Terakreditasi SINTA Peringkat 4
Surat Keputusan Dirjen Penguatan Riset dan Pengembangan Ristek Dikti No. 28/E/KPT/2019
masa berlaku mulai Vol.3 No. 1 tahun 2018 s.d Vol. 7 No. 1 tahun 2022

Terbit online pada laman web jurnal:
http://publishing-widyagama.ac.id/ejournal-v2/index.php/jointecs

JOINTECS

JOINTECS
(Journal of Information Technology and Computer Science)

Vol. 7 No. 1 (2022) 17 - 26

e-ISSN:2541-6448 p-ISSN:2541-3619

Implementasi Metode Triple DES Pada Aplikasi Keamanan Pesan Berbasis Mobile

Muhamad Alda[1], Mhd Ikhsan Rifki[2]
[1]Program Studi Sistem Informasi, Fakultas Sains dan Teknologi, Universitas Islam Negeri Sumatera Utara
[2]Program Studi Ilmu Komputer, Fakultas Sains dan Teknologi, Universitas Islam Negeri Sumatera Utara
[1]muhamadalda@uinsu.ac.id, [2]rifki.mhdikhsan@uinsu.ac.id

Abstract

The Message is something that is delivered from sender to receiver. Messages can be text, audio, video or images. The process of delivering text messages on an Android smartphone is not equipped with adequate security. So that messages that have been sent or have been received can be seen by others. Confidentiality of messages that have been sent and received is not guaranteed. Based on these problems, the authors want to build a cryptographic application that can be used in security during the process of sending and receiving messages. The cryptographic application built by the author can encrypt and describe messages to be sent or received using the mobile-based Triple Des method. While the application development method used is the waterfall method, consisting of analysis, design, coding, testing and implementation. With this application, it is hoped that it will provide security for Android smartphone users in sending and receiving messages.

Keywords: *application; cryptography; mobile; messages; triple DES.*

Abstrak

Pesan merupakan Sesuatu yang disampaikan dari pengirim ke penerima. Pesan dapat berupa teks, audio, video maupun gambar. Proses penyampaian pesan teks pada *smartphone* android belum dilengkapi keamanan yang memadai. Sehingga pesan yang telah dikirim ataupun telah diterima dapat dilihat oleh orang lain. Kerahasiaan pesan yang telah dikirim dan diterima menjadi tidak terjamin. Berdasarkan permasalahan tersebut, penulis ingin membangun sebuah aplikasi kriptografi yang dapat digunakan dalam keamanan pada saat proses pengiriman dan penerimaan pesan. Aplikasi kriptografi yang dibangun penulis dapat melakukan enkripsi dan deskripsi pesan yang akan di kirim atau yang telah diterima dengan menggunakan metode *Triple DES* berbasis *mobile*. Sedangkan metode pengembangan aplikasi yang digunakan adalah metode waterfall, terdiri dari analisis, desain, coding, testing dan implementasi. Dengan adanya aplikasi ini, diharapkan akan memberikan keamanan pada pengguna smartphone android dalam melakukan pengiriman maupun penerimaan pesan.

Kata kunci: aplikasi; kriptografi; mobile; pesan; triple DES.

1. Pendahuluan

Pada perkembangan teknologi informasi yang semakin maju, kebutuhan manusia akan sarana informasi semakin bertambah. Namun hal itu seringkali terhambat oleh masalah-masalah seperti jarak, mobilitas, dan keamanan data. Telepon seluler memungkinkan seseorang berkomunikasi dengan jarak jauh [1]. Perkembangan *mobile phone* saat ini sudah memiliki berbagai macam kemampuan seperti akses internet dan juga mempunyai sistem operasi seperti layaknya komputer sehingga sering disebut dengan istilah *smartphone*. Kemampuan *smartphone* untuk keperluan di beberapa bidang pun dikembangkan dengan aplikasi-aplikasi yang mampu mendukung penggunaannya termasuk salah satunya adalah media pendidikan

Diterima Redaksi : 05-01-2022 | Selesai Revisi : 31-01-2022 | Diterbitkan Online : 31-01-2022

kesehatan. Salah satu sistem operasi yang dapat dioperasikan pada *smartphone* adalah android [2].

Android merupakan sistem operasi yang diluncurkan oleh Google khususnya untuk *smartphone* dan tablet. Android memiliki *store* dimana terdapat 1 miliar pengguna yang aktif. Berbicara mengenai pemrograman tentunya tidak terlepas dari *Integrated Development Environment* (IDE) yang bisa dipakai oleh para d*eveloper* [3]. Salah satu masalah yang terjadi yaitu dari sisi keamanan saat melakukan komunikasi menggunakan teks melalui aplikasi yang terdapat pada *smartphone* android. Pesan yang telah diterima atau dikirim masih dapat dilihat oleh orang lain. Sehingga dapat mengakibatkan kerahasiaan dari pesan yang telah dikirim dan diterima menjadi tidak terjaga dengan baik.

Kriptografi merupakan ilmu dan juga seni yang berguna untuk menjaga suatu keamanan pesan dengan menggunakan teknik atau algoritma matematika. Dalam menjaga keamanan data menggunakan kriptografi, data sederhana yang dikirim diubah kedalam bentuk sandi, lalu data sandi hanya bisa dibaca atau dikembalikan ke data yang sebenarnya hanya dengan menggunakan kunci *(key)* tertentu yang dimiliki oleh pihak tertentu [4]. Tujuan dilakukannya penelitian ini adalah untuk membangun sebuah aplikasi kriptografi untuk keamanan pesan berbasis android dengan menggunakan metode Triple DES. Sehingga dapat memberikan keamanan bagi *user* dalam proses mengirim dan menerima pesan pada *smartphone* android.

