Jurnal Informatika dan Ilmu Komputer (JIKO)
Vol. 2, No. 2, Oktober 2019, hlm. 87-94
DOI: http://dx.doi.org/10.33387/jiko

p-ISSN: 2355-7699
e-ISSN: 2528-6579

PENERAPAN KRIPTOGRAFI *CAESAR CIPHER* PADA FITUR *CHATTING* SISTEM INFORMASI *FREELANCE*

Yuningrat Dwi Putri[1], Rosihan[2], Salkin Lutfi[3]
Program Studi Teknik Informatika, Fakultas Teknik, Universitas Khairun
Jl. Jati Metro, Kota Ternate Selatan

E-Mail : *juni.dwiputri@gmail.com*[1], *icanunkhair@gmail.com*[2], *Salkin.lutfi@gmail.com*[3]

(Naskah masuk: 3 April 2019, diterima untuk diterbitkan: 20 Oktober 2019)

Abstrak

Chatting sebagai sarana pengiriman pesan yang banyak digunakan oleh mansyarakat telah menimbulkan kekhawatiran mengenai keamanannya, masalah keamanan dan kerahasiaan data merupakan salah satu aspek penting dalam komunikasi menggunakan Komputer, sehingga dalam penelitian ini nanti akan diterapkan metode Kriptografi *Caesar Chiper* pada fitur *Chat* Sistem Informasi *Freelance*. Adapun metode pengembangan sistem yang digunakan dalam penelitian ini adalah metode *Prototype* dan pengujian sistemnya menggunakan metode *Whitebox*. Hasil yang didapatkan dari penelitian ini adalah pesan pada fitur *chat* ini dienkripsi dengan menggunakan kriptografi *caesar cipher* dengan pengkeripsian pesan menggunakan teknik *end to end* dimana proses enkripsi dan dekripsi pesan dilakukan pada saat proses *chatting* berlangsung. Dalam pengujian menggunakan *whitebox* ini telah menunjukan bahwa sistem telah berjalan dengan baik, untuk melihat kebenaran data seperti yang dijelaskan sebelumnya bahwa sistem dapat berjalan sesuai dengan fungsinya dapat dilihat pada hasil implementasi pada sistem yang dapat menunjukan fungsi-fungsinya berjalan sesuai apa yang diketik pada halaman sistem tersebut.

***Kata Kunci** : Kriptografi Caesar cipher, Chatting*

APPLICATION OF CAESAR CIPHER CRIPTOGRAPHY IN FREELANCE INFORMATION SYSTEM CHATTING FEATURES

Abstract

Chatting as a means of sending messages that is widely used by people has raised concerns about its security, security issues and confidentiality of data is one of the important aspects in communication using computers, so in this study the Caesar Chiper Cryptography method will be applied in the Freelance Information System Chat feature. The system development method used in this study is the Prototype method and system testing using the Whitebox method. The results obtained from this study are that the message on this chat feature is encrypted using caesar cipher cryptography with message manipulation using end to end techniques where the message encryption and decryption process is carried out during the chat process. In testing using whitebox it has been shown that the system has been running well, to see the truth of the data as explained earlier that the system can run according to its functions can be seen in the results of implementation on the system that can show the functions that match what is typed on the system page that is.

***Keywords:** Caesar Cipher, Cryptography , Chat*

I. PENDAHULUAN

Kriptografi adalah ilmu mengenai teknik enkripsi dimana "naskah asli" *(plaintext)* diacak menggunakan suatu kunci enkripsi menjadi "naskah acak yang sulit dibaca" *(ciphertext)* oleh seseorang yang tidak memiliki kunci dekripsi. Dekripsi menggunakan kunci dekripsi bisa mendapatkan kembali data asli. Probabilitas mendapat kembali naskah asli oleh seseorang yang tidak mempunyai kunci dekripsi dalam waktu yang tidak terlalu lama adalah sangat kecil.

Ilmu kriptografi juga adalah suatu teknik untuk mengamankan data atau pesan, pengamanan data atau pesan dapat dilakukan dengan menggunakan berbagai algoritma, salah satunya dapat menggunakan sandi *caesar*.

Caesar Cipher merupakan salah satu jenis *cipher* substitusi yang membentuk cipher dengan cara melakukan penukaran satu karakter diganti dengan karakter yang berada di sejumlah digit sebelah kanan atau kirinya, tergantung arah pergeserannya. Teknik

seperti ini disebut juga sebagai *cipher* abjad tunggal. *Caesar cipher* adalah dasar enkripsi yang sangat baik untuk dipahami sebelum membahas enkripsi berbasis karakter lainnya yang lebih rumit [1].

Pengiriman pesan singkat (*chatting*) sebagai sarana pengiriman pesan yang meningkat telah menimbulkan kekhawatiran mengenai keamanannya. Teks pesan yang dikirim melalui pengirim pesan dapat diganggu oleh pihak-pihak yang ingin tahu tentang isi percakapan tersebut dengan mudah karena tidak melalui proses enkripsi dalam perjalanannya.

