APLIKASI PENYANDIAN PESAN TEKS BERBASIS WEB MENGGUNAKAN ALGORITMA BLOWFISH

Nelly Permatasari[1*], Yessi Mardiana[2]
Program Studi Rekayasa Sistem Komputer, Fakultas Ilmu Komputer,
Universitas Dehasen Bengkulu[1,2]
Nelly_permatasari@gmail.com[1], yessimrd@unived.ac.id[2]*

ABSTRACT

The Blowfish algorithm is one of the existing encoding systems. Encoding aims to make a message more secure for its confidentiality. The blowfish algorithm is one of the modern cryptographic algorithms that uses symmetric keys in the encryption and decryption process. The application of the blowfish algorithm in this study is to secure text messages between the sender and recipient of the text message through a web-based application. Cryptography is the art and science of protecting data transmission by converting it into a certain code and is only intended for people who only have a key to change the code back which functions to maintain the confidentiality of data or messages. Applications for sending
messages using the blowfish algorithm are made using the PHP programming language and MySQL database. This web-based text message encoding application consists of several menus, including login menus, lists, incoming messages and sending messages. The web-based text message encoding application runs well according to each existing menu.

Keywords: Blowfish,PHP and MySQL,

ABSTRAK

Algoritma Blowfish merupakan salah satu sistem penyadian yang ada. Penyadian bertujuan untuk membuat sebuah pesan menjadi lebih terjamin kerahasiaannya. Algoritma blowfish merupakan salah satu algoritma kriptografi modern yang menggunakan kunci simetris dalam proses enkripsi dan dekripsi. Penerapan algoritma blowfish dalam penelitian ini yakni untuk mengamankan pesan teks antara pengirim dan penerima pesan teks tersebut melalui aplikasi berbasis web. Kriptografi merupakan seni dan ilmu untuk memproteksi pengiriman data dengan mengubahnya menjadi kode tertentu dan hanya ditujukan untuk orang yang hanya memiliki sebuah kunci untuk mengubah kode itu kembali yang berfungsi dalam menjaga kerahasiaan data atau pesan. Aplikasi pengiriman pesan dengan menggunakan algoritma blowfish dibuat dengan menggunakan Bahasa pemrograman PHP dan database MySQL. Aplikasi penyadian pesan teks berbasis web ini terdiri dari beberapa menu, diantaranya menu login, daftar, pesan masuk dan kirim pesan. Aplikasi penyadian pesan teks berbasis web berjalan dengan baik sesuai dengan masing-masing menu yang ada.

Kata kunci : Blowfish, PHP dan MySQL,

1. Pendahuluan

Pertukaran informasi mempermudah pengguna dalam mendapatkan informasi secara cepat dan dapat saling berinteraksi satu dengan yang lainnya. Banyak keuntungan yang dapat diperoleh dengan melakukan pertukaran informasi, yaitu untuk mengefisienkan waktu sehingga informasi dapat diterima tepat waktu. Namun di samping keuntungan tersebut terdapat kelemahan dimana munculnya pihak ketiga yang menginginkan informasi tersebut untuk keperluan pribadi dan tentunya membuat informasi menjadi tidak rahasia lagi.

Oleh karena itu, dalam penelitian ini, dilakukan pengembangan dengan membuat aplikasi penyandian pesan teks yang membuat informasi tersebut dirahasiakan. Adapun proses keamanan dilakukan dengan catatan ada pengirim dan ada penerima pesan teks tersebut. Dimana

pengirim mengirimkan pesan teks untuk dienkripsi, kemudian menentukan kunci, hasil dari pesan teks terenkripsi tersebut akan dikirim ke penerima. Dan dari sisi penerima akan membuka pesan teks tersebut dengan kunci yang telah ditentukan, sehingga pesan teks tersebut dapat dibaca.

Algoritma blowfish merupakan salah satu algoritma kriptografi modern yang menggunakan kunci simetris dalam proses enkripsi dan dekripsi. Penerapan algoritma blowfish dalam penelitian ini yakni untuk mengamankan pesan teks antara pengirim dan penerima pesan teks tersebut melalui aplikasi berbasis web.