Penelitian sejenis yang pernah dilakukan antara lain oleh Deny Adhar (2019) dengan judul "Implementasi Algoritma DES *(Data Encryption Standard)* Pada Enkripsi dan Deskripsi SMS Berbasis Android". Pada Penelitian ini membahas tentang proses keamanan pesan SMS dengan metode enkripsi dan deskripsi menggunakan algoritma DES. Sedangkan penelitian yang dilakukan oleh penulis menggunakan metode Triple DES dan pesan yang akan di enkripsi dan deskripsi bukan hanya pesan SMS. Tetapi juga pesan yang menggunakan aplikasi lain [5].

Penelitian sejenis pernah dilakukan oleh Elvara Delfriantina Saragih, et al (2018) dengan judul "Implementasi Algoritma Triple DES dan Algoritma *Advanced Encyption Standard* Dalam Penyandian File Teks". Penelitian ini membahas tentang penyandian pada file dengan menggunakan algoritma Triple DES dan AES. File di sandi secara bertingkat dengan menggunakan algoritma Triple DES terlebih dahulu, kemudian hasil chiperteks dari Triple DES akan di sandi Kembali dengan algoritma AES. Aplikasi yang dibuat berbasis desktop. Sedangkan penulis membuat keamanan pesan dalam bentuk teks berbasis android dengan menggunakan metode Triple DES [6].

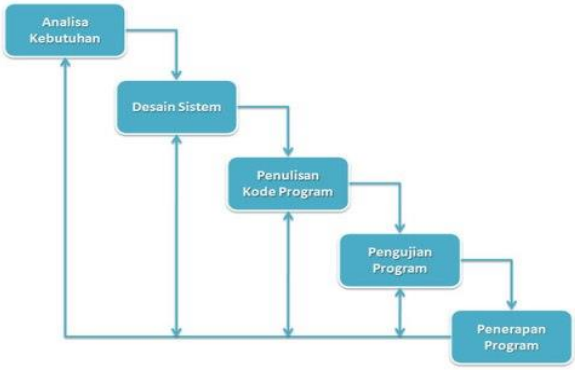
Penelitian sejenis pernah dilakukan oleh Bagas Putra Pratama & Wasis Haryono (2020) dengan judul "Perancangan Aplikasi Kriptografi Pada Dokumen Pengarsipan Dengan Menggunakan Algoritma Triple DES Berbasis WEB". Penelitian ini membahas mengenai keamanan pengarsipan dokumen dengan menggunakan algoritma Triple DES berbasis Web. Hal ini disebabkan karena masih banyak pihak yang tidak bertanggung jawab dapat mengakses file secara bebas. Sehingga dibangun sebuah aplikasi berbasis web yang dapat memberikan keamanan pada file dengan menggunakan algoritma Triple DES. Sedangkan penulis melakukan penelitian untuk membangun sebuah aplikasi keamanan pesan yang akan dikirimkan ataupun diterima dengan menggunakan algoritma Triple DES berbasis android [7].

2. Metode Penelitian

Metode penelitian merupakan langkah-langkah yang dilakukan penulis dalam melakukan penelitian. Dalam melakukan penelitian ini penulis menggunakan tiga metode, terdiri dari metode pengembangan perangkat lunak, metode Triple DES, dan metode pengumpulan data. Metode pengembangan perangkat lunak yang digunakan penulis adalah metode waterfall, sedangkan metode pengumpulan data adalah wawancara, kuisioner dan studi pustaka.

2.1. Metode Pengembangan Perangkat Lunak

Metode pengembangan aplikasi yang digunakan dalam penelitian sesuai dengan tahapan yang terdapat pada model *waterfall*. Model *waterfall* merupakan model klasik yang sederhana dengan aliran sistem linier yang dipergunakan untuk pengembangan perangkat lunak. Model ini diperkenalkan oleh Winston Royce pada tahun 70-an. Pada model ini, keluaran dari tahap sebelumnya merupakan masukan untuk tahap berikutnya [8]. Gambar *waterfall* dapat dilihat pada Gambar 1.



Gambar 1. Model *Waterfall*

Pada model *waterfall* terdapat tahapan-tahapan yang dilakukan dalam proses pengembangan perangkat lunak. Dalam melakukan penelitian ini, penulis melakukan tahapan - tahapan yang terdapat pada model *waterfall* tersebut. Tahapan tersebut terdiri dari tahapan analisa kebutuhan, tahapan desain sistem, tahapan penulisan kode program, tahapan pengujian program, dan tahapan penerapan program.

Tahap analisa kebutuhan merupakan langkah awal untuk menentukan desain sistem dengan menu-menu yang diperlukan oleh *user* untuk melakukan pembangunan aplikasi. Sebelum melakukan analisis kebutuhan, penulis melakukan analisis permasalahan yang terjadi pada keamanan pesan yang dikirimkan dan diterima oleh para pengguna *smartphone* android. Setelah melakukan analisis permasalahan, penulis melakukan analisis dari kebutuhan sistem yang akan dibangun untuk menyelesaikan permasalahan tersebut.

Tahap desain sistem merupakan tahap pembuatan rancangan dari aplikasi yang akan dibangun. Dalam proses pembangunan aplikasi, penulis membuat dua jenis desain sistem, terdiri dari desain sistem secara visual dan desain *interface* sistem. *Tools* yang digunakan dalam membuat desain sistem secara visual adalah UML (*Unified Modeling Language)* yang terdiri dari: *Use Case Diagram, Activity Diagram dan Sequence Diagram* sedangkan tools yang digunakan untuk membuat desain *interface* sistem adalah *Microsoft Visio*.

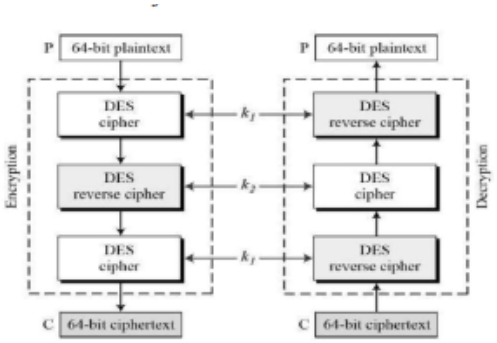
Tahap penulisan kode program merupakan tahapan menerjemahkan desain sistem ke dalam bentuk perintah-perintah yang dimengerti oleh komputer. Pada tahap ini penulis melakukan proses pembangunan aplikasi berdasarkan hasil dari desain yang telah dibuat pada tahapan sebelumnya. Dalam melakukan proses pembangunan aplikasi, penulis menggunakan *tools* Kodular yang dapat diakses secara *online*.

