IMPLEMENTASI ALGORITMA VIGENERE CIPHER DALAM APLIKASI CHATTING UNTUK PENGAMANAN INFORMASI BERBASIS DESKTOP

Marchandi [1)], Ferdiansyah [2)]
[1]Program Studi Teknik Informatika, Fakultas Teknologi Informasi, Universitas Budi Luhur
[1,2]Jl. Raya Ciledug, Petukangan Utara, Kebayoran Lama, Jakarta Selatan 12260
E-mail : 1211520174@student.budiluhur.ac.id[1)] , ferdiansyah@budiluhur.ac.id[2)]

Abstrak

Perkembangan teknologi jaringan dan internet memungkinkan setiap orang untuk saling bertukar data, informasi, atau pesan kepada orang lain tanpa batasan jarak dan waktu. Masalah keamanan dan kerahasiaan data dan informasi merupakan suatu hal yang penting. Ditengah berkembang pesatnya teknologi komunikasi tentunya harus diiringi dengan tingkat keamanan yang baik pula. Tanpa adanya jaminan keamanan, orang lain dapat dengan mudah mendapatkan informasi yang dikirimkan melalui jaringan komputer dan internet. Oleh karena itu, dikembangkanlah cabang ilmu yang mempelajari tentang cara-cara pengamanan data atau dikenal dengan istilah kriptografi. Metode kriptografi yang digunakan pada penelitian ini adalah vigenere cipher. Teknik ini merupakan salah satu jenis algoritma yang popular dan sering digunakan sebagai metode penyembunyian pesan (kriptografi), di mana huruf pada pesan yang akan dikirimkan digantikan dengan huruf lain yang memiliki perbedaan tertentu pada urutan alfabet. Dalam penelitian ini algoritma vigenere cipher dapat melakukan kriptografi pada teks berupa huruf, angka dan simbol, dan key yang digunakan juga dapat berupa teks huruf, angka dan symbol. Aplikasi yang dibuat dalam penelitian ini merupakan aplikasi chatting berbasis desktop, dan menggunakan bahasa pemrograman c# dan visual studio sebagai aplikasi editornya. Aplikasi chatting ini menggunakan algoritma vigenere cipher sebagai metode enkripsi, yang bertujuan agar pembicaraan yang dilakukan dengan aplikasi chatting ini tidak dapat dibaca oleh orang-orang yang tidak berkepentingan dan hanya dapat dibaca oleh orang-orang yang memiliki key. Manfaat dari penelitian ini adalah menjelaskan bagaimana teori dan proses dalam mengenkripsi dan dekripsi sebuah pesan, dan dapat menghasilkan sebuah aplikasi yang dapat melakukan pengiriman teks dan dienkripsi serta dilengkapi dengan key yang kemudian dikirim melewati sebuah jaringan local dan didekripsi setelah diterima oleh penerimanya. Setelah mempelajari permasalahan yang dihadapi, dapat disimpulkan bahwa teknik kriptografi mampu menyembunyikan pesan dengan baik, dan dapat diimplementasikan dalam sebuah aplikasi chatting, yang membuat kerahasiaan dari pesan dalam percakapan tersebut dapat terjaga keamanannya.

Kata Kunci : Kriptografi, vigenere cipher, Enkripsi, Chatting, Key

1. PENDAHULUAN

Perkembangan teknologi jaringan dan *internet* memungkinkan setiap orang untuk saling bertukar data, informasi, atau pesan kepada orang lain tanpa batasan jarak dan waktu. Masalah keamanan dan kerahasiaan data dan informasi merupakan suatu hal yang penting. Ditengah berkembang pesatnya teknologi komunikasi tentunya harus diiringi dengan tingkat keamanan yang baik pula. Banyak kejahatan cyber yang terjadi salah satunya yang terkait, dengan manipulasi data pada jaringan internet. Masalah terpenting dalam jaringan komputer adalah masalah keamanan data yang dikirimkan. Sebagian besar data menyimpan informasi bagi tiap individu, yang dipertukarkan membutuhkan pengamanan untuk menjaga integritas pesan tersebut agar tidak disalahgunakan oleh pihak yang tidak berhak mengetahui informasi dari data tersebut.