Penelitian terkait juga dilakukan oleh (Nurani & Siswanto, 2018). Penelitian ini bertujuan untuk membuat sistem Secure Chatting (Instan Messanging) menggunakan aplikasi enkripsi dan deskripsi dengan menggunakan Algoritma Blowfish. Hasil dari pengujian yang di dapatkan bahwa untuk enkripsi dan dekripsi pesan atau karakter tidak membutuhkan banyak waktu hanya tidak melebihi 1 detik. Kesimpulan yang di dapat jumlah karakter hampir tidak mempengaruhi waktu proses enkripsi dan dekripsi.

Berdasarkan uraian tersebut di atas, maka penulis tertarik untuk mengangkat judul penelitian yaitu tentang **"Aplikasi Penyandian Teks Berbasis** Web **Menggunakan Algoritma Blowfish"**

2. Tinjauan Pustaka dan Pengembangan Hipotesis

A. Kriptografi

Blowfish termasuk dalam enkripsi block Chiper 64-bit dengan panjang kunci minimal 32 bit sampai 448-bit. Blowfish alias "OpenPGP.Cipher.4" merupakan enkripsi yang termasuk dalam golongan Symmetric Cryptosystem, metode enkripsinya mirip dengan DES (DES like Cipher) diciptakan oleh seorang Cryptanalyst bernama Bruce Schneier Presiden perusahaan Counterpane Internet Security, Inc (Perusahaan konsultan tentang kriptografi dan keamanan komputer) dan dipublikasikan tahun 1994. Dibuat untuk digunakan pada komputer yang mempunyai mikroprosesor besar (32-bit k eatas dengan cache data yang besar) (Wardoyo, 2016)

Blowfish dikembangkan untuk memenuhi kriteria desain yang cepat dalam implementasinya di mana pada keadaan optimal dapat mencapai 26 clock cycle per Byte, kompak di mana dapat berjalan pada memori kurang dari 5 KB, sederhana dalam algoritmanya sehingga mudah diketahui kesalahannya, dan keamanan yang variable panjang kunci bervariasi (minimum 32 bit, maksimum 448 bit, multiple 8 bit, default 128 bit).

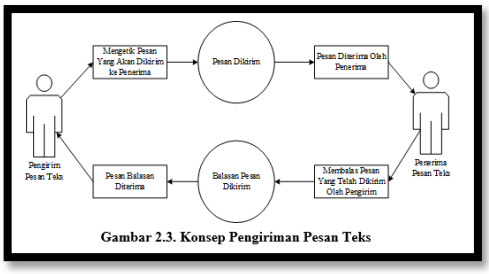
B. Kriptografi

Sejarah kriptografi sebagian besar merupakan sejarah kriptografi klasik, yaitu metode enkripsi yang menggunakan kertas dan pensil atau mungkin dengan bantuan alat mekanik sederhana. Secara umum algoritma kriptografi klasik dikelompokkan menjadi dua kategori, yaitu algoritma transposisi (transposition cipher) dan algoritma substitusi (substitution cipher). Cipher transposisi mengubah susunan huruf-huruf di dalam pesan, sedangkan cipher substitusi mengganti setiap huruf atau kelompok huruf dengan sebuah huruf atau kelompok huruf lain (Pabokory, Astuti, & Kridalaksana, 2015).

Kriptografi merupakan seni dan ilmu untuk memproteksi pengiriman data dengan mengubahnya menjadi kode tertentu dan hanya ditujukan untuk orang yang hanya memiliki sebuah kunci untuk mengubah kode itu kembali yang berfungsi dalam menjaga kerahasiaan data atau pesan. Dalam kriptografi, data atau pesan yang dikirimkan melalui jaringan akan disamarkan sedemikian rupa. Sehingga seandainya data tersebut bisa diperoleh dan dibaca oleh orang lain, maka pihak yang tidak berhak atau berwenang tersebut tidak akan bisa mengerti arti dari data tersebut.

