Jurnal Online Universitas Budi Luhur

SKANIKA

Sistem Komputer dan Teknik Informatika

Vol. 1, No. 1, Juli 2018

Diterbitkan oleh:
Universitas Budi Luhur
Jl. Raya Ciledug Petukangan Utara, Jakarta Selatan

Editorial Team

Aplikasi Data Mining Dengan Menggunakan Algoritma Fuzzy C-Means dan Metode Recency Frequency Monetary (RFM) Untuk Pengelompokan Pelanggan pada PT Eka Cipta Rasa

Nindya Rahmawati Syarif, Windarto Windarto 1093-1099

Download PDF  Abstract views: 1792 times.  Downloaded: 1395 times.

Penerapan Algoritma Kriptografi Vigenere Cipher Dan Rc4 (Rivest Code 4) Pada Database Berbasis Java

Lutfi Risnanda, Noni Juliasari 1100-1107

Download PDF  Abstract views: 1142 times.  Downloaded: 1124 times.

Implementasi Kriptografi dengan Algoritma AES-128 dan Blowfish Berbasis Android pada Fitur One-To-One Chat Blucareer Aplikasi Blucampus pada Universitas Budi Luhur

Destriyani Destriyani, Painem Painem 1108-1115

Download PDF  Abstract views: 1349 times.  Downloaded: 658 times.

Implementasi Algoritma Kriptografi Dengan Metode Des, Vernam Dan Diffie Helman Pada Web Service Berbasis Rest Aplikasi Blucampus Fitur Pmb Pada Universitas Budi Luhur

Riyan Sugiharto, Painem Painem 1116-1122

Download PDF  Abstract views: 932 times.  Downloaded: 727 times.

Implementasi Kompresi Citra Digital Menggunakan Kuantisasi Dan K-Means Clustering Pada Fitur Blucare Di Aplikasi Blucampus Universitas Budi Luhur

Kaishananda Dwi Takanwiedi, Painem Painem 1123-1129

Download PDF  Abstract views: 1591 times.  Downloaded: 682 times.

Implementasi Kriptografi dengan Algoritma AES-128 dan Blowfish Berbasis Android pada Fitur *One-To-One Chat* Blucareer Aplikasi Blucampus pada Universitas Budi Luhur

Destriyani [1)], Painem [2)]
[1]Program studi, Fakultas Teknologi Informasi, Universitas Budi Luhur
[1,2]Jl. Raya Ciledug, Petukangan Utara, Kebayoran Lama, Jakarta Selatan 12260
E-mail : destrisarbini@gmail.com[1)], painem@budiluhur.ac.id[2)]

Abstrak

Bagi kaum milenial masa kini, adanya layanan chatting menjadi salah satu fitur yang paling diharapkan keberadaannya di dalam suatu aplikasi. Melihat belum adanya fitur chatting pada aplikasi BLuCareer maka dihadirkan fitur tersebut agar para pengguna tidak mendapati kendala melakukan percakapan dalam satu ruang yang sama, yaitu tetap pada aplikasi BLuCareer. Namun, kemudahan tersebut memberikan ancaman berupa permasalahan keamanan dan kerahasiaan data. Oleh karena itu, dibutuhkan suatu sistem pengamanan data yang bertujuan menanggulangi ancaman yang mungkin timbul tersebut, serta meminimalisir rasa khawatir pengguna dalam berkomunikasi menggunakan fitur chatting pada suatu aplikasi. Salah satu ilmu pengamanan data yang terkenal adalah kriptografi, dimana metode algoritma AES dengan penggunaan kunci 128 bit dan algoritma Blowfish akan diterapkan dalam kasus ini. Hasil dari penelitian ini diimplementasikan dalam sebuah fitur aplikasi berbasis Android yang memberikan kemudahan bagi pengguna untuk tetap merasa aman dan nyaman saat melakukan chatting. Hasil pengujian menunjukkan 0.64 detik merupakan rata-rata waktu untuk satu kali proses enkripsi sementara proses dekripsi memerlukan waktu 1.23 detik, sedangkan berdasarkan hasil kuesioner yang terhimpun dari 25 responden didapati bahwa secara keseluruhan seberapa puas mereka dengan fitur chatting ini adalah 12% merasa cukup puas, 32% puas dan 56% merasa sangat puas. Dengan presentase kegagalan mengirim pesan sebesar 12%.

