Penerapan Kombinasi Metode Enkripsi Vigenere Chiper Dan Transposisi Pada Aplikasai Client Server Chatting

Gede Angga Pradipta
STMIK STIKOM Bali
Jl. Raya Puputan No. 86 Renon, Denpasar-Bali
e-mail: angga_pradipta@stikom-bali.ac.id

Abstrak

Masalah keamanan pada komputer menjadi isu penting pada era teknologi informasi ini. Banyak kejahatan cyber yang terjadi salah satunya yang terkait dengan manipulasi data pada jaringan. Masalah terpenting dalam jaringan komputer adalah masalah keamanan data yang dikirimkan.Vigenere cipher merupakan salah satu jenis algoritma klasik yang populer dan sering digunakan sebagai metode penyembunyian pesan (kriptografi). Vigenere cipher ini menggunakan teknik substitusi dalam pengenkripsian pesannya dimana setiap karakter plainteks pada pesan akan dienkripsi mejadi karakter lain pada cipherteks berdasarkan kunci yang digunakan. Selanjutnya adalah metode penyandian transposisi adalah metode penyandian dengan cara mengubah letak dari teks pesan yang akan disandikan. Dan untuk membaca pesan aslinya kembali, cukup dengan mengembalikan letak dari pesan tersebut berdasarkan kunci dan algoritma pergeseran huruf yang telah disepakati. Pada penelitian ini dilakukan pengamanan data yang dikirimkan melalui jaringan ke server yang rentan untuk di serang hacker. Metode enkripsi yang diterapkan adalah vigenere chipper yang dikombinasikan dengan metode transposisi untuk mendapatkan data yang sudah diacak atau disebut dengan chipper text yang menghasilkan pengacakan data yang lebih kompleks dan sulit untuk di pecahkan pada saat pesan chatting memasuki server .

Kata kunci: *vigenere, transposisi, chipper text, plaintext.*

Abstract

Security becoming an important issue in information technology. Many cyber crimes that occurred aims to manipulated data on the network. Vigenere cipher is one of the classic algorithms that are popular and used as a method of hiding messages (cryptography). Vigenere cipher used encryption techniques message substitution, where each plaintext character in messages will be encrypted based on the key used. After that, the transposition changing the posisition of the text messages and to read back the original message, simply by returning the location of the message based on the key and algorithm shifts the letters that have been agreed. In this research, the security of data transmitted over the network to the server vulnerable to hackers attacked. Encryption method that is applied is vigenere chipper combined with transposition method to get the data that has been encrypted or called chipper text. Implementation of this method is applied to a chat client server applications that perform scrambling data or text sent by one user to another through a server. The result is chiper text that transmitted over server is more secure and difficult to decrypted because of this two combination method.

Keywords*: vigenere, transposisi, chipper text, plaintext.*

1. Pendahuluan

Keamanan jaringan saat ini menjadi isu yang sangat penting dan terus berkembang. Perkembangan teknologi komputer, selain menimbulkan banyak manfaat juga memiliki banyak sisi buruk. Salah satunya adalah serangan terhadap sistem komputer yang terhubung ke Internet [1]. Sebagai akibat dari serangan itu, banyak sistem komputer atau jaringan yang terganggu bahkan menjadi rusak. Untuk menanggulangi hal tersebut, diperlukan sistem keamanan yang dapat menanggulangi dan mencegah kegiatan-kegiatan yang mungkin menyerang sistem jaringan kita. Perkembangan dunia digital saat ini lalu lintas pengiriman data elektronik semakin ramai dan sensitive. Data yang dipertukarkan juga bervariasi dan dari jenis kerahasiaannya. Mulai dari data pribadi hingga data Negara yang sangat rahasia, hal ini yang menuntut adanya pengamanan data yang terkirim melalui lalu lintas jaringan computer. Telah banyak ditemukan