C. Pesan Teks

Pesan teks adalah suatu layanan yang memungkinkan user dapat mengirim sebuah pesan yang berisi informasi kepada user lain secara cepat dengan biaya yang kecil. Pesan teks yang dikirim jauh lebih cepat daripada pengiriman pesan suara atau video karena hanya terdiri dari karakter teks dan angka (Ramdan & Maliki, 2019).



Gambar 2.3. Konsep Pengiriman Pesan Teks

D. Adobe Dream Weaver

Adobe Dreamweaver merupakan aplikasi pengembang yang berfungsi untuk mendesain web yang dibuat, dikembangkan, dan diproduksi oleh Adobe System. Aplikasi pengembang web ini sangat digemari oleh web desainer dalam merancang web sebab perangkat lunak komputer ini memiliki kelebihan dan kemudahan dalam penggunaannya. Dengan menggunakan aplikasi ini, pengembangan web dapat dilakukan secara visual, sehingga hasil perancangan web dapat langsung terlihat tanpa harus menggunakan aplikasi bantu peramban seperti Google Chrome, Firefox atau Internet Explorer. Teknologi web yang didukung oleh Adobe Dreamweaver sangat beragam, salah satunya adalah teknologi untuk kebutuhan pengembangan web berbasis mobile (Mandar, 2017).

E. Bahasa Pemrograman PHP

PHP berasal dari kata Hypertext Preprocessor yaitu bahasa pemrograman universal untuk penanganan pembuatan dan pengembangan sebuah situs web dan bisa digunakan bersamaan dengan HTML.PHp sebagai sekumpulan skrip atau bahasa program memiliki fungsi utama, yaitu mampu mengumpulkan dan mengevaluasi hasil survei atau bentuk apapun ke server database dan pada tahap selanjutnya akan menciptakan efek beruntun. Efek beruntun PHP ini berupa tindakan dari skrip lain yang akan melakukan komunikasi dengan database, mengumpulkan dan mengelompokkan informasi, kemudian menampilkannya pada saat ada tamu website memerlukannya (menampilkan informasi sesuai permintaan user) (Mundzir, 2020).

PHP dikenal sebagai sebuah bahasa scripting yang menyatu dengan tag-tag HTML yang dieksekusi di server dan digunakan untuk membuat halaman web yang dinamis. Konsep kerja PHP diawali dengan satu permintaan suatu halaman web oleh browser. Berdasarkan URL (Uniform Resource Locator) atau dikenal dengan alamat internet, browser mendapat alamat dari webserver, mengidentifikasikan alamat yang dikehendaki, dan menyampaikan segala informasi yang dibutuhkan oleh web server. Adapun cara kerja PHP seperti Gambar 2.5 (Krisbiantoro & Abda'u, 2021).

F. Basis Data

Basis data merupakan suatu kumpulan data terhubung yang disimpan secara bersama-sama pada suatu media, yang diorganisasikan berdasarkan sebuah skema atau struktur tertentu, dan dengan software untuk melakukan manipulasi untuk kegiatan tertentu. Basis data bisa diartikan juga sebagai sekumpulan data yang disusun dalam bentuk beberapa tabel yang saling memiliki relasi maupun berdiri sendiri (Widodo, 2017).

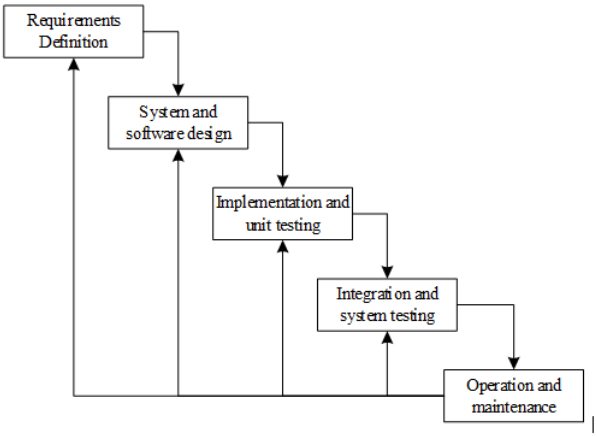
Basis data adalah kumpulan data yang saling berhubungan secara logis dan didesain untuk mendapatkan data yang dibutuhkan oleh suatu organisasi. Basis Data merupakan data yang terintegrasi, yang diorganisasi untuk memenuhi kebutuhan para pemakai di dalam suatu organisasi (Hardiansyah, 2020)