Keamanan dan kerahasiaan merupakan faktor penting yang dibutuhkan dalam proses pertukaran informasi melalui *internet*, karena ikut berkembang pula kejahatan teknologi dengan berbagai macam teknik, seperti penyebaran virus, penyadapan, modifikasi, *spamming*, serangan *hacker*, dan lain-lain. Tanpa adanya jaminan keamanan, orang lain dapat dengan mudah mendapatkan informasi yang dikirimkan melalui jaringan komputer dan *internet*.

PT Mutiara Sinergi Abadijaya merupakan salah satu perusahaan lokal yang bergerak di bidang distributor mesin peralatan dan perlengkapan sablon manual dan digital/chemical printing suplier. Informasi perusahaan yang bersifat rahasia tidak boleh diketahui oleh sembarang orang agar rahasia perusahaan tetap aman.

Informasi perusahaan yang bersifat rahasia tersebut harus terjamin keamanannya. Karena, jika informasi rahasia tersebut diketahui oleh pihak yang tidak bertanggung jawab, dan dibocorkan kepada pihak kompetitor, tentunya hal tersebut dapat mengganggu penjualan ataupun pemasaran produk perusahaan. Dalam skala yang lebih kompleks, tidak mustahil akan menyebabkan kerugian yang cukup besar.

Pada saat ini perusahaan belum menerapkan sistem keamanan dalam aplikasi percakapan internal perusahaan mereka. Sehingga jaminan bahwa informasi perusahaan mereka yang berasal dari percakapan di aplikasi internal mereka tidak bocor

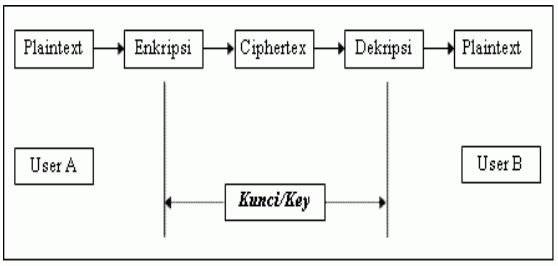
ke pihak kompetitor masih belum ada. Oleh sebab itu diperlukan salah satu cara mengamankan informasi tersebut adalah dengan mengembangkan aplikasi *chatting* kriptografi dimana informasi yang akan dikirimkan akan diubah menjadi *ciphertext* terlebih dahulu, sehingga pesan asli yang dikirimkan tidak terbaca oleh pihak luar. Teknik Teknik *vigenere cipher* merupakan salah satu jenis algoritma klasik yang popular dan sering digunakan sebagai metode penyembunyian pesan (kriptografi), dimana huruf pada pesan yang akan dikirimkan digantikan dengan huruf lain yang memiliki perbedaan tertentu pada urutan alfabet.

2. RANCANGAN SISTEM DAN APLIKASI

2.1. DESAIN SISTEM

Teknik kriptografi dalam pengacakan pesan dan mengembalikan pesan menjadi pesan asli, terdiri dari dua proses, yaitu proses enkripsi dan dekripsi. Proses enkripsi adalah proses mengubah plaintext menjadi ciphertext sehingga pesan asli diacak menjadi pesan yang sudah dibaca isinya, sedangkan proses dekripsi merupakan kebalikan dari enkripsi yaitu mengubah ciphertext menjadi plaintext atau pesan aslinya.

Berikut adalah gambaran sederhana proses pengacakan pesan dan mengembalikan pesan menjadi pesan asli kembali.