Masalah keamanan dan kerahasiaan data merupakan salah satu aspek penting dalam komunikasi menggunakan komputer, sehingga dalam penelitian ini nanti akan diterapkan metode Kriptografi *Caesar Chiper* pada fitur *Chat* Sistem Informasi *Freelance* yang bertujuan untuk melindungi pesan para pengguna web *freelance*.

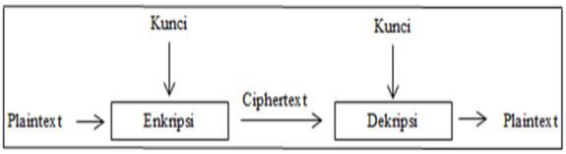
Dengan permasalahan di atas penulis ingin melakukan penelitian dengan judul "Penerapan Kriptografi *Caesar Chiper* Pada Fitur *Chat* Sistem Informasi *Freelance*" dimana pada fitur *chatting* ini dapat melindungi isi percakapan dalam module *chatting* Sistem Informasi *Freelance*.

II. TINJAUAN PUSTAKA

A. Kriptografi

Kriptografi (*cryptography*) merupakan ilmu dan seni untuk menjaga pesan agar aman. (*Cryptography is the art and science of keeping messages secure*) "*Crypto*" berarti "*secret*" (rahasia) dan "*graphy*" berarti "*writing*" (tulisan). Jadi, kriptologi adalah ilmu dan seni untuk menjaga keamanan pesan yang akan dikirim ke penerima sehingga data atau pesan tersebut aman dan tidak diketahui oleh pihak ketiga. Data atau pesan yang akan di kirim di ubah menjadi kode-kode yang tidak dipahami oleh pihak ketiga [2].

Kriptografi membuat data atau pesan menjadi kode-kode terlebih dahulu oleh pengirim. Proses ini dikenal dengan enkripsi. Enkripsi diartikan sebagai proses diubahnya data atau pesan yang hendak dikirim menjadi bentuk yang hampir tidak dikenali oleh pihak ketiga setelah data atau pesan itu sampai kepada penerima, maka penerima melakukan dekripsi yang merupakan kebalikan dari enkripsi. Dekripsi diartikan sebagai proses mengubah data atau pesan kembali kebentuk semula sehingga data atau pesan dapat tersampaikan dan dimengerti oleh penerima, data atau pesan asli dinamakan *plaintext* sedangkan sesudah dikodekan dinamakan *chipertext*. Proses enkripsi dan dekripsi memerlukan kunci dalam mekanismenya dan biasanya berupa *string* atau deretan bilangan. Berikut ini contoh proses enkripsi dan dekripsi yang digunakan dalam pengiriman pesan. Proses enkripsi dan dekripsi yang digunakan dalam pengiriman pesan dapat dilihat pada Gambar 1.

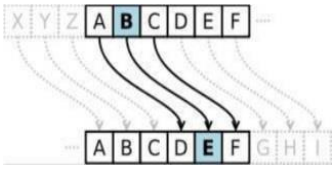


Gambar 1 Skema Enkripsi Dan Dekripsi Dengan Menggunakan Kunci [2]

B. *Caesar Cipher*

Metode penyandian ini dinamakan *caesar chiper*, setelah digunakan *Julius Caesar* untuk berkomunikasi dengan para panglimanya. Dalam kriptografi *caesar chiper* dikenal dengan beberapa nama seperti: *shift cipher, Caesar's code* atau *Caesar shift*.

Caesar Chiper merupakan teknik enkripsi yang paling sederhana dan banyak digunakan. *Chiper* ini berjenis *chiper* substitusi, dimana setiap huruf pada *plaintex nya* digantikan dengan huruf lain yang tetap pada posisi alfabet. Misalnya diketahui bahwa pergeseran = 3, maka huruf A akan digantikan oleh huruf D, huruf B menjadi huruf E, dan seterusnya, untuk proses pergeseseran dapat dilihat pada gambar 2.



Gambar 2 Proses pergeseran 3 huruf

Gambar 2 dapat direpsentasikan dengan menyelaraskan *plaintext* dengan *chipertext* ke kiri atau kanan sebanyak jumlah pergeseran yang diinginkan. Sebagai contoh dengan jumlah pergeseran sebanyak 3

Plaintext : ABCDEFGHIJKLMNOPQRSTUVWXYZ
Cipher : DEFGHIJKLMNOPQRSTUVWXYZABC

Untuk membaca pesan yang dienkripsi penerima dapat menyelaraskan huruf *chipertext* yang diterima dengan *plaintex* yang tepat berada di atasnya. Sebagai contoh dekripsinya sebagai berikut.