Kata kunci: *Chatting*, Kriptografi, AES, Blowfish, Enkripsi, Dekripsi

1. PENDAHULUAN

Bagi kaum milenial masa kini, adanya layanan *chatting* menjadi salah satu fitur yang paling diharapkan keberadaannya di dalam suatu aplikasi. Karena hal tersebut mempermudah antarsesama pengguna untuk saling berkomunikasi. Melihat belum adanya fitur *chatting* pada aplikasi BLuCareer maka diterapkan teknologi berbasis Android untuk menghadirkan fitur tersebut agar para pengguna tidak mendapati kendala melakukan percakapan dalam satu ruang yang sama, yaitu tetap pada aplikasi BLuCareer. Namun, hal ini memiliki kelemahan berupa permasalahan keamanan dan kerahasiaan data, karena pengguna melakukan komunikasi secara tidak langsung dengan menggunakan perantara aplikasi dimana jaringan internet sebagai sarananya rentan diakses oleh pihak yang tidak berhak. Pada fitur *one-to-one chat* BluCareer ini tersemat implementasi kriptografi algoritma AES-128 dan Blowfish sebagai upaya tercapainya tujuan dari penelitian ini yaitu memanfaatkan kedua algoritma tersebut untuk mengamankan data dari kejadian seperti penyadapan, pencurian data dan/atau pemalsuan pesan oleh pihak-pihak yang tidak bertanggung jawab sekaligus untuk menjaga *privacy* pengguna saat *chatting* dengan cara melakukan enkripsi terhadap pesan yang akan dikirimkan pengguna. Sementara pesan yang tampil merupakan pesan terenkripsi yang sudah dikembalikan isinya seperti semula dengan melalui proses dekripsi terlebih dahulu, sehingga tidak ada perubahan pada isi pesan walau sempat terenkripsi.

2. TINJAUAN PUSTAKA

2.1. Pengertian *Chatting*

Chatting dalam bahasa Indonesia berarti ngobrol atau berbicara dua arah antara satu atau beberapa orang. Di dalam dunia komputer, *chatting* berarti berbicara dengan orang lain dengan menggunakan komputer [2].

Chatting adalah percakapan dua orang atau lebih secara *realtime* melalui jaringan internet. Dengan adanya layanan *chat* memungkinkan kita untuk dapat berkomunikasi melalui internet dengan orang-orang yang berada di seluruh dunia [1].

2.2. Definisi Kriptografi

Kriptografi adalah suatu ilmu yang mempelajari bagaimana cara menjaga agar data atau pesan tetap aman saat dikirimkan, dari pengirim ke penerima tanpa mengalami gangguan dari pihak ketiga [4].

Kriptografi adalah ilmu mengenai teknik enkripsi dimana data diacak menggunakan suatu kunci enkripsi menjadi sesuatu yang sulit dibaca oleh seseorang yang tidak memiliki kunci dekripsi [3].

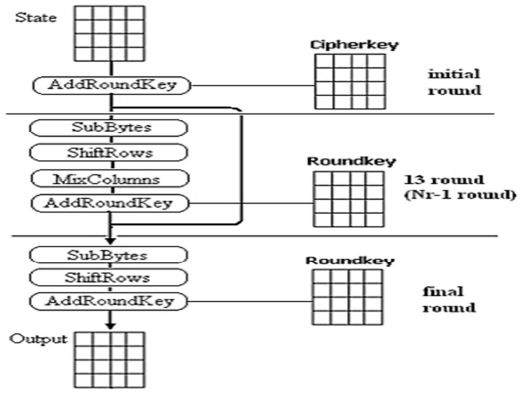
2.3. Algoritma AES

AES *(Advanced Encryption Standard)* adalah teknik enkripsi yang dijadikan standard FIPS oleh

NIST tahun 2001. AES dimaksudkan akan, secara bertahap, menggantikan DES sebagai standard enkripsi di Amerika Serikat untuk abad ke 21. Perbedaan utama antara teknik enkripsi AES dan teknik enkripsi DES adalah AES menggunakan substitusi (menggunakan S-boxes) secara langsung terhadap naskah, sedangkan DES tidak.

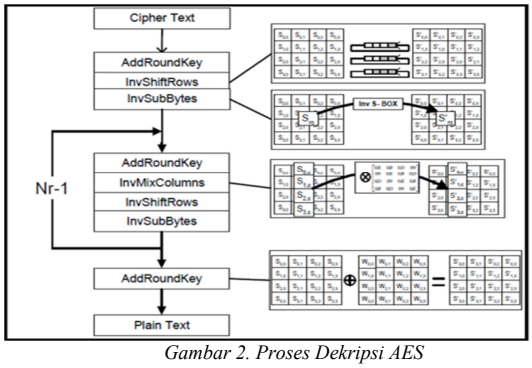
Di bawah ini adalah inti dari alur kerja Algoritma Rijndael pada blok 128 bit dengan kunci 128 bit tanpa diliputi proses pembangkitan *round key* di dalamnya:

1) *AddRoundKey*: melakukan operasi XOR antara *state* awal (*plainteks*) dengan cipher key. Tahap ini biasa disebut *initial round*.
2) Putaran sebanyak *Nr* – 1 kali. Ada beberapa proses yang terjadi pada setiap putaran, berikut adalah penjelasannya:
   a) *SubBytes*: substitusikan byte menggunakan tabel substitusi (S-box).
   b) *ShiftRows*: pergeseran baris-baris *array state* secara *wrapping*.
   c) *MixColumns*: mengacak data di masing-masing kolom *array state*.
   d) *AddRoundKey*: melakukan operasi XOR antara *state* sekarang *round key*.
3) Proses pada putaran terakhir (*final round)*:
   a) SubBytes
   b) ShiftRows
   c) MixColumn
   d) AddRoundKey



Gambar 1. Enkripsi AES

Untuk Proses Dekripsi AES, Transformasi *cipher* dilakukan secara terbalik dan diimplementasikan berlawanan arah agar menghasilkan *inverse cipher* yang tidak sulit dipahami untuk algoritma AES. Transformasi byte yang digunakan pada invers cipher adalah *InvShiftRows, InvSubBytes, InvMixColumns,* dan *AddRoundKey*.



