. Islamy, S. T. Agatha, R. Ameron, B. H. Fuad, E. and N. A. Rakhmawati, "Pentingnya Memahami Penerapan Privasi di Era Teknologi Informasi," *Jurnal Teknologi Informasi dan Pendidikan*, vol. 11, no. 2, 2018