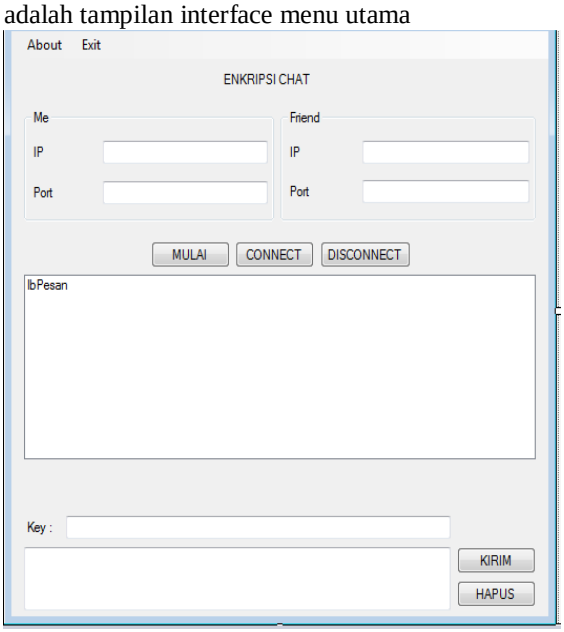
Gambar 1. Desain Konsep Aplikasi

2.2. USE CASE DIAGRAM

Use case diagram adalah diagram yang merupakan representasi visual yang mewakili interaksi anara pengguna dan sistem informasi unruk menunjukan peran dari pengguna dan bagaimana peran – peran menggunakan sistem. Use case diagram digunakan untuk memodelkan bisnis proses berdasarkan perspektif pengguna sistem. Use case diagram terdiri atas diagram untuk use case dan actor. Actor yang melakukan operasi dihubungkan dengan garis lurus ke use case. Use case Berfungsi untuk memodelkan aplikasi berorientasi obyek. Use case merupakan gambaran fungsionalitas dari suatu sistem, sehingga aktor atau pengguna sistem paham dan mengerti mengenai kegunaan sistem yang akan dibangun. Setiap use case mengekspresikan goal dari sistem yang harus dicapai. Diberi nama sesuai dengan goal-nya dan digambarkan dengan elips dengan nama di dalamnya. Fokus tetap pada goal bukan bagaimana mengimplementasikannya walaupun use case berimplikasi pada prosesnya nanti. Setiap use case biasanya memiliki trigger pemicu yang menyebabkan use case memulai. Ada 2 trigger pertama trgiger eksternal, kedua trigger temporal.

2.3. INTERFACE MENU UTAMA

Pada tampilan layar menu utama berisi beberapa *field* isian, yaitu *field* untuk memasukkan *ip* dan *port* yang kita gunakan dalam jaringan dan aplikasi yang kita gunakan, *field* untuk memasukkan *ip* dan *port* yang digunakan oleh lawan kita, *field* untuk memasukkan kunci yang akan digunakan, serta *field* untuk memasukan pesan yang akan dikirim. Terdapat 2 menu *item* yaitu *about* dan *exit*. Berikut adalah tampilan interface menu utama



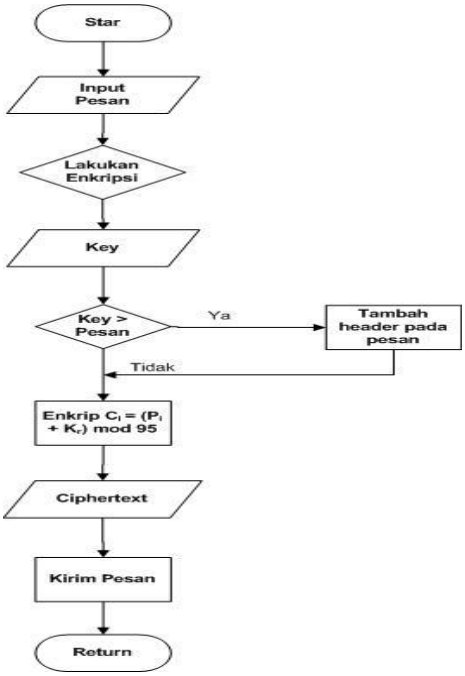
Gambar 2. Rancangan Layar Menu Utama

2.4. FLOWCHART DAN ALGORITMA

Flowchart adalah untuk menggambarkan, menyederhanakan rangkaian proses atau prosedur sehingga mudah dipahami dan mudah dilihat berdasarkan urutan langkah dari suatu proses.

Flowchart dan algoritma merupakan langkah awal pembuatan program. Dengan adanya flowchart dan algoritma, urutan proses kerja menjadi lebih jelas. Jika ada penambahan suatu proses maka akan dapat dilakukan dengan lebih mudah. *Flowchart* dan algoritma aplikasi *chatting* enkripsi ini terbagi menjadi dua, yaitu proses enkripsi pesan dan proses dekripsi pesan.