Tahap pengujian program merupakan tahap dimana semua proses *input output* diuji coba sehingga kemungkinan terjadi *error* dan *bug* dapat segera diketahui dan dilakukan perbaikan pada penulisan kode program. Proses pengujian ini dilakukan sebelum aplikasi yang telah dibangun akan diimplementasikan pada lingkungan pemakai. Dalam melakukan proses pengujian, penulis menggunakan strategi *testing* yang terdiri dari *unit test, integration test, operational test* dan *system test.*

Tahapan penerapan program merupakan tahapan terakhir yang dilakukan penulis dalam metode *waterfall*. Pada tahap ini penulis menerapkan aplikasi yang telah dibangun pada lingkungan pemakai setelah melalui tahap pengujian. Penulis menerapkan aplikasi pada para pengguna *smartphone* android dalam memberikan keamanan pada saat mengirim dan menerima pesan.

2.2. Metode Triple DES

Triple Data Encryption Standard (3 DES) adalah jenis kriptografi komputerisasi di mana algoritma *block* cipher diterapkan tiga kali untuk masing-masing blok data. Ukuran kunci meningkat di Triple DES untuk memastikan keamanan tambahan melalui kemampuan enkripsi. Setiap blok berisi 64bit data. Tiga kunci yang disebut sebagai bundel kunci dengan 56 bit per kunci. Ada tiga *keying* Pilihan dalam standar enkripsi data yaitu semua kunci menjadi *independent*, kunci 1 dan kunci 2 menjadi kunci *independent* dan semua tiga kunci yang identic. *Key option* 3 seperti yang ditunjukkan pada Triple DES panjang kunci mengandung 168 bit tapi keamanan kunci jatuh ke 112 bit [9]. Konsep kerja Triple DES dapat dilihat pada Gambar 2.



Gambar 2. Konsep Kerja Triple DES

2.3. Metode Pengumpulan Data

Pengumpulan data merupakan tahapan yang dilakukan penulis dalam memperoleh data yang dibutuhkan dalam penelitian. Dalam proses pengumpulan data, penulis melakukan beberapa metode yang digunakan. Metode tersebut meliputi metode wawancara, metode kuisioner serta metode studi pustaka.

Pada tahap wawancara ini penulis melakukan proses tanya jawab secara langsung kepada para pengguna *smartphone* android. Penulis menyusun beberapa pertanyaan yang ditujukan kepada para pengguna smartphone android. Pertanyaan yang diberikan penulis berhubungan dengan tema penelitian yang dilakukan penulis terkait mengenai proses pengiriman pesan dan keamanan dari pesan yang telah dikirim dan diterima pada *smartphone* android.

Selain menggunakan metode wawancara, penulis juga membuat kuisioner menggunakan Google Form, pada kuisioner ini terdiri dari beberapa pertanyaan berkaitan dengan keamanan pesan pada smartphone android. Kuisioner tersebut kemudian disebarkan pada beberapa pengguna *smartphone* android. Hal ini bertujuan untuk memperoleh data yang lebih akurat dari berbagai sumber.

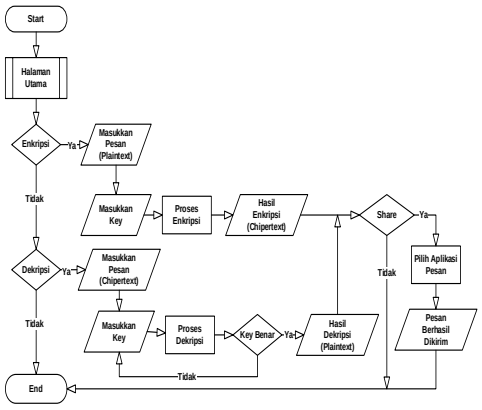
Dalam tahap metode studi pustaka ini, penulis mencari sumber referensi yang dibutuhkan dalam melakukan penelitian yang lakukan. Referensi yang dibutuhkan penulis terkait dengan kriptografi, metode Triple DES dan pembangunan aplikasi android. Penulis mencari referensi dari berbagai sumber, baik dari buku, jurnal, internet maupun dari sumber lainnya.

3. Hasil dan Pembahasan

Pada bagian ini penulis membahas dan menjelaskan mengenai tahapan – tahapan yang dilakukan pada penelitian ini. Tahapan yang dilakukan penulis dalam

penelitian ini, sesuai dengan tahapan yang terdapat pada metode *waterfall*. Hasil dan pembahasan pada penelitian ini terdiri dari analisis permasalahan, analisis kebutuhan sistem, perancangan aplikasi, pengujian aplikasi dan penerapan aplikasi. Selain itu, penulis juga menampilkan hasil dari setiap tahapan penelitian yang dilakukan.

Sebelum melakukan tahapan perancangan, penulis terlebih dahulu melakukan analisis permasalahan mengenai sistem yang sedang berjalan. Analisis yang dilakukan oleh penulis berfokus pada permasalahan keamanan yang terjadi pada proses pengirima dan penerimaan pesan di s*martphone* android. Permasalahan yang terjadi pada pesan yang dikirim ataupun yang diterima. Selama ini pesan yang telah dikirim ataupun diterima masih dalam bentuk *plaintext* yang dapat mudah dibaca oleh siapapun. Sehingga terjadi adanya *user* yang dapat membaca ataupun mengakses pesan *user* lain secara bebas pada *smartphone* android. Sehingga kerahasiaan pesan tersebut menjadi tidak aman.