G. ***Unified Modeling Language* (UML)**

Unified Modeling Language merupakan bahasa visual untuk pemodelan dan komunikasi mengenai sebuah sistem dengan menggunakan diagram dan teks-teks pendukung. UML hanya berfungsi untuk melakukan pemodelan. Jadi penggunaan UML tidak terbatas pada metodologi tertentu, meskipun pada kenyataannya UML paling banyak digunakan pada metodologi berorientasi objek (Rosa & Shalahuddin, 2016)..

3. Metode Penelitian

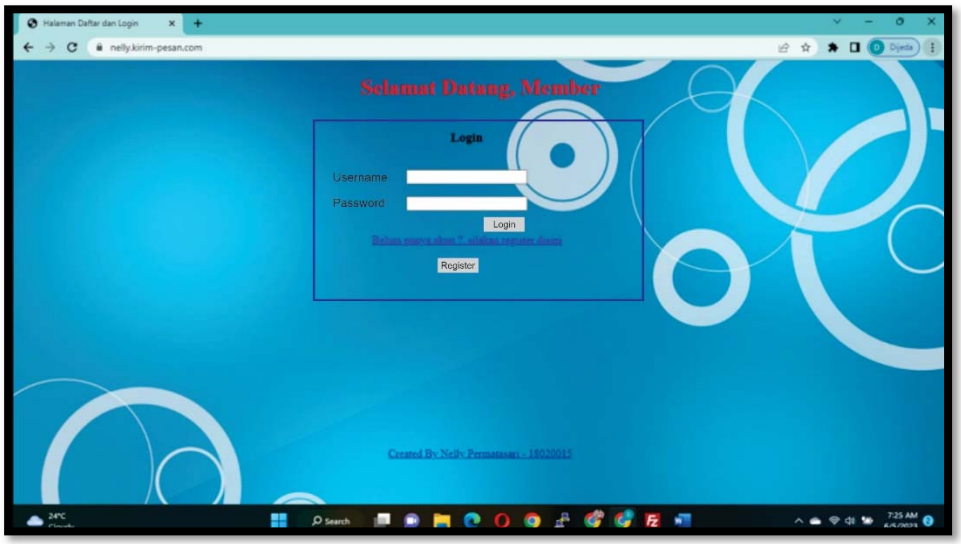
Metode penelitian yang diterapkan pada penelitian ini adalah dengan pengembangan metode waterfall. Metode waterfall merupakan model pengembangan sistem informasi yang sistematik dan sekuensial. Metode waterfall memiliki tahapan-tahapan seperti Gambar 3.1. (Trsitianto, 2018). dalam satu sistem.