Gambar 2. Proses Dekripsi AES

2.4. Algortima Blowfish

Blowfish merupakan enkripsi yang termasuk dalam golongan *Symmetric Cryptosistem* yang mana masih serupa dengan DES (DES-like Cipher), diciptakan oleh seorang *Cryptanalyst* bernama Bruce Schneier dan dipublikasikan pada tahun 1994.

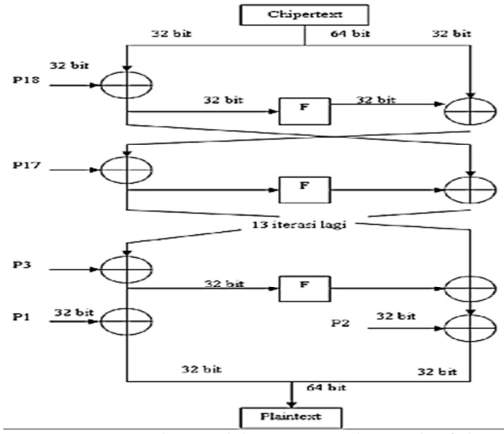
Algoritma Blowfish terdiri atas dua bagian, yaitu ekspansi kunci dan enkripsi data [5]. Berikut penjelasannya:

1. Ekspansi kunci (*Key-expansion*), berfungsi merubah kunci menjadi beberapa array subkunci (*subkey*). Berikut ini adalah uraian langkah pembangkitan subkunci yang dimaksudkan tersebut:
   1) Inisialisasi *P-array* yang pertama dan empat Sbox, berurutan, dengan string yang telah pasti. String tersebut terdiri dari *hexadecimal digits* dari phi, tidak termasuk angka tiga di awal.
      P1 = 243f6a88
      P2 = 85a308d3
      P3 = 13198a2e
      P4 = 03707344, dst.
      (hingga S-box urutan yang terakhir)
   2) XOR-kan P1 dengan 32-bit awal kunci, XOR-kan P2 dengan 32-bit berikutnya dari kunci, dan seterusnya untuk semua bit kunci. Ulangi siklus seluruh bit kunci secara berurutan sampai seluruh P-array terXOR-kan dengan bit-bit kunci. Berikut analoginya:
      P1 = P1 XOR K1
      P2 = P2 XOR K2
      P3 = P3 XOR K3, ... P14 = P14 XOR K14
      P15 = P15 XOR K1, ... P18 = P18 XOR K4
   3) Enkripsikan string yang seluruhnya nol (*all-zero string*) dengan algoritma Blowfish, menggunakan subkunci yang telah dideskripsikan pada langkah 1 dan 2.
   4) Gantikan P1 dan P2 dengan *output* dari langkah 3.
   5) Enkripsikan *output* langkah 3 menggunakan algoritma Blowfish dengan subkunci yang telah dimodifikasi.
   6) Gantikan P3 dan P4 dengan *output* dari langkah 5.

7) Lanjutkan langkah-langkah pada proses sebelum ini, gantikan seluruh elemen *P-array* dan kemudian keempat S-box secara berurutan, dengan hasil keluaran algoritma Blowfish yang terus-menerus berubah. Total keseluruhan, terdapat 521 iterasi.