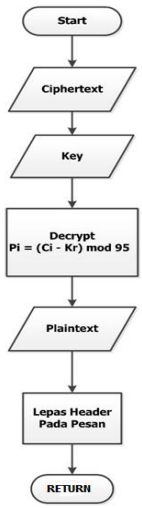
1) Flowchart Proses Enkripsi



Gambar 3. Flowchart Proses Enkripsi

2) Algoritma Proses Enkripsi
Start
Input pilih
Input pesan
Pilih = YA
Input key
IF KEY > LENGTH(pesan)
Tambah header pada pesan
ELSE
proses Encrypt $C_i = (P_i + K_r) \bmod 95$
Tampil output berupa ciphertext
END IF
END IF
RETURN

3) Flowchart Proses Dekripsi



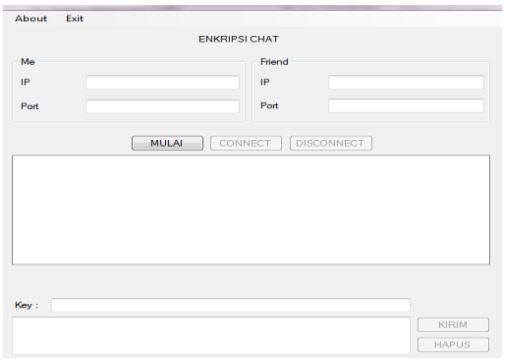
Gambar 4. Flowchart Proses Dekripsi

4) Algoritma Proses Dekripsi
Start
Input Pilih
Input key
IF Pilih = YA THEN
Proses decrypt $P_i = (C_i - K_r) \bmod 95$
Proses melepas header
Tampil output berupa plaintext
END IF
RETURN

3. HASIL DAN PEMBAHASAN

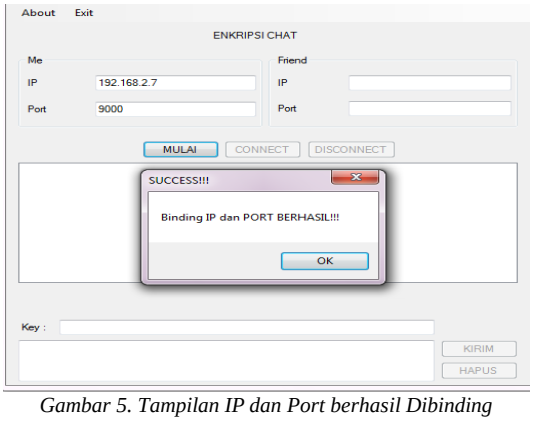
3.1. PROSEDUR MENJALANKAN APLIKASI

Pada aplikasi enkripsi dan deskripsi chatting dengan menggunakan metode Vigenere Cipher terdapat beberapa *form* atau *interface* yang di desain untuk mempermudah user atau pemakai dalam menggunakan atau menjalankan aplikasi. Pada langkah pertama, jalankan aplikasi sehingga muncul tampilan menu utama dari aplikasi seperti pada gambar dibawah ini:



Gambar 4. Tampilan Menu Utama

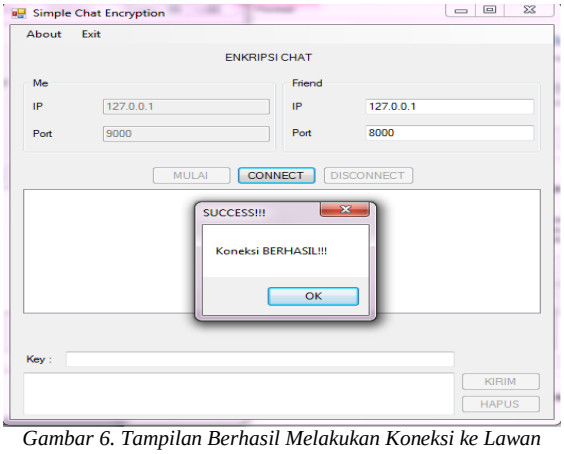
Pada proses selanjutnya adalah memasukkan *IP* dan *port* yang akan digunakan oleh user pada kolom *IP* dan *port* yang berada pada *group box me*, kemudian klik tombol mulai maka akan tampil pesan berhasil Binding Ip dan Port seperti gambar dibawah ini:



Gambar 5. Tampilan IP dan Port berhasil Dibinding

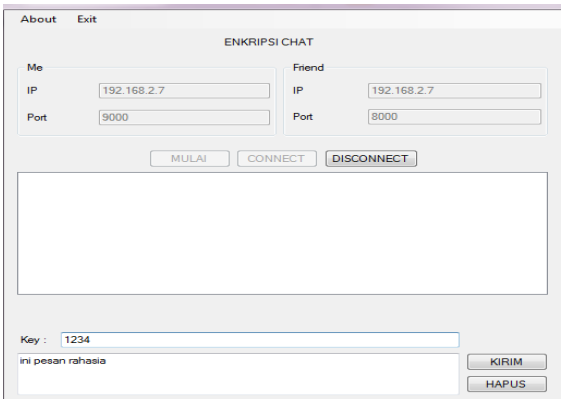
Lakukan hal yang sama dengan yang diatas pada desktop lawan bicara, kemudian, jika system berhasil melakukan koneksi dengan lawan bicara,

maka system akan menampilkan pesan bahwa koneksi telah terbentuk, seperti pada gambar dibawah ini:



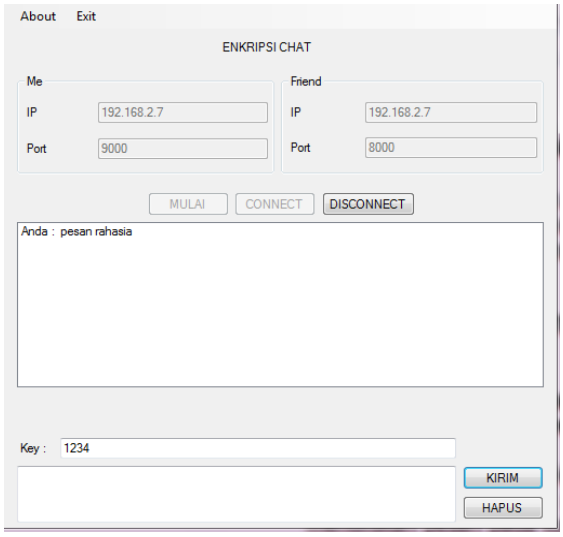
Gambar 6. Tampilan Berhasil Melakukan Koneksi ke Lawan Bicara

Setelah koneksi dengan lawan bicara telah terbentuk, selanjutnya adalah melakukan pengiriman pesan dengan enkripsi. Langkah pertama yang harus dilakukan adalah menuliskan pesan pada kolom pesan yang tersedia, kemudian masukuan key untuk enkripsi pesan seperti gambar dibawah ini:



Gambar 7. Tampilan Menuliskan Pesan dan key pada Kolom Pesan dan kolom key

Setelah pesan dikirim, dan diterima oleh lawan bicaranya, maka pesan yang dituliskan sebelumnya akan muncul di kotak percakapan di sisi *user* dan di sisi lawan bicaranya. Seperti yang terlihat pada gambar di bawah ini:



Gambar 8. Tampilan Kotak Percakapan Sisi User

3.2. PENGUJIAN SISTEM

Proses pengujian sistem yang dilakukan adalah mencoba memasukkan kata kedalam aplikasi yang telah dibuat dan kemudian disesuaikan dengan perhitungan manual algoritma vigenere sebagai contoh