Cipher:VHPLQDU QDVLRQDOP DWHPDWLND
Plaintext : SEMINAR NASIONAL MATEMATIKA

Proses enkripsi pada *Caesar Cipher* dapat direperesentasikan menggunakan operator aritmetika modulo 26 setelah sebelumnya setiap huruf di transformasi kedalam angka, yaitu: A = 0, B = 1,…, Z = 25. Maka *caesar cipher* dirumuskan sebagai berikut: Proses enkripsi suatu huruf P dengan pergeseran K dapat dinyatakan secara matematis sebagai berikut:

Enkripsi: C = E(P) = (P + K) mod26
Dekripsi: P = D(C) = (C − K) mod26

dengan C adalah *ciphertext*, P adalah *plaintext*, K adalah kunci rahasia, E(P) adalah enkripsi, dan D(C) adalah dekripsi.

Kelemahan dari *caesar cipher* adalah dapat dipecahkan dengan cara *brute force attack*, suatu bentuk serangan yang dilakukan dengan mencoba-coba berbagai kemungkinan untuk menemukan kunci. Bisa juga menggunakan *exhaustive key search*, karena jumlah kunci sangat sedikit (hanya ada 26 kunci) [2].

C. *Chatting*

Chat messenger adalah suatu teknologi jaringan yang mengijinkan penggunanya mengirimkan pesan secara realtime ke pengguna lain yang tersambung dalam sebuah jaringan LAN atau *Local Area Network* ataupun internet. Dalam dunia komputer dan internet, pengertian *chatting messenger* adalah suatu fasilitas dalam internet untuk berkomunikasi sesama pengguna internet yang sedang *online*, komunikasi dapat berupa teks [3].

D. Sistem Informasi

Pada saat ini dunia industri dan bisnis memerlukan informasi yang tepat, cepat dan relevan. Untuk mendapatkan informasi yang diinginkan tentunya harus menggunakan system informasi. Sistem informasi dalam suatu organisasi dapat dikatakan sebagai suatu sistem yang menyediakan informasi bagi semua tingkatan dalam organisasi tersebut kapan saja diperlukan. Sistem ini menyimpan, mengambil, mengubah, mengolah dan mengkomunikasikan informasi yang diterima dengan menggunakan sistem informasi atau peralatan sistem lainnya [4].

Menurut Mc leod "Sistem Informasi merupakan sistem yang mempunyai kemampuan untuk mengumpulkan informasi dari semua sumber dan menggunakan berbagai media untuk menampilkan informasi "Sistem informasi dapat didefinisikan sebagai suatu sistem di dalam suatu organisasi yang merupakan kombinasi dari orang-orang, fasilitas, teknologi, media prosedur-prosedur dan pengendalian yang ditujukan untuk mendapatkan jalur komunikasi penting, memproses tipe transaksirutin tertentu, memberi sinyal kepada manajemen dan yang lainnya terhadap kejadian-kejadian internal dan eksternal yang penting dan menyediakan suatu dasar informasi untuk pengambilan keputusan.

Informasi dalam suatu lingkungan sistem informasi harus mempunyai persyaratan umum sebagai berikut :

1. Harus diketahui oleh penerima sebagai referensi yang tepat
2. Harus sesuai dengan kebutuhan yang ada dalam proses pembuatan / pengambilan keputusan
3. Harus mempunyai nilai *surprise*, yaitu hal yang sudah diketahui hendaknya jangan diberikan
4. Harus dapat menuntun pemakai untukmembuat keputusan. Suatu keputusan tidak selalu menuntut adanya tindakan.

Sistem informasi harus mempunyai beberapa sifat seperti :

1. Pemrosesan informasi yang efektif. Hal ini berhubungan dengan pengujian terhadap data yang masuk, pemakaian perangkat keras dan perangkat lunak yang sesuai
2. Manajemen informasi yang efektif, dengan kata lain, operasi manajemen, keamanan dan keutuhan data yang ada harus diperhatikan
3. Keluwesan sistem informasi hendaknya cukup luwes untuk menangani suatu macam operasi
4. Kepuasan pemakai, hal yang paling penting adalah pemakai mengetahui dan puas terhadap sistem informasi [4].

III. METODE PENELITIAN

A. Pengumpulan Data

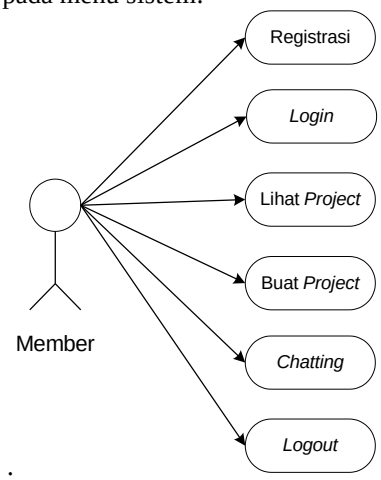
Pada studi pustaka ini, penulis melakukan pencarian sumber yang dapat menjadi acuan dalam pengerjaan tugas akhir seperti sumber dari internet dan buku-buku.