2. Enkripsi Data, terdiri atas iterasi fungsi sederhana (*Feistel Network*) sebanyak 16 kali iterasi, masukannya adalah 64 bit elemen data X. Langkahnya adalah seperti di bawah ini:
   1) Bentuk inisial *P-array* sebanyak delapan belas buah (P1,P2,……..P18) masing-masing bernilai 32-bit. *P-array* terdiri atas delapan belas kunci 32-bit subkunci: P1,P2,…….,P18
   2) Bentuk S-box sebanyak 4 buah masing-masing bernilai 32-bit yang memiliki masukan 256. Empat 32-bit S-box masing-masing mempunyai 256 entri:
      S1,0,S1,1,……..,S1,255
      S2,0,S2,1,……..,S2,255
      S3,0,S3,1,……..,S3,255
      S4,0,S4,1,……..,S4,255
   3) Plainteks yang akan dienkripsi dianggap sebagai masukan, kemudian ambil sebanyak 64-bit tapi bila kurang dari 64-bit maka plainteks tersebut kita tambahkan bitnya agar dalam operasi nanti sesuai dengan datanya. Plainteks atau masukan dari proses ini diinisialkan menjadi "x".
   4) Bagi x menjadi 2 buah bagian sama besar, 32-bit pertama disebut xL (x kiri) dan 32-bit yang kedua disebut xR (x kanan).
   5) Lakukan iterasi sebanyak i=1 hingga i=16 untuk:
      $xL = xL \oplus P[i];$
      $xR = F(xL) \oplus xR;$
      Keterangan:
      $\oplus$ ialah simbol untuk operasi XOR.
   6) Hasil dari operasi diatas ditukar xL menjadi xR dan xR menjadi xL.
   7) Fungsi F adalah sebagai berikut: Bagi xL menjadi empat buah 8-bit a,b,c, dan d.
      $F(xL) = ((S_{0,a} + S_{1,b} \bmod 2^{32}) \oplus S_{2,c}) + S_{3,d} \bmod 2^{32}$
   8) Langkah terakhir adalah:
      $Swap(xL, xR);$
      $xR = xR \oplus P[17];$
      $xL = xL \oplus P[18];$
      Keterangan:
      $\oplus$ ialah simbol untuk operasi XOR.
   9) Kemudian gabungkan xL dan xR menjadi 64-bit *return* hasil gabungan.

Terdapat keunikkan pada proses dekripsi pada Algoritma Blowfish, yaitu urutan proses dekripsi dilakukan secara sama persis seperti pada proses enkripsi, akan tetapi saat proses dekripsi P1, P2,…, P18 digunakan dengan urutan terbalik (*reverse*). Berikut ini adalah gambaran dari dari blok diagram dekripsi Blowfish:



Gambar 3. Blok Diagram Dekripsi Blowfish

3. METODE PENELITIAN

3.1. Metodologi Penelitian

Dalam penelitian ini, beberapa metode digunakan untuk memperoleh informasi yang diperlukan dan menyelesaikan masalah yang ditemui. Adapun metode – metode ini sebagai berikut:

a. Studi literatur
   Metode ini digunakan untuk memperoleh pembelajaran data atau informasi dengan cara mengumpulkan berbagai referensi baik itu dalam bentuk makalah, jurnal, serta referensi lainnya untuk mendapatkan informasi yang dibutuhkan.
b. Analisis Data
   Metode ini digunakan untuk menganalisis algoritma kriptografi yang digunakan yaitu metode algoritma kriptografi AES-128 dan Blowfish serta teknik-teknik yang digunakan.
c. Perancangan Sistem
   Metode ini digunakan untuk merancang sistem aplikasi untuk mengimplementasikan metode algoritma kriptografi AES-128 dan Blowfish dengan menggunakan bahasa pemrograman Android.
d. Pengujian Sistem
   Metode ini dilakukan dengan menguji dan mengecek jalannya program.

3.2. Analisis dan Penyelesaian Masalah

Seiring dengan perkembangan teknologi yang semakin canggih, hal-hal yang bersifat manual mulai banyak ditinggalkan atau bahkan sudah tidak diminati lagi. Seperti halnya dalam berkomunikasi, banyak orang kini lebih suka mengobrol atau berkirim pesan melalui perantara aplikasi dimana fitur chatting menjadi satu hal yang paling diharapkan keberadaannya di dalam suatu aplikasi. Sayangnya, pemanfaatan internet untuk menunjang

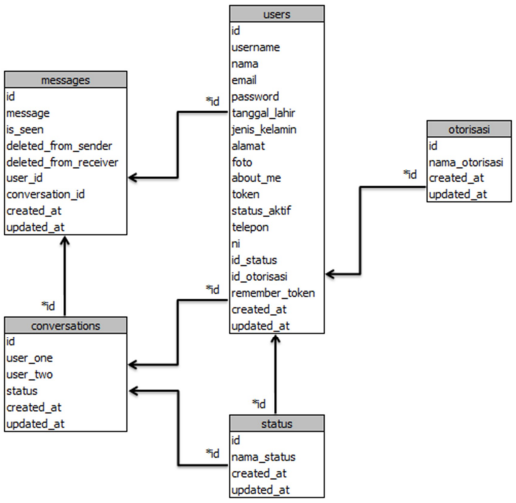
kegunaan fitur tersebut membuat keamanan dan kerahasiaan data menjadi suatu kekhawatiran tersendiri mengingat rawannya penyalahgunaan yang bisa dilakukan oleh pihak tertentu yang tidak berhak mengakses data atau pesan itu.

Dari permasalahan yang telah dijabarkan sebelumnya, maka perlu adanya sebuah fitur untuk ditambahkan pada aplikasi agar mampu menjebatani keinginan para pengguna untuk saling berkomunikasi dalam satu ruang yang sama, dengan jaminan privacy nya tetap terjaga. Kriptografi, sebagai ilmu pengamanan data, dipilih untuk diimplementasikan ke dalam fitur chatting pada aplikasi BLuCareer demi menjaga keamanan dan kerahasian pesan dari setiap pengguna.