Gambar 3. *Flowchart* Aplikasi

Berdasarkan hasil dari analisis sistem yang telah berjalan, penulis menentukan solusi yang dapat dilakukan untuk mengatasi permasalahan keamanan yang terjadi pada proses penyampaian pesan di *smartphone* android. Penulis melakukan penelitian dengan membangun sebuah aplikasi keamanan pesan untuk memberikan keamanan pengiriman pesan pada *smartphone* android dengan menggunakan metode Triple DES. Pesan yang akan dikirim akan di enkripsi menjadi *chipertext* kemudian setelah penerima menerima pesan, maka pesan tersebut akan di deskripsi kembali menjadi *plaintext* Penelitian ini dilakukan dan ditujukan penulis untuk semua pengguna *smartphone* android. Alur dan fungsi dari aplikasi yang akan dibangun pada penelitian ini di gambarkan dalam bentuk *flowchart*. *Flowchart* dapat dilihat pada Gambar 3.

Enkripsi merupakan istilah lain dari proses menyandikan data penting ke dalam bentuk simbol-simbol yang tidak dapat dimengerti lagi oleh pihak lain sehinggan keaslian dan keamanan data dapat terjaga. Sedangkan Dekripsi adalah proses untuk merubah atau mengembalikan data bersandi ke bentuk aslinya agar arti data dapat dimengerti oleh penerima [10]. Proses enkripsi dan dekripsi algoritma Triple DES dapat dicapai dengan beberapa cara, yaitu: Cara Pengenkripsian dan Pendekripsian. Enkripsi dan dekripsi dapat dilihat pada Tabel 1

Tabel 1. Cara Enkripsi dan Deksripsi

Cara	Enkripsi	Dekripsi
1	DES – EDE2 $K_1 \neq K_2, K_3 = K_1$ $C = E [D \{E (P, K_1), K_2\}, K_3]$	DES – DED2 $K_1 \neq K_2, K_3 = K_1$ $P = D [E \{D (C, K_3), K_2\}, K_1]$
2	DES – EEE2 $K_1 \neq K_2, K_3 = K_1$ $C = E [E \{E (P, K_1), K_2\}, K_3]$	DES – DDD2 $K_1 \neq K_2, K_3 = K_1$ $P = D [D \{D (C, K_3), K_2\}, K_1]$
3	DES – EDE3 $K_1 \neq K_2 \neq K_3 \neq K_1$ $C = E [D \{E (P, K_1), K_2\}, K_3]$	DES – DED3 $K_1 \neq K_2 \neq K_3 \neq K_1$ $P = D [E \{D (C, K_3), K_2\}, K_1]$

Algoritma merupakan suatu metode yang digunakan untuk menyelesaikan suatu masalah. Algoritma merupakan langkah-langkah untuk merancang program yang dinyatakan dalam bahasa yang dapat dimengerti. Dalam proses kriptografi menggunakan algortima Triple DES terdiri dari dua algoritma yang digunakan, yaitu enkripsi dan dekripsi.

Dalam-dalam melakukan proses enkripsi terdapat proses pembangkitan kunci. Proses pembangkitan kunci pada proses enkripsi dapat dilakukan melalui contoh berikut, yaitu contoh plainteks adalah ALIKHSAN dengan kunci UINSUMUT. Langkah pertama yang dilakukan adalah dengan mengubah plainteks dalam bentuk bilangan biner. Berikut adalah hasil perubahan plainteks menjadi bilangan biner yaitu A = 01000001, L = 01001100, I = 01001001, K = 01001011, H = 01001000, S = 01010011, A = 01000001, N = 01001110. Setelah itu, proses perubahan key menjadi biner, berikut adalah hasilnya U = 01010101, I = 01001001, N = 01001110, S = 01010011, U = 01010101, M = 01001101, U = 01010101, T = 01010100. Kemudian hasil dari perubahan tersebut merupakan kunci di-*generate* untuk melakukan enkripsi plainteks dengan menggunakan tabel permutasi kompresi PC-1. Pada tahap ini dilakukan kompresi dengan membuang 1 bit masing-masing blok kunci dari 64 bit menjadi 56 bit. PC-1 dapat dilihat pada Tabel 2.

Tabel 2. PC-1

Urutan Bit Tabel PC-1						
57	49	41	33	25	17	9
1	58	50	42	34	26	18
10	2	59	51	43	35	27
19	11	3	60	52	44	36
63	55	47	39	31	23	15
7	62	54	45	38	30	22
14	6	61	53	45	37	29
21	13	5	28	20	12	4

Dari Tabel 2, tidak terdapat urutan bit 8, 16, 24, 32, 40, 48, 56, 64 karena telah dilakukan kompres. Berikut adalah hasil dari *output*-nya CD(k) = 0000000 0111111 1100000 0001101 0000110 0111101 0100100 1101001, Kemudian Pecah CD(k) menjadi dua bagian kiri dan kanan, sehingga menjadi C_0 = 0000000 0111111 1100000 0001101 dan D_0 = 0000110 0111101 0100100 1101001. Setelah itu melakukan pergeseran kiri *(left shift)* pada C_0 dan D_0 sebanyak 1 atau 2 kali berdasarkan jumlah putaran sesuai dengan Tabel. *Left shift* dapat dilihat pada Tabel 3.

Tabel 3. *Left Shift*

Putaran Ke-i	Jumlah Pergeseran *(left shift)*
1	1
2	1
3	2
4	2
5	2
6	2
7	2
8	2
9	1
10	2
11	2
12	2
13	2
14	2
15	2
16	1

Lakukan pergeseran *left shift* berdasarkan Tabel 3 sebanyak 16 kali putaran, sehingga menghasilkan *output* $C_{16}D_{16}$ = 0000000 0111111 110000 0001101 0011001 1110101 0010001 1010010. Kemudian Pecah CD(k) menjadi dua bagian kiri dan kanan, sehingga menjadi C_{16} = 0000000 0111111 110000 0001101 dan D_{16} = 0011001 1110101 0010001 1010010. Setiap putaran digabungkan kembali menjadi CiDi dan di-input ke dalam tabel *permutasi compression* (PC-2) dan terjadi kompresi data CiDi 56 bit menjadi CiDi 48 bit.