teknik-teknik pengamanan data , baik teknik klasik maupun teknik modern. Dalam dunia kriptografi, suatu algoritma dikatakan aman jika memecahkannya butuh waktu dan biaya yang cukup besar serta proses algoritma yang rumit. Salah satu algoritma klasik yang ada yaitu algoritma vigener cipher. Algoritma ini memiliki konsep yaitu suatu metode untuk enkripsi alphabet dari teks dengan menggunakan berbagai macam seri dari Caesar cipher berdasarkan huruf-hurif yang ada pada kunci [2]. Vigenere cipher ini menggunakan teknik subtitusi dalam enkripsi pesannya dimana setiap karakter palinteks pada pesan akan dienkripsi menjadi karakter lain pada cipherteks berdasarkan kunci yang digunakan. Perbedaaan antara Caesar chipher dan vigenere chipher adalah huruf yang sama pada plainteks tidak selalu dienkripsi menjadi huruf yang sama pada chiphertext. Hal ini terjadi karena pada vigenere cipher, pergeseran karakternya ditentukan oleh karakter yang ada pada kata kunci dan kata ini selalu diulang. Akibatnya karakter yang sama pada plaintext bisa saja memiliki karakter yang berbeda pada chipertextnya. Karena hal ini lah, vigenere cipher merupakan cipher subtitusi abjad-majemuk dengan tujuan utama dari metode ini adalah menyembunyikan keterhubungan antara plainteks dan cipherteks dengan menggunakan kata kunci sebagai penentu pergeseran karakternya.

Metode vigenre cipher telah dapat dilakukan kriptanalisis terhadap panjang kunci dengan metode kasiski. Kelamhan vigenere dipecahkan dengan memanfaatkan vigenere yang menggunakan kunci yang sama berulang-ulang sehingga menghasilkan potongan cipherteks yang sama untuk plainteks yang sama. Metode kasiski memanfaatkan keuntungan bahwa bahasa inggris tidak hanya mengandung perulangan huruf tetapi tripel huruf seperti TH,THE,dsb[3]. Perulangan kelompok huruf ini menghasilkan kriptogram yang berulang. Pada dasarnya, jika jarak antara dua buah string yang berulang di dalam plainteks merupakan kelipatan dari panjang kunci, maka string yang sama tersebut akan muncul menghasilkan kriptogram yang berulang. Maka dari itu pada penelitian ini dilakukan pengembangan algoritma vigenere dengan mengkombinasikannya dengan satu metode kriptografi klasik yaitu transposisi. Metode transposisi adalah teknik penyandian dengan cara mengubah letak dari teks pesan yang akan disandikan. Dan untuk membaca pesan aslinya kembali, cukup dengan mengembalikan letak dari pesan tersebut berdasarkan kunci dan algoritma pergeseran huruf yang telah disepakati. Kombinasi dari dua metode ini diharapkan dapat mempersulit kriptanalisis melakukan pemecahan kunci.

Sebuah aplikasi enkripsi data email dilakukan oleh rosyadi [4]. Algoritma yang digunakan adalah AES(Rjindael) 128 bit dengan 10 kali perputaran kunci. Aplikasi yang dibuat bertujuan untuk mengamankan data email walaupun email tersebut dapat dicuri tetapi sulit untuk dipecahkan karena telah diubah menjadi rangkaian data chipper text.

Penggabungan metode vigenere dengan mode operasi CBC (Cipher block chaining) dilakukan oleh kumalasari [7]. Penggabungan kedua metode ini menghasilkan metoode baru yang diberi nama vigener +. Metode ini menutupi kekurangan dari vigenere yaitu mempeluas jangkauan 26 huruf alfabeth menjadi 256 karakter ASCII.

Penerapan vigenere chipper biasanya dilakukan pada alafabet latin. Penelitian yang menerapkan vigenere pada aksara korea dilakukan oleh galman [8]. Pada penelitiannya menghasilkan 11268 kombinasi sehingga akan membuat bilangan mod yang sebelumnya berjumlah 26 menjadi 11268. Dengan demikikan walaupun masih dapat dipecahkan dengan metode kasiski namun dengan jumlah bilangan mod sebersar 11268 bukan perkara mudah dibandingkan dengan vigenere pada umumnya.

2. Metode Penelitian

2.1 Vigenere Cipher

Kode vigènere termasuk kode abjad-majemuk (polyalphabetic substitution cipher). Dipublikasikan oleh diplomat (sekaligus seorang kriptologis) Perancis, Blaise de Vigènere pada abad 16, tahun 1586. Sebenarnya Giovan Batista Belaso telah menggambarkannya untuk pertama kali pada tahun 1533 seperti ditulis di dalam buku La Cifra del Sig. Algoritma ini baru dikenal luas 200 tahun kemudian dan dinamakan kode vigènere. Vigènere merupakan pemicu perang sipil di Amerika dan kode vigènere digunakan oleh Tentara Konfederasi (Confederate Army) pada perang sipil Amerika (American Civil War). Kode vigènere berhasil dipecahkan oleh Babbage dan Kasiski pada pertengahan abad 19.[2]