Selain itu juga ada beberapa penelitian terkait pada pustaka dimana peneliti mengambil buku maupun jurnal yang terkait dengan penelitian, seperti halnya tentang perancangan aplikasi kriptografi, dan jurnal yang terkait dengan Pemrograman Web.

B. Fitur *Chat* pada Sistem Informasi *Freelance*

Perancangan fitur *chat* disini adalah bagaimana penulis mengambarkan dari sebuah perangkat lunak yang direncanakan, perancangan ini akan ditentukannya informasi, fungsi, proses atau prosedur yang diperlukan beserta unjuk kerjanya.

Pada gambar 3 menunjukkan kegiatan- kegiatan dari *menu* yang telah disediakan Sistem Informasi *Freelance* yang bisa dipilih dan digunakan oleh pengguna, pengguna dapat memilih beberapa kegiatan yang ada pada menu sistem.

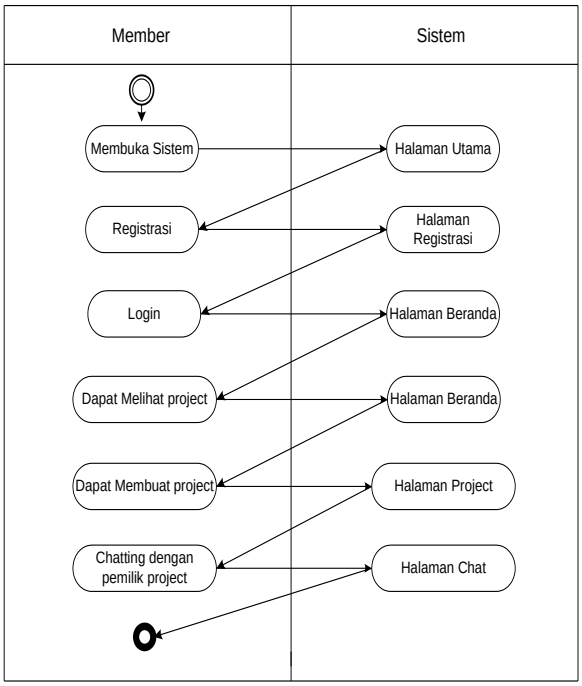


Gambar 3 *Use case* member

Keterangan:

Sebelum masuk ke sistem untuk melihat *project* dan melakukan *chat*, member diminta untuk registrasi terlebih dahulu, kemudian login dan member akan di beri hak untuk melihat *project* apa yang dapat di kerjakan, member juga dapat membuat *project* dan melakukan *chat* untuk membahas dan menyepakati hal-hal terkait *project* yang akan diambil, dan *project* yang telah selesai dikerjakan akan diberikan melalui email.

C. Diagram *Activity*

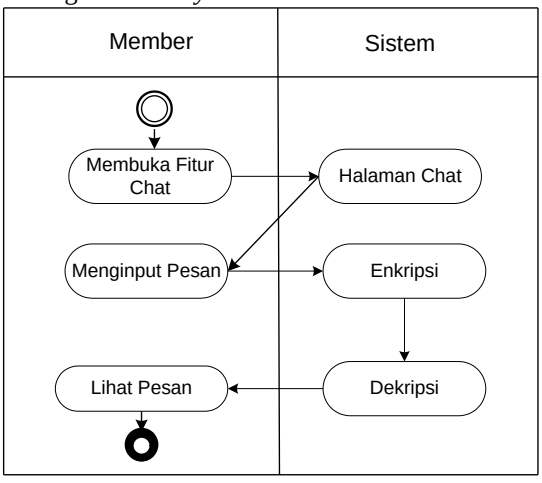


Gambar 4 Diagram *Activity*

Keterangan :

1. Member membuka sistem Informasi *Freelance*
2. Sistem Menampilkan halaman utama yang terdapat daftar tampilan *project, form login* dan menu registrasi
3. Member melakukan registrasi
4. Sistem menampilkan halaman registrasi
5. Member *login* untuk masuk ke sistem Informasi
6. Sistem menampilkan halaman beranda yang terdapat tampilan *project-project* yang telah dibuat oleh member-member yang sudah terdaftar dalam sistem.
7. Member dapat membuat *project*
8. Sistem menampilkan halaman membuat *project*
9. Member melakukan *chatting* dengan pemilik *project* atau member lainnya
10. Sistem menampilkan halaman *chat*

D. Diagram *Activity Chat*



Gambar 5 Diagram *Activity Chat*

Keterangan:

1. Member membuka fitur *chat* yang tersedia dalam sistem informasi
2. Sistem menampilkan halaman *chat*
3. Member menginput pesan
4. Sistem mengenkripsi pesan yang ditampilkan, pesan yang tersenkripsi masuk ke *database* kemudian pesan kembali di dekripsi untuk ditampilkan.
5. Member melihat pesan