Tabel 4. PC-2

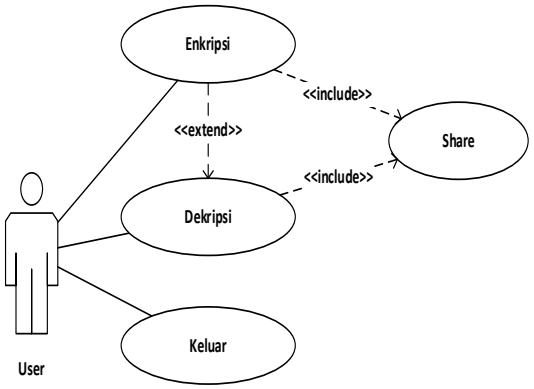
Urutan Bit Tabel PC-2					
14	17	11	24	1	5
3	28	15	6	21	10
23	19	12	4	26	8
16	7	27	20	13	2
41	52	31	37	47	55
30	40	51	45	33	48
44	49	39	56	34	53
46	42	50	36	29	32

Pada proses kompresi data CiDi 56 bit menjadi CiDi 48 bit, Data C1D1 akan dilakukan proses putaran sebanyak 16 kali berdasarkan pada data Tabel 4 dan cara tersebut dilakukan sebanyak tiga kali. Dari proses yang dilakukan, maka dihasilkan sebuah *output* yang kemudian *output* tersebut akan dikonversi menjadi chiperteks berikut GbHPQJiyBB1Mh1L37TkBqw. Chiperteks tersebut merupakan hasil dari plainteks yang telah di enkripsi dengan menggunakan algoritam Triple DES

Untuk proses dekripsi terhadap cipherteks merupakan kebalikan dari proses enkripsi. Triple DES menggunakan algoritma yang sama untuk proses enkripsi dan dekripsi. Jika pada proses enkripsi urutan kunci internal yang digunakan adalah K1, K2, …, K16, maka pada proses dekripsi urutan kunci yang digunakan adalah K16, K15, …, K1. Untuk tiap putaran 16, 15, …, 1, kemudian di lakukan pengulangan sebanyak tiga kali sehingga chiperteks akan diubah menjadi plainteks ALIKHSAN.

Tools yang digunakan dalam membuat rancangan sistem informasi adalah Diagram UML (*Unified Modeling Languange)*. UML yang merupakan singkatan dari *"Unified Modelling Language"* yaitu suatu metode permodelan secara visual untuk sarana perancangan sistem berorientasi objek dan UML juga sebagai suatu bahasa yang sudah menjadi standar pada visualisasi, perancangan dan juga pendokumentasian sistem [11]. Diagram UML (*Unified Modeling Languange)* yang digunakan dalam penelitian ini terdiri dari *Use Case Diagram, Activity Diagram dan Sequence Diagram*.

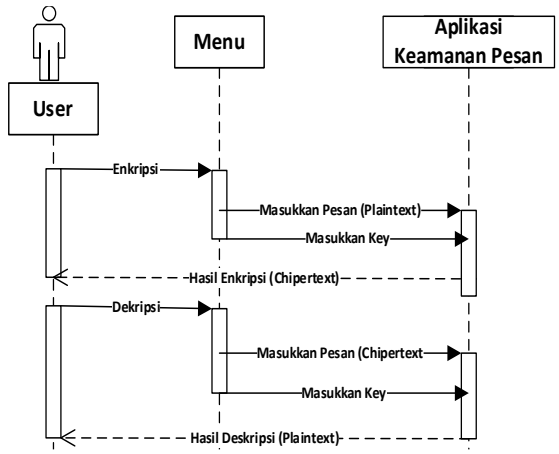
Use Case Diagram merupakan diagram yang mendeskripsikan interaksi antara satu atau lebih aktor dengan aplikasi yang akan dibuat [12]. Dalam aplikasi yang akan dibangun, *user* dapat melakukan enkripsi dengan memasukkan pesan yang akan di enkripsi kemudian memasukkan kunci yang digunakan dalam proses enkripsi tersebut, kemudian pesan yang telah di enkripsi dapat di share menggunakan aplikasi pesan yang terdapat pada *smartphone* android, setelah itu *user* juga dapat melakukan deskripsi dengan memasukkan chiperteks dan memasukkan *key* yang digunakan dalam melakukan enkripsi. Gambar *use case diagram* dapat dilihat pada Gambar 4.



Gambar 4. *Use Case Diagram*

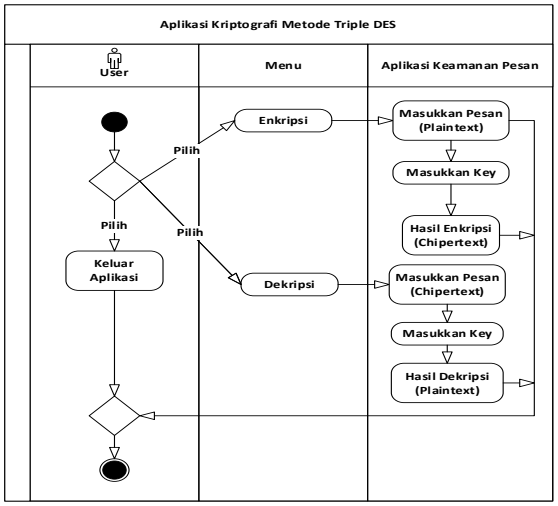
Sequence Diagram merupakan diagram yang menggambarkan bagaimana *user* melakukan interaksi dengan aplikasi untuk mendapatkan informasi yang dibutuhkan [13]. Pada diagram ini, penulis menggambarkan tahapan yang dilakukan user pada saat

menggunakan aplikasi yang akan dibangun. Gambar *sequence diagram* dapat dilihat pada Gambar 5.