Algoritma enkripsi jenis ini sangat dikenal karena mudah dipahami dan diimplementasikan. Teknik untuk menghasilkan ciphertext bisa dilakukan menggunakan substitusi angka maupun bujursangkar vigènere [4]. Teknik susbtitusi vigènere dengan menggunakan angka dilakukan dengan menukarkan huruf dengan angka, hampir sama dengan kode geser. Contoh

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

Gambar 1. Substitusi algoritma vigenere [4]

Sedangkan metode lain untuk melakukan proses enkripsi dengan metode vigènere cipher yaitu menggunakan tabula recta (disebut juga bujursangkar vigènere).

	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	Z
a	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	Z
b	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
c	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
d	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
e	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
f	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
g	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
h	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
i	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
j	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
k	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
l	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
m	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
n	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
o	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
p	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
r	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
s	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
t	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
u	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
v	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
w	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
x	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
z	Z	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

Gambar 2. Tabula recta algoritma vigenere [5]

Kolom paling kiri dari bujursangkar menyatakan huruf-huruf kunci, sedangkan baris paling atas menyatakan huruf-huruf *plaintext*. Setiap baris di dalam bujursangkar menyatakan huruf-huruf *ciphertert* yang diperoleh dengan *Caesar cipher*, yang mana jumlah pergeseran huruf *plaintext* ditentukan nilai numerik huruf kunci tersebut (yaitu, a=0, b=1, c=2, …, z=25). Bujursangkar *vigènere* digunakan untuk memperoleh *ciphertert* dengan menggunakan kunci yang sudah ditentukan. Jika panjang kunci lebih pendek daripada panjang *plaintext*, maka kunci diulang penggunaannya (sistem periodik). Bila panjang kunci adalah *m*, maka periodenya dikatakan *m*.

2.2 Metode Transposisi

Metode penyandian transposisi adalah metode penyandian dengan cara mengubah letak dari teks pesan yang akan disandikan. Dan untuk membaca pesan aslinya kembali, cukup dengan mengembalikan letak dari pesan tersebut berdasarkan kunci dan algoritma pergeseran huruf yang telah disepakati.[6]. Misalkan sebuah susunan karakter didefinisikan pada sebuah grup karakter yang panjangnya delapan, sebagai "mengumpulkan dan mengurutkan karakter bernomor prima dan diikuti sisanya". Maka hasil permutasinya (∏) ialah

$$\prod = c_2, c_3, c, c_7, c_1, c_4, c_6, c_8$$

Dengan cn adalah karakter ke-n dalam blok karakter. Misalkan plainteksnya adalah "TOLONG PERMUTASIKAN PESAN INI YA ", maka langkah pertama ialah mengelompokkan plainteks itu ke dalam blok-blok yang panjangnya delapan karakter, sebagai berikut (spasi diperhitungkan)

```
TOLONG P
ERMUTASI
KAN PESA
N INI YA
```

Langkah berikutnya, aturan permutasi yang telah ada (∏), diterapkan ke masing-masing blok pesan, menjadi OLN TOGP RMTSEUAI ANPSK EA IIYNN A. Terakhir, blok-blok pesan itu disatukan kembali menjadi cipherteks yang utuh: OLN TOGPRMTSEUAIANPSK EA IIYNN A Bila jumlah karakter dalam plainteks bukan kelipatan dari panjang ∏, maka pada akhir pesan dapat ditambahkan (padding) karakter-karakter dummy . Selain itu, terdapat alternatif lain dalam metode ini, diantaranya dengan membuang spasi.

Pada penelitian ini menerapkan pemrograman socket menggunkan UDP untuk keterhubungan antara beberapa aplikasi. Aplikasi yang menginisialisasi koneksi, disebut aplikasi client. Sedangkan aplikasi yang menerima inisialisasi disebut sebagai aplikasi server. Oleh karena itu, dibangun suatu aplikasi jaringan yang lengkap, maka kita harus membuat aplikasi client maupun aplikasi server. Secara umum aplikasi chatting yang dibuat memiliki tahap-tahap seperti dibawah ini :

1. Client membaca inputan dari keyboard, kemudian mengirimkan hasilnya ke server melalui socket-nya. Data yang dikirim melalui socket connection merupakan data yang telah di enkripsi.
2. Server membaca data yang dikirim oleh client di connection socket.
3. Server mengirimkan data yang telah diubah menuju client melalui socket-nya. Pihak client melakukan dekripsi data yang ada di server