Aplikasi kriptografi ini berbasis Android menggunakan bahasa pemrograman Java dan metodenya menggunakan algoritma AES dengan pemilihan panjang kunci sebesar 128-bit serta algoritma Blowfish. Algoritma kriptografi AES-128 dan Blowfish merupakan algoritma kunci simetris atau dikenal juga sebagai algoritma kriptografi konvensional, yaitu algoritma yang menggunakan kunci yang sama untuk kedua proses ini, enkripsi maupun dekripsi.

3.3. Rancangan Basis Data

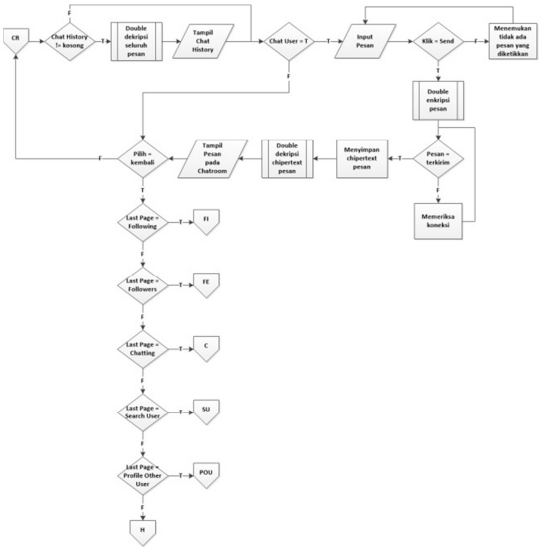
Berikut ini adalah *Logical Record Structure* (LRS) yang terdapat didalam basis data yang digunakan:



Gambar 4. Logical Record Structure (LRS)

3.4. Flowchart dan Algoritma Program

Berikut ini merupakan rancangan *flowchart* dan algoritma pemrograman pada *form* menu *chatroom* tempat dimana proses enkripsi dan dekripsi pesan terjadi, menggunakan algoritma AES-128 dan Blowfish.



Gambar 5. Flowchart Form Menu Chatroom

Flowchart pada Gambar 4 menjelaskan alur proses saat pengguna berkirim pesan pada *form* menu *chatroom.* Berikut adalah algoritma proses dari *flowchart* di atas:

```
1.  If Ada Chat History Then
2.      Jalankan Proses Double Dekripsi pada Seluruh
        Pesan
3.  Else
4.      If User Ingin Kirim Chat Then
5.      Ketik Pesan
6.      Pilih Action
7.      If Action = Send Then
8.          Cek Isi Pesan
9.          If Pesan Terisi Then
10.             Double Enkripsi Pesan
11.             Mengirim Pesan ke Tujuan
12.             If Pesan Terkirim Then
13.                 Simpan Chipertext Pesan ke
                    Database
14.                 Double Dekripsi Chipertext Pesan
15.                 Tampilkan Pesan
16.                 Lompat ke Baris 23
17.             Else
18.                 Memeriksa Koneksi
19.             End If
20.         Else
21.             Kembali ke Baris 5
22.         End If
23.     Else
24.         Pilih Action
25.         If Action = kembali Then
26.             If Last Page = Following Then
27.                 Kembali ke Form Menu Following
28.             Else If Last Page = Followers Then 40
29.                 Kembali ke Form Menu Followers
30.             Else If Last Page = Chatting Then
31.                 Kembali ke Form Menu Chatting
32.             Else If Last Page = Search User Then
33.                 Kembali ke Form Menu Search User
```

```
34.         Else
35.         Kembali ke Form Menu Open Class Home
36.         End If
37.      Else
            Tetap di Chatroom
39.   End If
40. End If
```

Algoritma pada Proses Double Enkripsi dengan algoritma AES-128:

```
1.  Ambil Pesan
2.  Inisialisasi Kunci
3.  Lakukan AddRoundKey
4.  Set Round = 0
5.  Round++
6.  Lakukan SubBytes
7.  Lakukan ShiftRows
8.  Lakukan MixColumns
9.  Lakukan AddRoundKey
10. If Round ≤ 9 Then
11.       Kembali ke Baris 6
12. Else
13.       Lakukan SubBytes
14.       Lakukan ShiftRows
15.       Lakukan AddRoundKey
16.       Menghasilkan Ciphertext Pesan AES-128
17. End If
18. End
```

Algoritma pada Proses Double Enkripsi dengan algoritma Blowfish:

```
1.  Start
2.  Ambil Ciphertext Pesan AES-128
3.  Inisialisasi x = Ciphertext Pesan AES-128
4.  Membagi x menjadi 2 bagian sama panjang =
    xL dan xR
5.  Set i = 0
6.  i++
7.  Hitung xL = xL XOR P[i] dan
    xR = F(xL) XOR xR
8.  Tukar xL dan xR
9.   If i ≤ 16 Then
10.      Kembali ke Baris 6
11. Else
12.      Tukar xL dan xR
13.      Hitung xR = xR XOR P[17] dan
         xL = xL XOR P[18]
14       Gabungkan Kembali xL dan xR
15       Menghasilkan Ciphertext Pesan Double
         Enkripsi
16. End If
17. End
```