Gambar 5. *Sequence Diagram*

Activity diagram menggambarkan rangkaian aliran dari aktivitas, digunakan untuk mendeskripsikan aktivitas yang dibentuk dalam satu operasi sehingga dapat juga untuk aktivitas lainnya [14]. Pada diagram ini, penulis menggambarkan aktivitas yang dilakukan sistem dalam menjalankan fungsi yang dipilih oleh *user*. Gambar *activity diagram* dapat dilihat pada Gambar 6.



Gambar 6. *Activity Diagram*

Dalam melakukan pengujian aplikasi penulis menggunakan strategi testing yang digunakan [15]. Strategi testing ini digunakan untuk melakukan pengujian aplikasi secara akurat sehingga menghasilkan aplikasi yang berjalan dengan baik. Strategi testing yang digunakan penulis terdiri dari Strategi testing yang digunakan penulis terdiri dari *unit test, integration test, operational test* dan *system test*.

Unit test mencakup set satu atau lebih program yang dirancang untuk memverifikasi unit kode sumber, seperti metode atau kelas. Platform Android dilengkapi kerangka kerja Junit 3.0 yang terintegrasi sebelumnya. Kerangka kerja open source untuk mengotomatisasi Pengujian Unit. Kerangka Pengujian Android adalah alat yang ampuh bagi pengembang untuk menulis program pengujian unit yang efektif. Dalam melakukan pengujian unit, penulis melakukan pengujian dari setiap unit atau *user interface* yang terdapat pada aplikasi keamanan pesan. Seperti *button, dialog box, image, menu, touch* dan lain sebagainya.

Tabel 5. Pengujian Aplikasi

Modul Pengujian	Skenario Pengujian	Hasil Diharapkan	Kesimpulan
Button Enkripsi	- Buka aplikasi - Pilih dan klik button enkripsi	Tampilkan halaman form enkripsi	Valid
Button Dekripsi	- Buka aplikasi - Pilih dan klik button dekripsi	Tampilkan halaman form dekripsi	Valid
Button Sharing	- Buka aplikasi - Masukkan pesan dan key - Klik enkripsi - Pilih dan klik button sharing	Tampilkan aplikasi pesan pada *smartphone* android	Valid
Form Enkripsi	- Masukkan Pesan dan Masukan Key - klik *"Enkripsi"*	Pesan berhasil di enkripsi dan siap untuk dikirimkan	Valid
Form Dekripsi	- Masukkan Pesan dan Masukan Key - klik *"Dekripsi"*	Pesan berhasil di dekripsi	Valid
Sharing	- Pilih Button Share - Pilih jenis aplikasi pesan	Pengiriman pesan berhasil	Valid

Dalam Pengujian Integrasi, semua modul atau unit yang diuji akan digabungkan dan diverifikasi. Di Android, tes integrasi sering melibatkan pemeriksaan integrasi dengan komponen Android seperti pengujian Layanan, pengujian aktivitas, pengujian Penyedia Konten, dan lain-lain. Dalam pengujian ini, penulis melakukan pengujian terhadap setiap proses dan modul yang terdapat pada aplikasi keamanan pesan dan hubungan dari masing-masing modul. Seperti proses enkripsi, dekripsi dan proses *sharing* pesan melalui aplikasi yang terdapat pada smartphone android.

Operasional juga disebut Tes Fungsional atau Tes Penerimaan. Operational tes tingkat tinggi yang dirancang untuk memeriksa kelengkapan dan kebenaran sistem informasi. Pada pengujian ini, penulis melakukan pengujian dari setiap kelengkapan formulir dari setiap proses yang terdapat pada aplikasi keamanan pesan. Seperti proses enkripsi pesan dan proses dekripsi pesan. Pada setiap proses, *user* harus melengkapi data yang dibutuhkan secara lengkap, jika data yang dimasukkan tidak lengkap, maka aplikasi akan menampilkan sebuah notifikasi. Data tersebut meliputi data yang akan di enkripsi atau dekripsi serta *key* yang dimasukkan. Dalam Pengujian Sistem, sistem diuji secara keseluruhan dan

interaksi antara komponen, perangkat lunak, dan perangkat keras diperiksa. Di Android, Pengujian Sistem biasanya mencakup Tes GUI, Tes kegunaan, Tes kinerja. Pengujian ini merupakan pengujian kompleks yang dilakukan oleh penulis dari aplikasi yang telah dibangun. Penulis melakukan pengujian dimulai dari pengujian interface atau tampilan aplikasi, kinerja dari setiap proses, input, proses serta output.

Metode yang digunakan penulis dalam melakukan pengujian adalah *black box testing*. *Black box testing* merupakan teknik pengujian yang berfokus pada spesifikasi fungsional dari perangkat lunak [16]. Hasil pengujian aplikasi dapat dilihat pada Tabel 5.

3.1. Penerapan Aplikasi

Tahap Implementasi aplikasi merupakan tahap penerjemahan perancangan berdasarkan hasil analisis ke dalam suatu bahasa pemrograman tertentu serta penerapan perangkat lunak yang dibangun pada lingkungan yang sesungguhnya. Setelah implementasi maka dilakukan pengujian sistem yang baru, dimana akan dilihat kekurangan yang terdapat pada aplikasi yang baru untuk selanjutnya diadakan pengembangan sistem [17]. Tampilan halaman dari aplikasi keamanan pesan yang akan dibangun. Tampilan halaman aplikasi terdiri dari tampilan halaman utama, halaman Enkripsi dan halaman Dekripsi.

Halaman utama merupakan halaman awal yang muncul saat *user* menggunakan aplikasi keamanan pesan. Pada halaman ini, penulis dapat memilih beberapa menu yang tersedia, antara lain menu Enkripsi, menu Dekripsi dan menu *Close*. Tampilan halaman utama dapat dilihat pada Gambar 7.