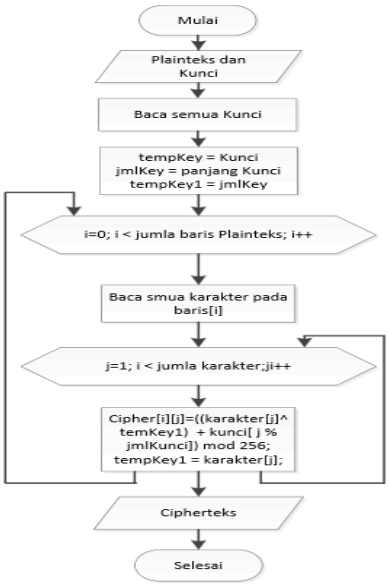
Untuk proses enkripsi data digunakan kombinasi antara metode vigenere dan transposisi. Pada metode vigenere data/ teks percakapan dari client yang dikirim melalui socket connection akan di enkrip menjadi chiper text sehingga data yang bersifat penting saat melati jaringan bukan lagi merupakan data mentah melainkan data yang telah diacak. Metode vigenere merupakan teknik untuk menghasilkan ciphertext yang dilakukan menggunakan substitusi angka maupun bujursangkar vigènere. Teknik susbtitusi vigènere dengan menggunakan angka dilakukan dengan menukarkan huruf dengan angka, hampir sama dengan kode geser. pada kriptografi Vigenere, plaintext akan dienkripsi dengan pergeseran huruf seperti pada kriptografi Caesar tetapi setiap huruf di dalam plaintext akan mengalami pergeseran yang berbeda. Kunci pada kriptografi Vigenere adalah sebuah kata bukan sebuah huruf. Kata kunci ini akan dibuat berulang sepanjang plaintext, sehingga jumlah huruf pada kunci akan sama dengan jumlah huruf pada plaintext. Pergeseran setiap huruf pada plaintext akan ditentukan oleh huruf pada kunci yang mempunyai posisi yang sama dengan huruf pada plaintext. fungsi enkripsi dan dekripsi adalah