E. Algoritma *Caesar Cipher*

Caesar Chiper merupakan teknik enkripsi yang paling sederhana dan banyak digunakan. *Chiper* ini berjenis *chiper* substitusi, dimana setiap huruf pada *plaintext*-nya digantikan dengan huruf lain yang tetap pada posisi alfabet. Proses enkripsi pada *Caesar Cipher* dapat direperesentasikan menggunakan operator aritmetika modulo 26 jumlah karakter yang digunakan oleh penulis, setelah sebelumnya setiap huruf di transformasi kedalam angka, yaitu: A = 0, B = 1,…, Z = 25. Maka *Caesar Cipher* dirumuskan sebagai berikut: Proses enkripsi suatu huruf dengan pergeseran K dapat dinyatakan secara matematis sebagai berikut:

Enkripsi: C = E(P) = (P + K) mod 26
Dekripsi: P = D(C) = (C − K) mod 26
dengan C adalah *ciphertext*, P adalah *plaintext*, K adalah kunci rahasia, E(P) adalah enkripsi, dan D(C) adalah dekripsi.

- Contoh perhitungan *Caesar Cipher*
- Pesan/*Plaintext = PROJECT*
- Kunci = 10

Tabel 1 Tabel Alfabet

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	X
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

- Enkripsi Pesan dengan rumus C=E(P) = (P+K) Mod 26

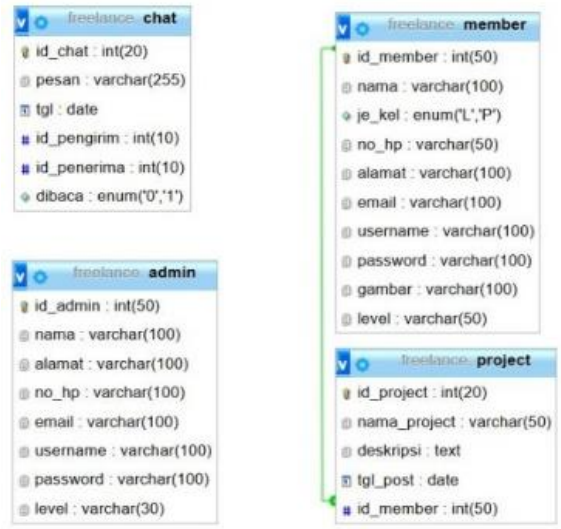
1. P = (15+10) Mod 26
   = 25 Mod 26
   = 25 = Z
2. R = (17+10) Mod 26
   = 27 Mod 26
   = 1 = B
3. O = (14+10) Mod 26
   = 24 Mod 26
   = 24 = Y
4. J = (9 + 10) Mod 26
   =19 Mod 26
   = 19 = T
5. E = (4+10) Mod 26
   = 14Mod 26
   = 14 = O
6. C = (2+10) Mod 26
   = 12 Mod 26
   = 12 = M
7. T = (19+10) Mod 26
   = 29 Mod 26
   = 3 = D

Jadi pada contoh perhitungan *caesar cipher*, pesan "*PROJECT*" di enkrpsi dan mengahasilkan *chipertext* berupa ZBYTOMD, kemudian untuk mendekripsi pesan yang telah didekripsi dapat menggunakan kunci yang sama agar pesan asli dapat terbaca kembali.

IV. HASIL DAN PEMBAHASAN

A. Implementasi Basis Data

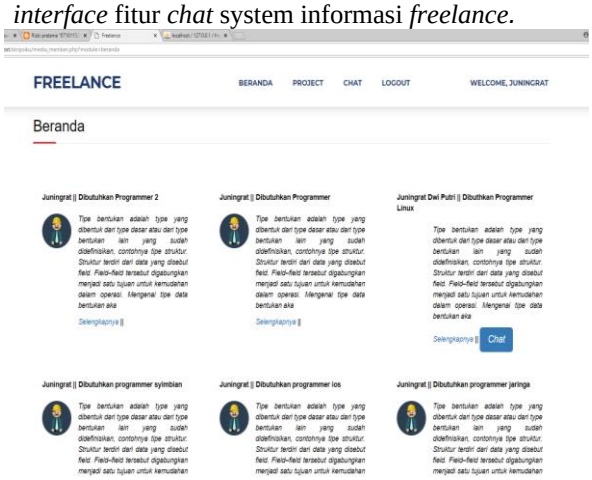
Pada fitur *chat* yang terdapat di dalam sistem informasi dengan menggunakan metode *Caesar cipher* ini mengimplementasikan *database* dengan nama *freelance*. Dalam *database* terdapat 4 tabel dengan nama table yaitu, tabel member, tabel *project*, tabel *chat* dan tabel admin. Pada *database* terdapat 1 relasi yaitu antara tabel member, dan tabel *project* seperti pada gambar 6