Plaintext adalah #VIGE1234nere#hallo

Kunci adalah 1234

Karakter	**A**	**B**	**C**	**D**	**E**
Posisi Karakter	0	1	2	3	4
Karakter	**F**	**G**	**H**	**I**	**J**
Posisi Karakter	5	6	7	8	9
Karakter	**K**	**L**	**M**	**N**	**O**
Posisi Karakter	10	11	12	13	14
Karakter	**P**	**Q**	**R**	**S**	**T**
Posisi Karakter	15	16	17	18	19
Karakter	**U**	**V**	**W**	**X**	**Y**
Posisi Karakter	20	21	22	23	24
Karakter	**Z**	**a**	**b**	**c**	**d**
Posisi Karakter	25	26	27	28	29
Karakter	**e**	**f**	**g**	**h**	**i**
Posisi Karakter	30	31	32	33	34
Karakter	**j**	**k**	**l**	**m**	**n**
Posisi Karakter	35	36	37	38	39
Karakter	**o**	**p**	**q**	**r**	**s**
Posisi Karakter	40	41	42	43	44
Karakter	**t**	**u**	**v**	**w**	**x**
Posisi Karakter	45	46	47	48	49
Karakter	**y**	**z**	**0**	**1**	**2**
Posisi Karakter	50	51	52	53	54
Karakter	**3**	**4**	**5**	**6**	**7**
Posisi Karakter	55	56	57	58	59
Karakter	**8**	**9**	**~**	**`**	**!**
Posisi Karakter	60	61	62	63	64
Karakter	**@**	**#**	**$**	**%**	**^**
Posisi Karakter	65	66	67	68	69
Karakter	**&**	*****	**(**	**)**	**-**
Posisi Karakter	70	71	72	73	74
Karakter	**_**	**=**	**+**	**[**	**{**
Posisi Karakter	75	76	77	78	79
Karakter	**]**	**}**	**|**	**;**	**:**
Posisi Karakter	80	81	82	83	84
Karakter	**,**	**.**	**<**	**>**	**/**
Posisi Karakter	85	86	87	88	89
Karakter	**?**	**'**	**_**	**"**	**space**
Posisi Karakter	90	91	92	93	94

Gambar 9. Susunan Karakter Tabel Vigenere Cipher Modifikasi

Untuk pengujiannya sebagai berikut;

(Huruf pertama dari Plaintex + Huruf pertama dari Kunci)mod 95

1. (# + 1)mod 95=(66 + 53)mod 95
   = 119 mod 95 = 24 =(Y)
2. (V + 2)mod 95=(21 + 54)mod 95
   = 75 mod 95 = 75 = (_)
3. (I + 3)mod 95=(8 + 55)mod 95
   = 63 mod 95 = 63 =(`)
4. (G + 4)mod 95=(6 + 56)mod 95
   = 62 mod 95 = 62 =(~)
5. (E + 1)mod 95=(4 + 53)mod 95
   = 57 mod 95 = 57 =(5)
6. (1 + 2)mod 95=(53 + 54)mod 95
   = 12 mod 95 = 12 =(M)
7. (2 + 3)mod 95=(54 + 55)mod 95
   = 14 mod 95 = 14 =(O)
8. (3 + 4)mod 95=(55 + 56)mod 95
   = 16 mod 95 = 16 =(Q)
9. (4 + 1)mod 95=(56 + 53)mod 95
   = 14 mod 95 = 14 =(O)
10. (n + 2)mod 95=(39 + 54)mod 95
    = 93 mod 95 = 93 =(“)
11. (e + 3)mod 95 =(30 + 55)mod 95
    = 85 mod 95 = 85 =(,)
12. (r + 4)mod 95=(43 + 56)mod 95
    = 4 mod 95 = 4 =(E)
13. (e + 1)mod 95=(30 + 53)mod 95
    = 83 mod 95 = 83 =(;)
14. (# + 2)mod 95=(66 + 54)mod 95
    = 25 mod 95 = 25 =(Z)
15. (h + 3)mod 95=(33 + 55)mod 95
    = 88 mod 95 = 88 =(>)
16. (a + 4)mod 95=(26 + 56)mod 95
    = 82 mod 95 = 82 =(|)
17. (l + 1)mod 95=(37 + 53)mod 95
    = 90 mod 95 = 90 =(?)
18. (l + 2)mod 95=(37 + 54)mod 95
    = 91 mod 95 = 91 =(‘)
19. (o +3)mod 95=(40 + 55)mod 95
    = 0 mod 95 = 0 = (A)

Dari perhitungan diatas dapat disimpulkan hasil enkripsi dari plaintext #VIGE1234nere#hallo dengan kunci 1234 adalah Y_’~5MOQO”,E;Z>|?’A

3.3. TABEL HASIL PENGUJIAN ENKRIPSI PESAN

Proses pengujian sistem yang dilakukan adalah mencoba memasukkan kata kedalam aplikasi yang telah dibuat dengan key yang berbeda kemudian disesuaikan dengan algoritma vigenere.