Gambar 3.1. Metode Waterfall

4. Hasil dan Pembahasan

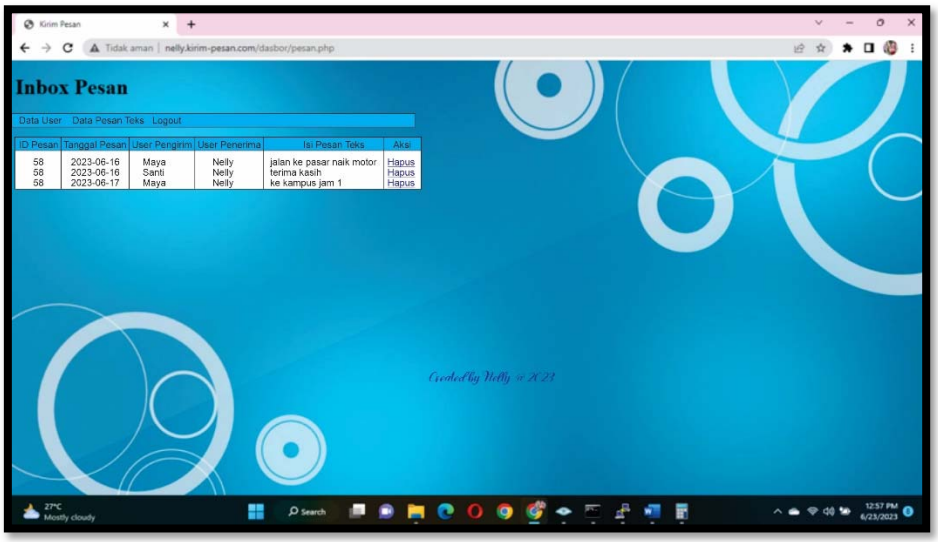
Dari serangkaian pengujian yang dilakukan pada aplikasi pengiriman pesan menggunakan metode blowfish dengan Bahasa pemrograman PHP dan MySQL berjalan dengan baik, sesuai dengan aturan-aturan yang diterapkan. Adapun hasil terima pesan (pesan masuk) yang berhasil diterima dapat dilihat pada tampilan login seperti gambar dibawah ini



Gambar 4.1 Tampilan Halaman *Login*

Seperti gambar 4.1 diatas dapat dilihat alamat web atau *hosting* nelly.kirim-pesan.com yang mana pertama kali dibuka masuk ke halaman login, Setelah berhasil

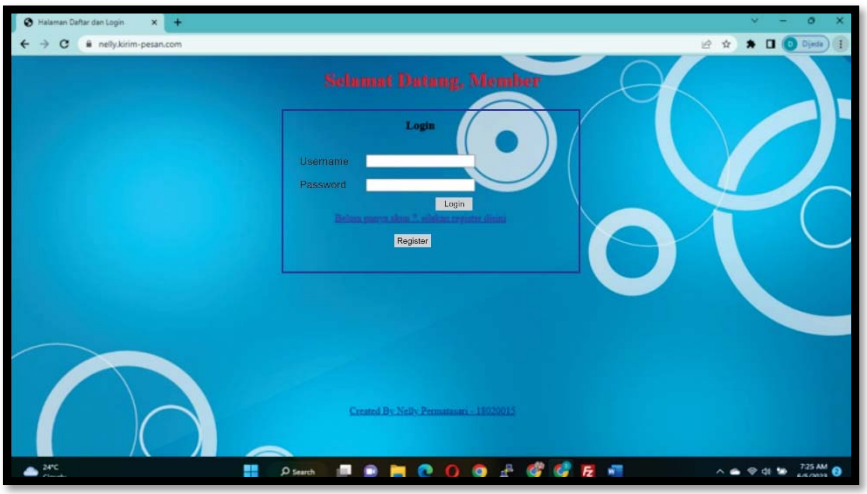
melakukan *login* dengan menggunakan akun yang dimiliki, untuk dapat melihat pesan masuk dapat klik menu pesan masuk, seperti tampilan gambar dibawah ini:



Gambar 4.2 Tampilan Detail Pesan Masuk

1. Pengujian Form Login

Pengujian *Form Login* dilakukan melalui *hosting* dengan alamat http://www.nelly.kirim-pesan.com. Adapun tampilan halaman *login* dapat dilihat pada tampilan gambar dibawah ini:

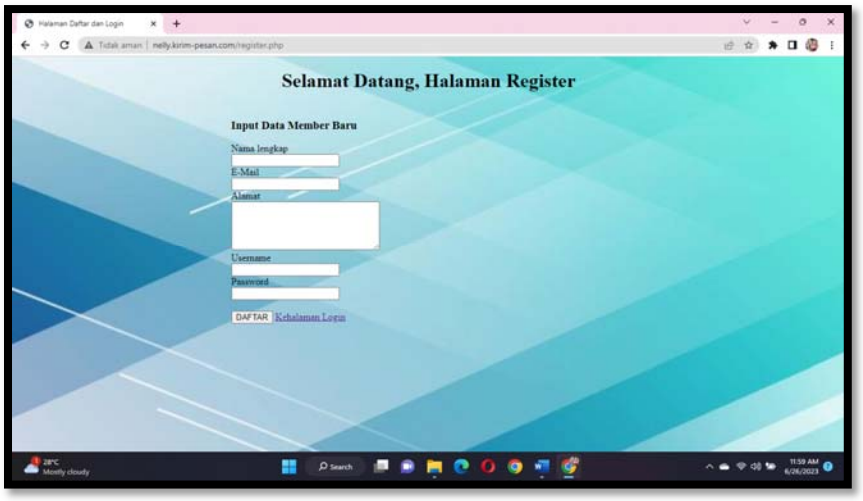


Gambar 4.3 Tampilan *Form Login*

Dari tampilan halaman *form login* diatas dapat dilihat terdiri dari ucapan Selamat Datang dan *input username* dan *password*. Jika pengguna ingin menggunakan aplikasi harus melakukan *login* terlebih dahulu pada sistem sesuai dengan akun yang telah di registrasi pada aplikasi

2. Pengujian Form Registrasi

Pengujian Form Registrasi dilakukan melalui hosting dengan alamat http://www.nelly.kirim-pesan.com, pada menu registrasi. Adapun tampilan halaman login dapat dilihat pada tampilan gambar dibawah ini:

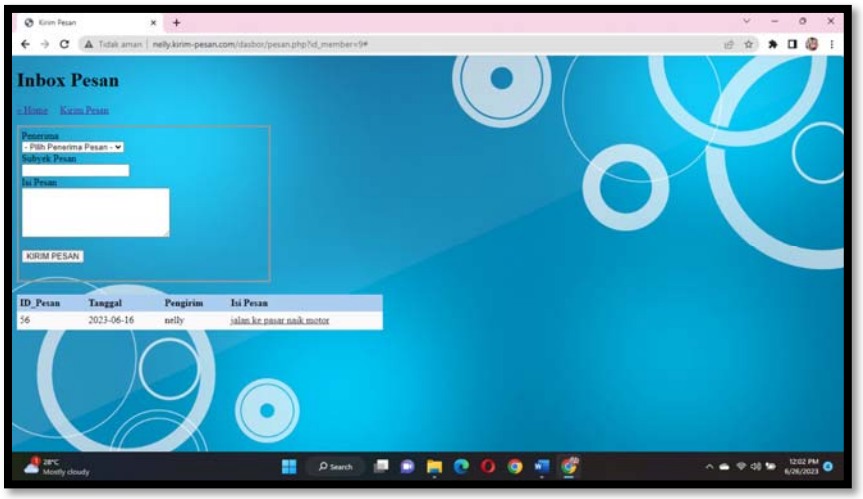


Gambar 4.4 Tampilan Form Registrasi

Dari tampilan halaman form regitrasi diatas dapat dilihat terdiri form input data pengguna seperi nama, email, alamat dan akun (username dan password) yang akan digunakan untuk menggunakan aplikasi.