Gambar 6. Struktur *Database*

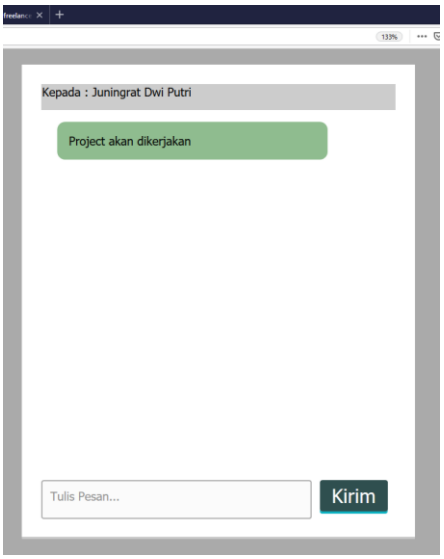
B. Implementasi *Interface*

Dalam perancangan fitur *chat* pada Sistem Informasi *Freelance* ini mengimplementasikan beberapa *interface*, berikut ini akan dijelaskan *interface* fitur *chat* system informasi *freelance.*



Gambar 7. Tampilan Halaman Beranda Sistem Informasi *Freelance*

Untuk tampilan halaman chat pada Sistem Informasi *Freelance* dapat dilihat pada gambar 8.



Gambar 8. Tampilan Halaman Chat

C. Implementasi Algoritma

Dalam perancangan ini penulis mengimplementasikan algortima *caesar cipher* pada fitur *chat*. Hasil fitur *chat* yang dilakukan oleh peneliti terhadap member yang menggunakan fitur *chat* pada sistem adalah, pesan pada *chatting* dilindungi dengan kriptografi *caesar cipher*.

Pesan yang dikirim oleh member akan di enkripsi menggunakan teknik enkripsi *end to end* yang mana pengenkripsian pesan dilakukan pada saat pesan akan dikirimkan dan kembali didekripsikan pada saat pesan sampai pada penerima, sehingga member yang melakukan *chatting* tidak perlu memasukkan kunci pada saat mengirim dan menerima pesan karena kunci telah dimasukkan langsung oleh sistem pada saat *chatting* berlangsung.

Dalam perancangan algoritma program penulis menggunakan *pseudocode*. Untuk lebih jelas proses enkripsi dan dekripsi *caesar chiper*, dapat dilihat pada *pseudocode* di bawah ini.

- *Pseudocode* Enkripsi *Caesar Chiper*

```
Teks = string
Panjang_teks = integer
Teks_encrypt = string
Teks_integer = integer
   Kunci = integer
   Mulai
   Input pesan
   Panjang_teks = strlen(teks)
   For (i=0 i<panjang_teks i++)

      Teks[i] = teks_integer
      Teks_encrypt =(teks [i] + kunci) mod 26

    Selesai
```

- *Pseudocode* Dekripsi *Caesar Chiper*

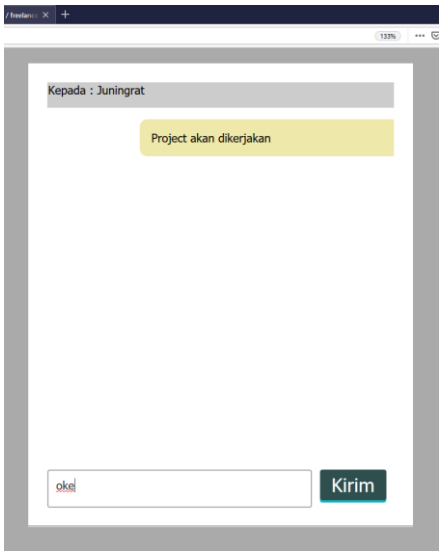
```
Teks_encrypt  = string
Teks_decrypt = string
Teks_integer = integer
Kunci = integer
Mulai
Panjang_teks = strlen(teks_encrypt)
For (i=0  i<panjang_teks i++)
      Teks_encrypt [i] = teks_integer
         Teks_decrypt =(teks_encrypt [i] - kunci) mod 26
      Selesai
```

D. Pengujian Pengujian Pengamanan Pesan dengan Teknik Enkripsi *End To End*

Teknik enkripsi *end-to-end* merupakan sebuah sistem dimana proses enkripsi terjadi pada saat pesan dikirimkan dan hanya terdekripsi pada saat pesan sampai kepada penerima. Sebagai ilustrasi pengirim pesan di *chat* Member 1 akan mengirimkan pesan berupa "*Project* akan dikerjakan" dapat dilihat pada gambar 9.