plaintext/pesan	Kunci	Hasil Enkripsi	Ukuran (Byte)	Lama Enkripsi (Milidetik)
alamat	123456789	Y_'~9QSUWPRTVXC/TY]|A:J	25	1
rahasia	abcdefghijk	\wkji579'@S68~!#&~=!G{082)!5	28	0
81345125	123456789	Y_'~9QSUWPRTVXC/TYTNQSURTX	27	1
perusahaan	123456abcdefg	Y_'~9Q]|:,>57};,</C4&6A*9_ED}/;:@	33	1
nama	123456	y_'~9QMOQSUC;Cb8:']	20	0
pesan	3256859	a_@!!RURRWUaB'D:cE?G<	22	0
chatting	idandaya	Fyith8{0)60/3@]^!A2(3*A8)9	26	1
vigenere	algoritma	\6ouv8|&#^*+[^)_}4\:#())_}4	27	1
apa kabar?	vigenerecipher	S3okr++~6)*=8*}_@8|^))6FS-4q;874|Z	34	1

Gambar 10. Hasil Dekripsi Pesan

4. PENUTUP

4.1. KESIMPULAN

Berdasarkan perancangan, uji coba, analisis pada system yang telah dibuat dapat dibuat kesimpulan sebagai berikut :

a. Aplikasi *chatting* enkripsi untuk desktop windows berhasil dibangun.
b. Enkripsi pesan *chatting* pada aplikasi ini berhasil dibangun dengan menerapkan algoritma *vigenere cipher*.
c. Aplikasi *chatting* enkripsi ini dapat mengubah *plaintext* ke *ciphertext* sebelum pesan dikirim, dan juga dapat merubah kembali *ciphertext* yang diterima menjadi *plaintext*.
d. Aplikasi dapat melakukan pengamanan terhadap pesan yang dikirim.

4.2. SARAN

Berdasarkan hasil pengujian yang dilakukan pada penelitian ini serta kesimpulan diatas, dapat disampaikan saran-saran untuk perbaikan pada pembangunan aplikasi pada penelitian selanjutnya yaitu :

a. Aplikasi *chatting* enkripsi ini hanya dapat mengirim dan menerima pesan dalam bentuk teks. Pada penelitian selanjutnya dapat dikembangkan sehingga aplikasi dapat mengirim dan menerima pesan dalam bentuk multimedia seperti pada gambar, suara, dan video Pada pengembangan selanjutnya aplikasi ini dapat dibuat dalam bentuk *mobile*.
b. Untuk pengembangan selanjutnya, percakapan bisa dilakukan tanpa harus melakukan input *IP* dan *port*, namun cukup memasukkan *username* dan *password*.
c. Pada pengembangan selanjutnya, percakapan dapat dilakukan secara kelompok.

5. DAFTAR PUSTAKA

[1] Amin, M. Miftakul. 2016, 'Implementasi Kriptografi Klasik Pada Komunikasi Berbasis Teks', *Jurnal Pseudocode*, vol III, No. 2, pp. 130-134.

[2] Efrandi, Asnawati dan Yupiyanti. 2014, 'Aplikasi Kriptografi Pesan Menggunakan Algoritma Vigenere Cipher', *Jurnal Media Infotama*, vol. 10, No. 2, pp. 121-122.

[3] Ahmad, Haidar. 2008, *TCP/IP Model dan OSI Model*. Diakses: 26 April 2017, diambil dari https://haidarahmad.wordpress.com/2008/02/28/tcpip-model-dan-osi-model/

[4] Gumelar, M. Ramdan dan Entik Insanudin.MT. 2016, 'Implementasi Kriptografi Metode Vigenere Chiper Pada Chatting Berbasis Web', *Jurnal Vigenere Cipher Chatting*, vol. 1, No. 20, pp. 2-3.

[5] Hasugian, Abdul Halim. 2013, 'Implementasi Algoritma Hill Cipher Dalam Penyandian Data', *Jurnal Pelita Informatika Budi Darma*, vol IV, No. 2, pp. 116-117.

[6] Yulianingsih, Pricilia, Hamdani dan Septya Maharani. 2014, 'Aplikasi Chatting Rahasia Menggunakan Algoritma Vigenere Cipher', *Jurnal Informatika Universitas Mulawarman*, vol. 9, No. 1, pp. 19-22