Algoritma pada Proses Double Dekripsi dengan algoritma Blowfish:

```
1.  Start
2.  Ambil Ciphertext Pesan Double Enkripsi
3.  Inisialisasi x = Ciphertext Pesan Double
    Enkripsi
4.  Membagi x menjadi 2 bagian sama panjang =
    xL dan xR
5.  Set i = 19
6.  i--
7.  Hitung xL = xL XOR P[i] dan
    xR = F(xL) XOR xR
8.  Tukar xL dan xR
9.   If i ≤ 3 Then
10.      Kembali ke Baris 6
11. Else
12.      Tukar xL dan xR
13.      Hitung xR = xR XOR P[2] dan
         xL = xL XOR P[1]
14.      Gabungkan Kembali xL dan xR
15.      Menghasilkan Pesan TerdekripsiBlowfish
16. End If
17. End
```

Algoritma pada Proses Double Dekripsi dengan algoritma AES-128:

```
1.  Start
2.  Ambil Pesan Terdekripsi Blowfish
3.  Inisialisasi Kunci
4.  Lakukan AddRoundKey
5.  Set Round = 0
6.  Round++
7.  Lakukan Inverse ShiftRows
8.  Lakukan Inverse SubBytes
9.  Lakukan AddRoundKey
10. Lakukan Inverse MixColumns
11.  If Round ≤ 9 Then
12.      Kembali ke Baris 6
13.  Else
14.       Lakukan Inverse ShiftRows
15.       Lakukan Inverse SubBytes
16.       Lakukan AddRoundKey
17.       Menghasilkan Pesan Asli
18.  End If
19. End
```

4. HASIL DAN PEMBAHASAN

4.1. Tampilan Layar

4.1.1. Tampilan Layar *Form* Menu *Chatroom*

Gambar 6. Tampilan Layar Menu History

Tampilan layar *Form* Menu *Chatroom* merupakan ruang dimana dua pengguna terhubung untuk saling berkirim pesan. Disini juga pengguna dapat melihat histori *chat* secara keseluruhan jika sebelumnya sudah melakukan obrolan dengan si penerima pesan. Jika belum, maka pengguna bisa mulai mengobrol dengan cara mengetikkan pesan pada kolom *input* pesan yang berada di paling bawah tampilan layar.

4.2. Pengujian Program

Tabel 1. Hasil Pengujian Proses Enkripsi dan Dekripsi

Pesan	Output AES-128	Output Blowfish	Waktu Enkripsi (detik)*	Waktu Dekripsi (detik)**
halo	4BOZiNL7VR1R2G0/dc5EHg	Mn1Edz0oQlhU5m6kOVVpOoz1rmZ6rr9e	00.50	00.87
apa kabar?	ae9dvxe+oJACDvvuwn5dJg	dvZW3OxGZdkM3E6UJkYrl23e3Gt60Ca3	00.54	01.03
boleh tanya sesuatu?	GPVyYPQ4wH5OMFf3aOm0M2B9WVp2wI7SX/gKXA16zCk	K76AFLIzUzqqOp2H5eIveMBlf+VvqCKyU68HNGyCB2DZiFmcjtRpu0OxOHOBlkwJ	00.56	01.26
ikut kelas java yuk!!!!	WNXQW/3rAd0Suq8o2gtT0+xUXAdiNAfPOosNYO+JnLA	rX3OaQyV5lRTFFdS8jBaHMruJMmAeHZ2E9O5ui70yov+kE3W9xGgsc5IGtNyD8YC	00.70	01.33
jangan	a+YrY8d	IY5KSYM	00.73	
lupa bayar 75.000	v5eTEIbHFEEDQjnpVHf6oZMj0mrfkWeP5hyw	R5cWYu4fLxRaYcyXz5k3TxEzr5e1eb6vQWtN3dWrqpnjmFT3KB68ABFju		01.35
besok ingetin aku uas jam 08:00 ya	o9lOS1j2DHNUsU2bnsRosItNk+T1pXMjoKjhK+fMZtk+2ufkvVEahW4e3BaKg/rd	yO3NyxIUWfci7fvo2AEOi2GdLlW+IxT+oO0y4wglF26lmj+iV4xRzrxnWtzBgnpKkjn7xAagCzUEdqs5IGbFZUa8Da+TcxTB	00.80	01.48
eh si *$** mau ketemu kamu tuh :p	v9iRz8AEgwt5niGFAO0wbf/Ra+QUv9ACn7jPAmfFeb/WNOhgxR4yl8ThA3pgttYT	XTi+uvnTW+71en8zaV9jawlnIu9kMIwPuj4tqz/q5SvyjRBL8frySmIsxteavuPIw5efnzWHMTfuasK0oTLzK0a8Da+TcxTB	00.76	01.42
BL kapan libur deh?!	H4PCW+V2fdduYieub47qOU5TeZ/bjZzxMXnA1EhEPkU	97f2klMjyIDCB9NpPpC6Bq0DROTjV7iCZtJwH5yIZ9VAf4/fV68AN+GWXgCeAUcU	00.57	01.25
numpang tes: !2345^ &'/}|"+	1Pfuej82M865nri+TBiyUvnaeM6baAHdimuQvKNgDbw	tVkU0pQdo14rae2p4z7p/xi4t3Cc5HcR/nhVoE6JT2spSwGlcn4eEE4ewqwsjB+R	00.74	01.37
BYE.	L5Pm5zUhdRcpCAtRObK2YA	LVdorHAnlHg/UERi12lA8bB0QoBkwoyk	00.50	00.89
Rata-rata Waktu			0.64	1.23