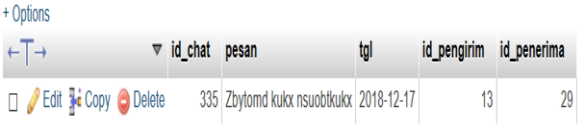
Gambar 9. *Chatting* member 1 sebagai pengirim

Pada saat pesan dikirimkan maka pesan tersebut akan dienkripsi secara otomatis menjadi "Zbytomd kukx nsuobtkukx " Tetapi sesampainya pesan ke penerima sebagai member 2 maka secara otomatis kode "Zbytomd kukx nsuobtkukx", akan kembali didekripsikan menjadi pesan semula "*Project* akan dikerjakan", dengan menggunakan kunci yang telah ditentukan langsung oleh penulis yaitu 10. Dapat dilihat pada gambar 10.



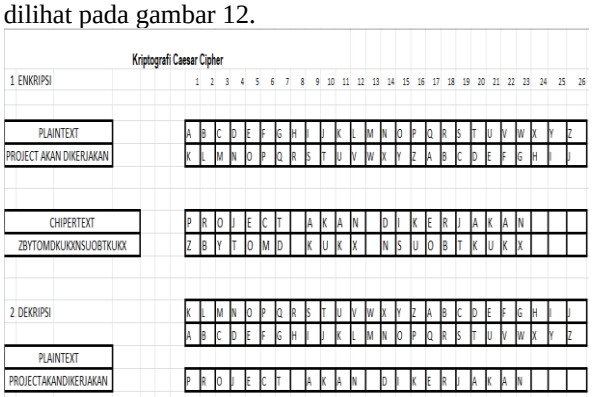
Gambar 10. *Chatting* member 2 sebagai Penerima

Dengan menggunakan teknik enkripsi *end-to-end*, dan hasil enkripsi dari pesan yang dikirimkan akan tersimpan ke *database*, dapat dilihat pada gambar 11.



Gambar 11. Hasil Enkripsi Pesan

Hasil pengujian tersebut diuji kembali dengan menggunakan perhitungan manual yaitu dengan *Excel*, dan menunjukan hasil yang sama dengan sistem, dilihat pada gambar 12.



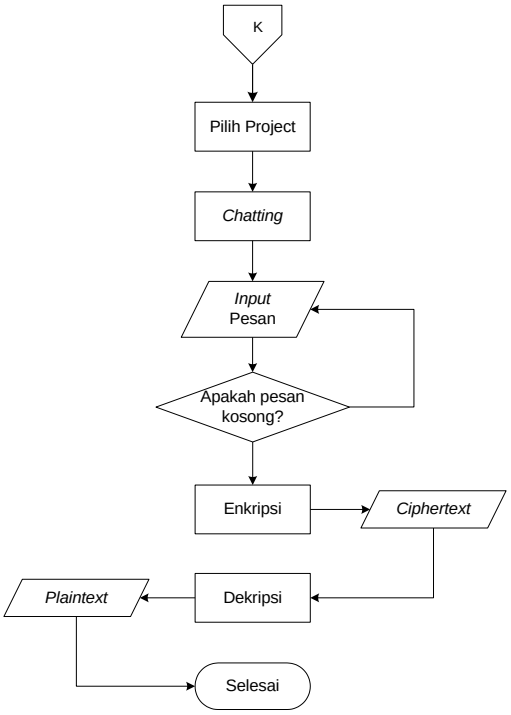
Gambar 12. Pengujian dengan *Excel*

E. Pengujian *Whitebox*

Metode pengujian sistem yang digunakan adalah model *Whitebox*. Pengujian perangkat lunak yang dilakukan terlebih dahulu memetakan *flowchart* kedalam *flowgraph* kemudian menghitung besarnya jumlah *edge* dan *node* untuk menentukan besarnya *cylomatic complexity*, adapun *flowchart* dan *flowgraph* yang diuji.

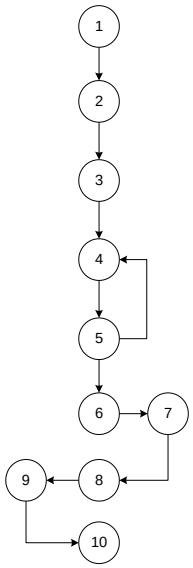
1. *Flowgrap*h *Chat*

Flowgraph chat diambil dari *flowchart* tampilan *chat, flowchart* menu *chat* dapat dilihat pada gambar 13.



Gambar 13. *Flowchart Chat*

Adapun *Flowgraph* dari modul *chat*i dapat dilihat pada gambar 14.



Gambar 14. *Flowgraph Chat*

Keterangan :

- *Node* (N) : 10
- *Edge* : 10
- Predikat : 1
- *Cylomatic Complexcity*

  V(G) = (E – N) + 2
  = (10 – 10) + 2
  = 2

  V(G) = P + 1
  =1 + 1
  = 2
- *Independent Path:*

  Path 1 : 1 2 3 4 5 4 5 6 7 8 9 10
  Path 2 : 1 2 3 4 5 6 7 8

Berdasarkan pada hasil yang di dapatkan *cylomatic complexity*, dan *independent path* bernilai 2, maka dapat diambil kesimpulan bahwa tampilan *chat* dapat dikatakan valid

F. Analisa

Berdasarkan hasil analisa pengujian maka dapat dipastikan bahwa sistem atau aplikasi yang telah dilakukan pengujian dapat berjalan dengan baik dan benar sesuai dengan tujuan dan manfaat penelitian. Metode pengembangan sistem menggunakan metode *prototype* yang kemudian dilanjutkan dengan perancangan desain yang menggunakan pemodelan UML yang dimulai dari membuat *use case*, a*ctivity* diagram, hingga pada perancangan *database* dan proses *coding* dilakukan dengan menggunakan bahasa pemrograman PHP dan *database* menggunakan MySQL.