Gambar 7. Tampilan Halaman Utama

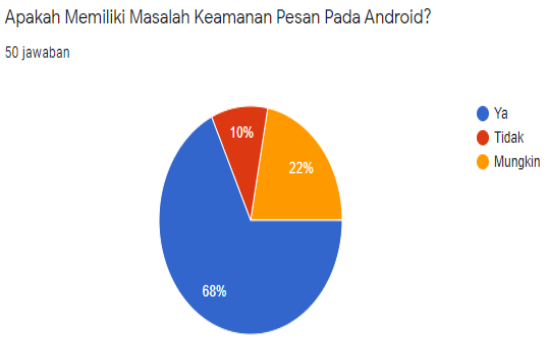
Pada halaman ini, *user* dapat melakukan enkripsi dari pesan yang akan dikirimkan dengan memasukkan pesan tersebut dan *key* pada kolom yang telah disediakan. Pesan yang telah di enkripsi dapat dikirimkan secara langsung kepada penerima melalui aplikasi pesan yang terdapat pada *smartphone* android. Tampilan halaman enkripsi dapat dilihat pada Gambar 8.

Gambar 8. Tampilan Halaman Enkripsi

Pada halaman ini, *user* dapat melakukan dekripsi dari pesan yang telah diterima kedalam bentuk yang mudah dimengerti *(Plaintext)*. Proses dekripsi pesan dengan cara memasukkan pesan diterima dalam bentuk *chipper text* dan memasukkan *key* yang telah ditentukan. *Key* yang digunakan dalam melakukan dekripsi data Tampilan halaman dapat dilihat pada Gambar 9.

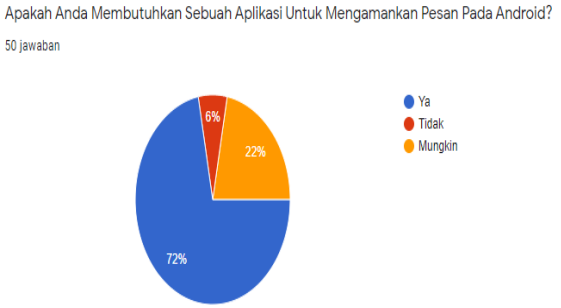
Gambar 9. Tampilan Halaman Dekripsi

Dalam melakukan penelitian ini, penulis melakukan *survey* yang berkaitan dengan tema penelitian yang dibahas. *Survey* yang dilakukan penulis berupa pertanyaan mengenai keamanan pesan pada *mobile* android, kebutuhan aplikasi dalam keamanan pesan pada *mobile* android dan manfaat kegunaan aplikasi yang dibangun dalam memberikan keamanan pesan pada *mobile* android. *Survey* yang telah dibuat kemudian diberikan kepada pengguna *mobile* android untuk melakukan pengisian *survey* tersebut. Dalam melakukan survey ini penulis menggunakan sample pengguna sebanyak 50 orang. Setiap pertanyaan yang terdapat pada form survey disesuaikan dengan permasalahan yang diangkat pada penelitian.



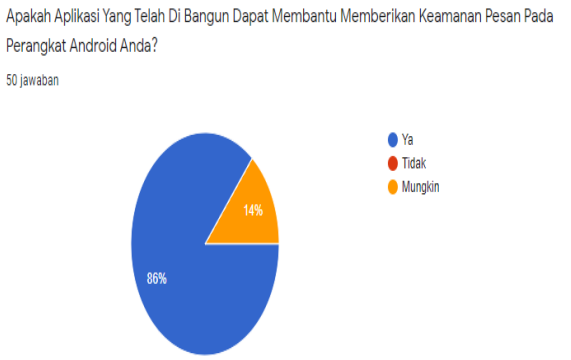
Gambar 10. Hasil Survey Masalah Keamanan Pesan

Pada Gambar 10 merupakan hasil survey kepada pengguna mengenai keamanan pesan pada s*martphone* android. Pada hasil survey tersebut sebanyak 68 % *user* mengalami permasalahan mengenai keamanan pesan pada *smartphone* android. Hal ini berkaitan dengan pengguna lain yang mengakses pesan tanpa izin dari pemilik *smartphone* android, sehingga dapat merugikan pemilik dalam menjaga *privacy* pesan yang diterima ataupun yang dikirim.



Gambar 11. Hasil Survey Kebutuhan Aplikasi Keamanan Pesan

Pada Gambar 11 merupakan hasil survey pengguna smartphone android mengenai kebutuhan aplikasi keamanan pesan. Berdasarkan hasil survey pada Gambar 10, maka pengguna membutuhkan sebuah aplikasi yang dapat digunakan untuk melakukan keamanan pesan tersebut. Pengguna membutuhkan sebuah aplikasi yang memberikan keamanan pesan pada *smartphone* android sehingga tidak dapat di akses oleh pihak lain.



Gambar 12. Hasil Survey Manfaat Aplikasi Keamanan Pesan

Pada Gambar 12 merupakan hasil survey mengenai penerapan aplikasi keamanan pesan yang telah dibangun. Sebanyak 86 % pengguna merasakan manfaat dari aplikasi yang telah dibangun. Aplikasi yang dibangun menggunakan metode Triple DES sehingga memberikan keamanan lebih tinggi dibandingkan dengan metode DES. Hal ini dikarenakan proses dilakukan dengan pengulangan sebanyak tiga kali. Sehingga pesan yang dihasilkan akan sulit dimengerti oleh pihak yang tidak mendapatkan akses pada aplikasi.