* waktu enkripsi dihitung mulai saat tombol send diklik hingga pesan terenkripsi terkirim

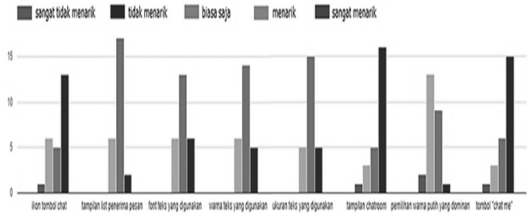
** waktu dekripsi dihitung ketika pesan asli muncul pada layar setelah dilakukan refresh.

Ditinjau dari hasil pengujian pada Tabel 1 diketahui bahwa jumlah presentase keberhasilan proses enkripsi dan dekripsi mencapai 100%. Dengan rata-rata waktu kurang dari satu menit, yaitu 0.64 detik untuk proses enkripsi dan 1.23 detik untuk proses dekripsi.

4.3. Tanggapan Pengguna

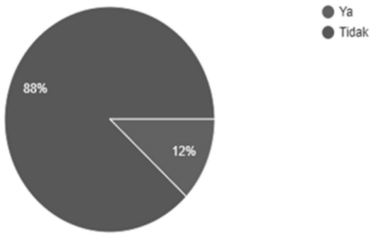
Setelah program rampung dibuat maka dilakukan *testing* program kepada para pengguna yang bersedia menuliskan *feedback*-nya melalui pengisian kuesioner yang penulis buat. Berikut adalah hasil yang didapatkan dari 25 responden yang bersedia.

1. Seberapa menarik tampilan fitur chatting kami?



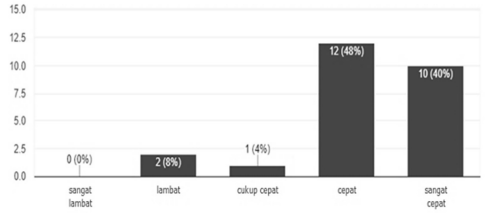
Gambar 7. Hasil kuesioner pertanyaan pertama

2. Apakah anda mengalami gagal mengirimkan pesan?



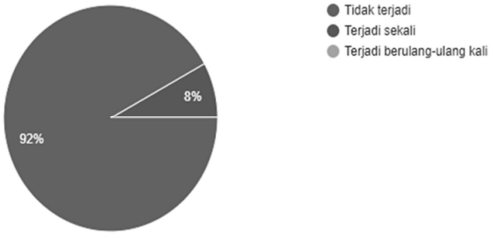
Gambar 8. Hasil kuesioner pertanyaan kedua

3. Seberapa cepat proses pengiriman pesan yang anda rasakan dengan menggunakan fitur chatting kami?



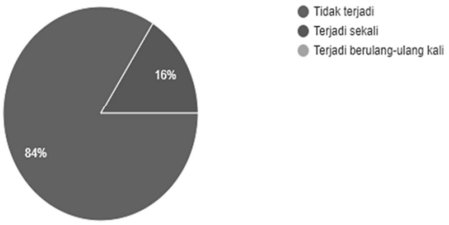
Gambar 9. Hasil kuesioner pertanyaan ketiga

4. Apakah pesan tertampil ganda atau terjadi duplikasi?



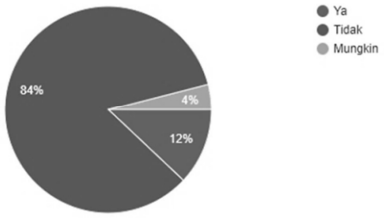
Gambar 10. Hasil kuesioner pertanyaan keempat

5. Apakah sempat terjadi error ketika chatting?



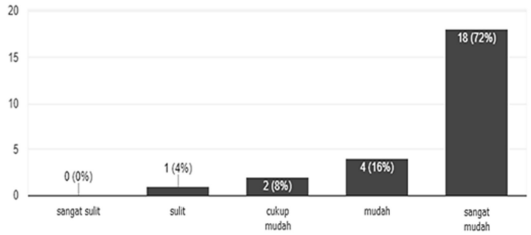
Gambar 11. Hasil kuesioner pertanyaan kelima