3. Pengujian Form Kirim Pesan Teks

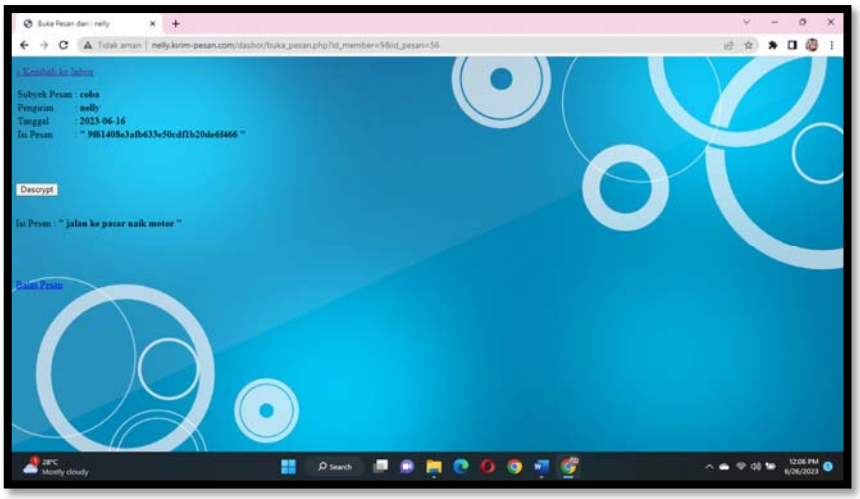
Pengujian Form kirim pesan dilakukan melalui hosting dengan alamat http://www.nelly.kirim-pesan.com, pada menu kirim pesan. Adapun tampilan halaman kirim pesan dapat dilihat pada tampilan gambar dibawah ini:



Gambar 4.4 Tampilan Form Registrasi

4. Pengujian *Form* Lihat Pesan Teks

Pengujian *Form* lihat pesan dilakukan melalui *hosting* dengan alamat http://www.nelly.kirim-pesan.com, pada menu lihat pesan. Adapun tampilan halaman lihat pesan dapat dilihat pada tampilan gambar dibawah ini:



Gambar 4.6 Tampilan Lihat Pesan

Dari tampilan halaman *form* regitrasi diatas dapat dilihat terdiri *form input* data pengguna seperi penerima, *subjek*, dan isi pesan yang akan dikirim.

Hasil Pengujian

Pengujian sistem merupakan proses eksekusi sistem dengan tujuan mencari kesalahan atau kelemahan dari program tersebut. Proses tersebut dilakukan dengan mengevaluasi kemampuan program. Suatu program yang diuji akan dievaluasi apakah keluaran atau output yang dihasilkan telah sesuai dengan yang diinginkan atau tidak. Metode pengujian yang dipakai dalam sistem ini adalah metode black box. Metode pengujian black box merupakan metode pengujian dengan pendekatan yang mengasumsikan sebuah sistem perangkat lunak atau program sebagai suatu kotak hitam.

Hasil pengujian yang dilakukan semua menu dan tombol yang ada berjalan dengan baik.. Adapun hasil pengujian dapat dilihat pada tabel dibawah ini:

Tabel 4.1. Hasil Pengujian

***Form* Yang Diuji**	**Skenario Pengujian**	**Hasil Pengujian**
Form *Login*	Memasukkan *username* dan *password* yang benar	Berjalan dengan baik. Dapat login ke aplikasi sesuai dengan akun yang dimiliki
	Memasukkan *username* atau *password* yang salah	Tidak dapat login ke aplikasi jika tidak memiliki akun atau username salah
Form Registrasi	Menambahkan data registrasi *user* baru	Dapat menambah *user* baru dari sub menu regitrasi user
Form Kirim Pesan Teks	Mengirim pesan teks ke penerima	Dapat mengirim pesan kepada tujuan sesuai dengan akun yang sudah terdaftar
	Melihat *record* pesan yang dikirim pada tabel pesan di dalam *database*	Admin dapat melihat *record* pesan pada *database* dari phpMyAdmin
Form Lihat Pesan Teks	Melakukan dekripsi pesan acak pada setiap pesan yang diterima	Dapat melihat pesan masuk sesuai dengan akun pengirim yang telah terdaftar

Pengujian *wireshark* pada proses enkripsi dan dekripsi	Melakukan *capturing* paket masuk dan keluar menggunakan *wireshark*	Tidak mempengaruhi paket masuk dan keluar karena pada prinsipnya metode blowfish digunakan untuk enkripsi dan dwskripsi pesan

5. Kesimpulan

Kesimpulan yang dapat diambil dari perancangan Aplikasi Penyandian Teks Berbasis *Web* Menggunakan Algoritma Blowfish adalah sebagai berikut :

1. Dengan Penyandian Teks Berbasis *Web* Menggunakan Algoritma Blowfish dapat membuat sebuah pesan menjadi lebih terjaga ke rahasiaannya.
2. Penyandian Teks Berbasis *Web* Menggunakan Algoritma Blowfish sangat baik dalam melakukan enkripsi dan deskripsi terhadap sebuah pesan.