4. Kesimpulan

Setelah melakukan penelitian ini, maka penulis mengambil kesimpulan dari pembangunan aplikasi keamanan pesan dengan menggunakan metode Triple Des berbasis android, yaitu aplikasi yang dibangun dapat membantu *user* dalam memberikan keamanan pada saat proses pengiriman pesan melalui *smartphone* android, aplikasi yang dibangun dapat melakukan *enkripsi* dan *dekripsi* dari pesan yang akan dikirim maupun yang telah diterima dengan menggunakan *key* yang sama pada saat proses *enkripsi* dan *dekripsi* dengan metode Triple Des dan pesan yang telah di enkripsi dapat langsung dikirim atau di *share* kepada penerima melalui aplikasi pesan yang terdapat pada *smartphone* android. Aplikasi yang dibangun dapat dikembangkan dengan menggunakan metode yang berbeda pada kriptografi. Metode yang digunakan dapat meningkatkan proses keamanan pesan pada *smartphone* android. Selain itu, aplikasi ini juga dapat dikembangkan pada perangkat *smartphone* berbasis IOS. Aplikasi keamanan pesan yang telah dibangun dapat memberikan manfaat kepada para pengguna mobile android dalam memberikan pesan. Dalam hal ini, peneliti melakukan survey kepada pengguna aplikasi keamanan pesan yang telah dibangun. Jumlah sample pengguna yang digunakan pada survey adalah 50 orang. Dari 50 orang tersebut 86 % mengatakan bahwa aplikasi yang dibangun memberikan manfaat dalam memberikan keamanan pesan, sedangkan 14 % sisanya mengatakan mungkin bermanfaat.

Daftar Pustaka

[1] R. Yusuf and M. R. Suheri, “Pengamanan Sms Pada Telepon Seluler Berbasis Android Menggunakan Algoritma Triple Des,” *Petir*, vol. 9, no. 1, pp. 63–70, 2019, doi: 10.33322/petir.v9i1.191.

[2] D. Fransisca and R. N. Yusuf, “Jurnal Kesehatan Medika Saintika,” *J. Kesehat. Med. Saintika Vol.*, vol. 10, no. 2, pp. 11–24, 2018.

[3] W. Gunawan, “Pengembangan Aplikasi Berbasis Android Untuk Pengenalan Huruf Hijaiyah,” *J. Inform.*, vol. 6, no. 1, pp. 69–76, 2019, doi: 10.31311/ji.v6i1.5373.

[4] R. Awwaliyah and K. Agung, “Pengkodean Polyalphabetic dengan Modifikasi Algoritma ElGamal- Caesar Cipher,” vol. 4, pp. 540–547,

2021.

[5] D. Adhar, "Implementasi Algoritma Des (Data Encryption Standard) Pada Enkripsi Dan Deskripsi Sms Berbasis Android," *J. Tek. Inform. Kaputama*, vol. 3, no. 2, pp. 53–60, 2019, [Online]. Available: https://jurnal.kaputama.ac.id/index.php/JTIK/article/view/185.

[6] E. D. Saragih, N. A. Hasibuan, and E. Bu'ulolo, "Implemantasi Algoritma Triple DES Dan Algoritma Advanced Encryption Standard dalam Penyandian File," *Maj. Ilm. INTI*, vol. 13, no. 3, pp. 263–269, 2018.

[7] B. P. Pratama and W. Haryono, "Perancangan Aplikasi Kriptografi Pada Dokumen Pengarsipan Dengan Menggunakan Algoritma Triple DES," vol. 1, no. 4, pp. 204–212, 2020.

[8] C. Tristianto, "Penggunaan Metode Waterfall Untuk Pengembangan Sistem Monitoring Dan Evaluasi Pembangunan Pedesaan," *J. Teknol. Inf. ESIT*, vol. XII, no. 01, pp. 8–22, 2018.

[9] F. Wafi, A. F. Oklilas, and S. D. Siswanti, "Implementasi Algoritma Triple-Des (3des) dalam Pengamanan ID Tag Rfid Berbasis Client Server," vol. 3, no. 1, pp. 3–6, 2017.

[10] N. R. Yanti, A. Alimah, and D. A. Ritonga, "Implementasi Algoritma Data Encryption Standard Pada Penyandian Record Database," *J-SAKTI (Jurnal Sains Komput. dan Inform.*, vol. 2, no. 1, p. 23, 2018, doi: 10.30645/j-sakti.v2i1.53.

[11] A. Yunus and A. C. Rohman, "Sistem Pendukung Keputusan Penentuan Lahan Pertanian, Pertambangan, Dan Perindustrian (Softplet) Dengan Menggunakan Metode Smarter," *SMARTICS J.*, vol. 4, no. 1, pp. 5–10, 2018, doi: 10.21067/smartics.v4i1.2693.

[12] S. Kurniawan, T. Bayu, "Perancangan Sistem Aplikasi Pemesanan Makanan dan Minuman Pada Cafetaria NO Caffe di TAnjung Balai Karimun Menggunakan Bahasa Pemrograman PHP dan My.SQL," *J. Chem. Inf. Model.*, vol. 53, no. 9, pp. 1689–1699, 2020.

[13] M. Alda, "Sistem Informasi Laundry Menggunakan Metode Waterfall Berbasis Android Pada Simply Fresh Laundry," vol. 3, no. 2, pp. 1–8, 2019.

[14] T. D. C. Rizki Septian Anwar, Mikhratunnisa, "Perancangan Aplikasi Berbasis Android Dengan Metode Economic Order Quantity Di PT. Samawa Tirta Alam Sumbawa," *J. TAMBORA*, vol. 3, no. 2, pp. 49–59, 2019.

[15] M. Alda and Afifudin, "Application of New Student Registration Based on Mobile Application," *JITK (Jurnal Ilmu Pengetah. dan Teknol. Komputer)*, vol. 6, no. 1, pp. 129–136, 2020, doi: 10.33480/jitk.v6i1.1382.

[16] T. Snadhika Jaya, "Pengujian Aplikasi dengan Metode Blackbox Testing Boundary Value Analysis (Studi Kasus: Kantor Digital Politeknik Negeri Lampung)," *J. Inform. J. Pengemb. IT*, vol. 03, no. 02, pp. 45–48, 2018.

[17] S. Surahman and E. B. Setiawan, "Aplikasi Mobile Driver Online Berbasis Android Untuk Perusahaan Rental Kendaraan," *J. Ultim. InfoSys*, vol. 8, no. 1, pp. 35–42, 2017, doi: 10.31937/si.v8i1.554.

Halaman ini sengaja dikosongkan