6. Apakah anda kesulitan dalam mengakses pesan masuk?



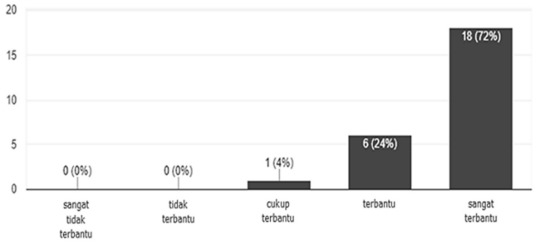
Gambar 12. Hasil kuesioner pertanyaan keenam

7. Apakah anda mengalami kesulitan dalam menggunakan fitur chatting kami?



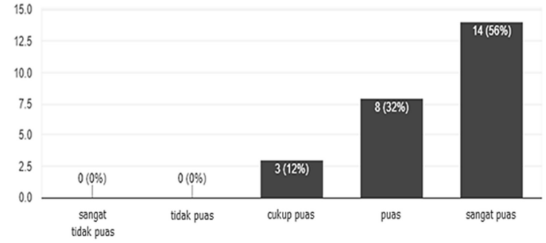
Gambar 13. Hasil kuesioner pertanyaan ketujuh

8. Apa anda merasa terbantu dengan adanya fitur chatting pada aplikasi ini untuk berkomunikasi antara sesama pengguna?



Gambar 14. Hasil kuesioner pertanyaan kedelapan

9. Secara keseluruhan seberapa puas anda dengan fitur chatting yg kami sediakan?



Gambar 15. Hasil kuesioner pertanyaan kesembilan

10. Silahkan beri saran dan masukan tambahan untuk kami

Gambar 16. Hasil kuesioner pertanyaan kesepuluh

4.4. Kelebihan Program

a. Aplikasi menjadi lebih aman karena menggunakan dua algoritma kriptografi yaitu AES-128 dan Blowfish yang merupakan algoritma kriptografi kunci simetris.
b. Isi pesan dari hasil dekripsi tidak mengalami perubahan atau kembali seperti pesan asli.
c. Proses enkripsi dan dekripsi berlangsung cepat.
d. Inputan pesan dapat berupa karakter angka, huruf dan simbol.

4.5. Kekurangan Program

a. Hasil enkripsi akan sama untuk setiap pesan yang berisi sama, karena kunci sudah diinsialisasikan pada program.
b. Hanya pesan berupa teks saja yang bisa dikirimkan ketika *chatting*.
c. Belum ada notifikasi pesan masuk.
d. Aplikasi ini belum bersifat real-time *chatting.*

5. KESIMPULAN

a. Aplikasi ini dapat menjaga kerahasiaan dan keamanan setiap pesan yang dikirimkan oleh pengguna karena mengimplementasikan kriptografi dengan menggunakan dua algoritma, yaitu algoritma AES-128 dan Blowfish.
b. Meski pesan yang dikirimkan mengalami proses enkripsi, tapi pesan yang tampil dilayar pengguna akan tetap sama seperti pesan asli yang diketikkan. Hal ini terjadi berkat proses dekripsi yang berhasil mengubahnya kembali seperti semula tanpa terjadi perubahan pada isi pesan.
c. Proses dekripsi dengan menggunakan kunci yang sesuai akan mengembalikan pesan yang telah terankripsi menjadi pesan asli tanpa mengalami perubahan pada isi.
d. Panjang pesan dan koneksi data mempengaruhi lama proses kerja enkripsi maupun dekripsi.
e. Dari hasil pengujian diketahui bahwa 0.64 detik merupakan rata-rata waktu yang diperlukan untuk satu kali proses enkripsi sementara untuk proses dekripsi memerlukan waktu 1.23 detik. Walaupun, proses dekripsi memakan waktu lebih lama daripada proses enkripsi tapi hal tersebut tidak terlalu menjadi pembeda yang signifikan di antara keduanya karena sama-sama masih terbilang cepat dan memiliki presentase keberhasilan mencapai 100%.

6. DAFTAR PUSTAKA

[1] Adinta, Firlya, dan Indri Neforawati. 2017. *Rancang Bangun Aplikasi Chatting Berbasis Web Menggunakan Docker*. Jakarta..
[2] Haryadi, Mohamad Fauzi, 2010. *Analisa dan Perancangan Aplikasi Chatting Berbasis Web Menggunakan Flash CS3*. Sekolah Tinggi Manajemen Informasi Dan Komputer. Yogyakarta.
[3] Kromodimoeljo, Sentot. 2009. *Teori dan Aplikasi Kriptografi*. Jakarta: SPK IT Consulting.
[4] Rahman, M.T., Aryo Pinandito, dan Eko S.P. 2017. *Perbandingan Performansi Algoritme Kriptografi Advanced Encryption Standard (AES) dan Blowfish pada Text di Platform Android*. Jawa Timur.
[5] Schneier, Bruce. 1996. *Applied Cryptography*. John Wiley & Sons, Inc.