REFERENSI

1. Bayuntara. (2017). Implementasi Web Service Dalam Pengembangan Sistem Informasi Akademik Berbasis Mobile Pada STIKES Nani Hasanuddin Makassar. *Jurnal Inspiration , Vol.7 No.1 Juni 2017*.
2. Enterprise, J. (2019). *PHP Untuk Programmer Pemula.* Jakarta: PT. Elex Media Komputindo.
3. Firdayanti, M. (2013). *Perancangan dan Implementasi Rekam Medis Pasien Poli Umum Di Rumah Sakit Aisyiah Muhammadiyah Padang Menggunakan PHP dan MySQL*. Dipetik 2020, dari repo.unand.ac.id
4. Firmansyah, R., & Permana, A. A. (2019). Implementasi Keamanan Pesan Teks Menggunakan Kriptografi Algoritma RSA Dengan Metode Waterfall Berbasis Java. *Joutica Vol.4 No.1 ISSN : 2503-071X*.
5. Krisbiantoro, D., & Abda'u, P. D. (2021). *Dasar Pemrograman Web Dengan Bahasa HTML, PHP dan Database MySQL.* Banyumas Jawa Tengah: Zahira Media Publisher.
6. Mandar, R. (2017). *Solusi Tepat Menjadi Pakar Adobe Dreamweaver CS6.* Jakarta: PT. Elexmedia Komputindo.
7. Mundzir, M. (2020). *Buku Sakti Pemrograman Web Seri PHP.* Yogyakarta: Anak Hebat Indonesia.
8. Nurani, C., & Siswanto. (2018). Implementasi Secure Chatting (Instan Messaging) Menggunakan Metode Algoritma Blowfish Berbasis Web Pada PT. Lautan Lepas Nusantara. *SKANIKA Vol.1 No.3*.
9. Pabokory, F. N., Astuti, I. F., & Kridalaksana, A. H. (2015). Implementasi Kriptografi Pengamanan Data Pada Pesan Teks, Isi File Dokumen, dan File Dokumen Menggunakan Algoritma Advanced Encryption Standard. *Jurnal Informatika Mulawarman , Vol. 10 No. 1 Februari 2015*.
10. Permana, A. A. (2018). Penerpaan Kriptografi Pada Teks Pesan Dengan Metode Vigenere Cipher Berbasis Android. *Jurnal Al-Azhar Indonesia Seri Sains dan Teknologi Vol.4 No.3*.
11. Ramdan, A., & Maliki, A. (2019). Penerapan Kriptografi RC4 Pada Aplikasi Chat Realtime Menggunakan Node JS dan Library Socket.IO. *Jurnal Universitas Siliwangi*.
12. Rosa, & Shalahuddin. (2016). *Rekayasa Perangkat Lunak Terstuktur dan Berorientasi Objek.* Bandung: Penerbit Informatika.
13. Santoso, & Nurmalina, R. (2017). Perencanaan dan Pengembangan Aplikasi Absensi Mahasiswa Menggunakan Smart Card Guna Pengembangan Kampus Cerdas (Studi Kasus Politeknik Negeri Tanah Laut). *Jurnal Integrasi, Vol.9 No.1 April 2017 e-ISSN : 2548-9828*.
14. Trsitianto, C. (2018). Penggunaan Metode Waterfall Untuk Pengembangan Sistem Monitoring dan Evaluasi Pembangunan Pedesaan. *Jurnal Teknologi Informasi ESIT Vol.XII No.1*.
15. Wardoyo, S. (2016). Enkripsi dan Dekripsi File Dengan Algoritma Blowfish Pada Perangkat Mobile Berbasis Android. *Jurnal Paper Aes , Vol. 5 No.1 ISSN 2302-2949*.