Untuk pengujian sistem terhadap hasil perancangan aplikasi yang telah diuji dengan menggunakan pengujian *white box.* Adapun modul-modul program yang telah diuji yaitu : *login*, registrasi, halaman utama, halaman beranda, halaman *project,* halaman pemberitahuan *chat*, dan halaman *chat.* Berdasarkan hasil pengujian yang telah dilakukan dengan mempunyai nilai kompleksitas dan *indenpenden path* berjumlah 17, ini menunjukan bahwa setiap modul sudah dapat teruji dengan baik.

Untuk melihat kebenaran data seperti yang dijelaskan sebelumnya bahwa sistem dapat berjalan sesuai dengan fungsinya dapat dilihat pada hasil implementasi pada sistem yang dapat menunjukan fungsi-fungsinya berjalan sesuai apa yang di-*input* pada halaman sistem tersebut. Beberapa hal yang perlu diketahui pada sistem yang dibangun ini bahwa data-data pada sistem ini membutuhkan data yang berbeda-beda dari setiap tabel artinya sistem ini pada *database* terdapat tabel *projec*t, *chat*, member dan admin dimana tabel member dan tabel *project* memiliki relasi.

Pada fitur *chat* sistem dilindungi dengan kriptografi *caesar cipher*, pesan yang dikirim oleh member di enkripsi menggunakan teknik enkripsi *end to end* yang mana pengenkripsian pesan dilakukan pada saat pesan akan dikirimkan dan kembali didekripsikan pada saat pesan sampai pada penerima. Pada fitur *chat* ini pesan yang dikirim tidak boleh kosong dan pesan yang terenkripsi berupa *alphabet* A-Z tidak mencakup simbol dan angka.

V. KESIMPULAN

1. Pembuatan fitur *chat* pada system informasi *freelance* dapat dilakukan dengan menggunakan bahasa pemrograman PHP.
2. Impementasi enkripsi dan dekripsi pada fitur *chat* menggunakan teknik *end to e*nd, dimana pengirim dan penerima pesan tidak perlu memasukan kunci pada saat melakukan *chat*.

3. Karakter yang digunakan pada enkripsi pesan menggunakan 26 karakter huruf Alfabet.
4. Metode *cipher* ini berjenis *cipher* substitusi, dimana setiap huruf pada *plaintext*nya digantikan dengan huruf lain yang tetap pada posisi *alphabet*, jadi kemungkinan dapat dipecahkan dengan cara *brute force attack*, suatu bentuk serangan yang dilakukan dengan mencoba-coba berbagai kemungkinan untuk menemukan kunci.
5. Setelah melewati beberapa proses pengujian enkripsi dan dekripsi dari algoritma *caesar cipher*, dapat disimpulkan bahwa hasil dari enkripsi pesan dalam sistem sama dengan hasil perhitungan pada *excel*.
6. Setelah dilakukan pengujian dengan *White Box*, hasil implementasi telah sesuai dengan perancangan dan semua modul program telah berfungsi dengan baik.

VI. DAFTAR PUSTAKA

[1] Kromodimoeljo Sentot, 2009. Teori dan Aplikasi Kriptografi, SPK IT Consulting.

[2] Sumandri. 2017. "Studi Model Algoritma Kriptografi Klasik Dan Modern." *Jurnal Pendidikan Matematika*: 265–72.

[3] Febryanta Ekky, 2015 Pengaruh Intensitas Penggunaan Aplikasi *Chatting Messenger* Terhadap Proses Penetrasi Sosial, Universitas Telkom.

[4] Nuryasin, 2016. Aplikasi Sistem Informasi Pendaftaran Wisuda Berbasis *Online* Studi Kasus Fst Uin Syarif Hidayatullah, Jakarta

[5] S. Lutfi, Rosihan, 2018 "Perbandingan Metode Steganografi LSB (*Least Significant Bit)* Dan MSB (Most Significant Bit) Untuk Menyembunyikan Informasi Rahasia, Teknik Informatika Unkhair" *JIKO*, vol. 02, no. 1, pp. 34–42.

[6] Faisal, 2014. Penerapan Kombinasi *Sandi Caesar* Dan *Vigenere* Untuk Pengamanan Data Pesan Pada Surat Elektronik, Jakarta.