$$ci = E(pi) = (pi + k) \bmod 26)$$
$$pi = D(ci) = (ci – k) \bmod 26)$$

$C = (P + K) \bmod n$ C = ciphertext K = kunci P = plaintext n = jumlah karakter

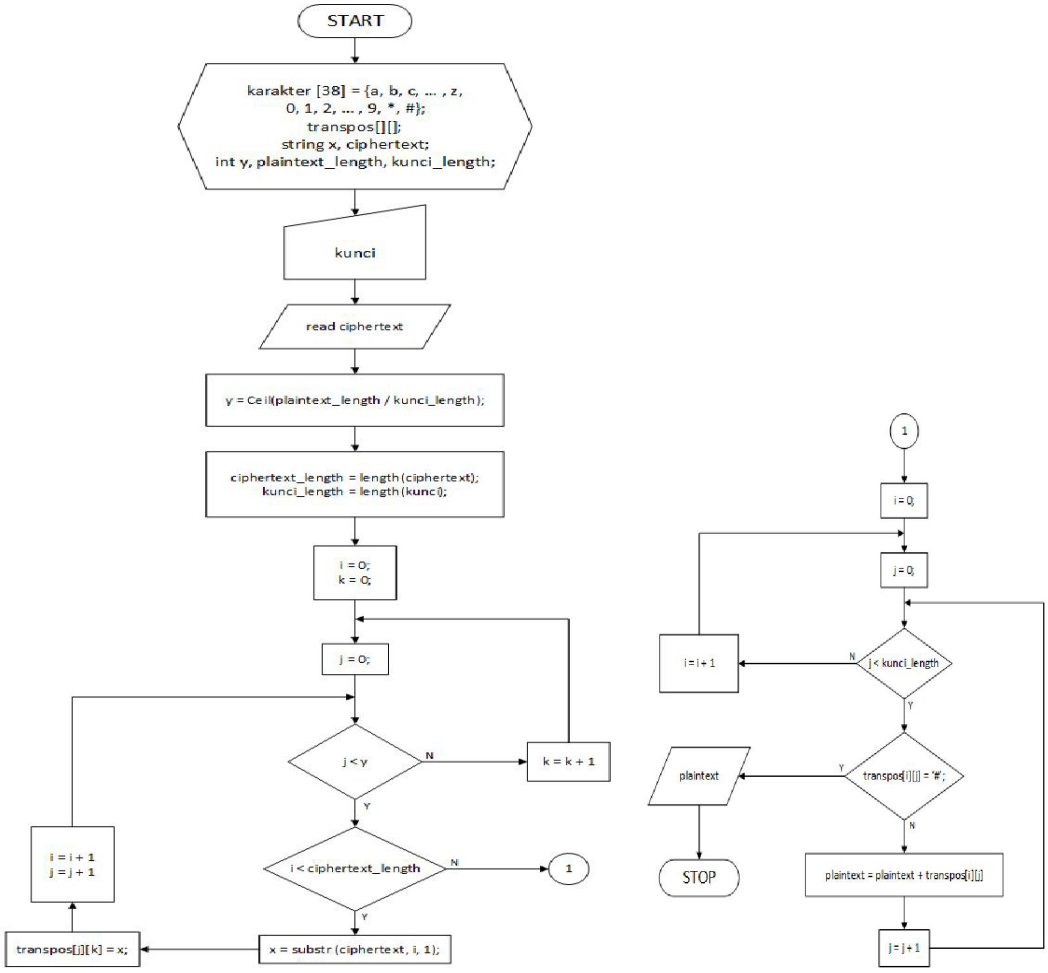
$P = (C - K) \bmod n$

Tahap-tahap enkripsi menggunakan metode vigenere chiper jika digambarkan menjadi sebuah flow chart ditunjukkan pada gambar berikut.



Gambar 3. Flowchart proses enkripsi dengan metode vigenere.

Tahap berikutnya adalah saat data sudah melalui proses enkripsi vigenere maka dilanjutkan dengan melakukan enkripsi sekali lagi menggunakan metode transposisi. Metode Transposisi adalah metode yang enkripsi dengan menyusun plain text pada matrix secara baris, lalu dari hasil susunan tersebut menghasilkan sebuah cipher text dengan mengambil rangkaian karakter secara kolom. Metode Transposisi juga disebut metode Permutasi. Flowchart langkah-langkah dari metode transposisi dapat dilihat pada gambar dibawah ini.



Gambar 4. Flowchart proses enkripsi dengan metode transposisi.

3. Hasil dan Pembahasan

3.1. Aplikasi Chatting

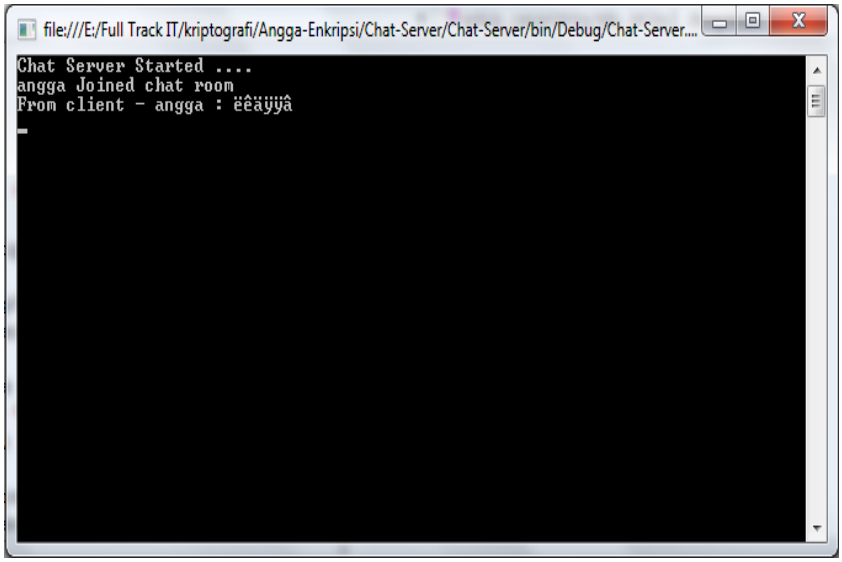
Desain antarmuka aplikasi chating ini dirancang untuk memudahkan user dalam berkomunikasi dalam bentuk percakapan. Data dalam percakapan inilah yang akan di enkripsi saat melewati server untuk lebih meningkatkan keamanan data mereka. Aplikasi terdiri dari 2 bagian yaitu :

1. Server
2. Interface aplikasi chatting

3.2.1 Server chatting

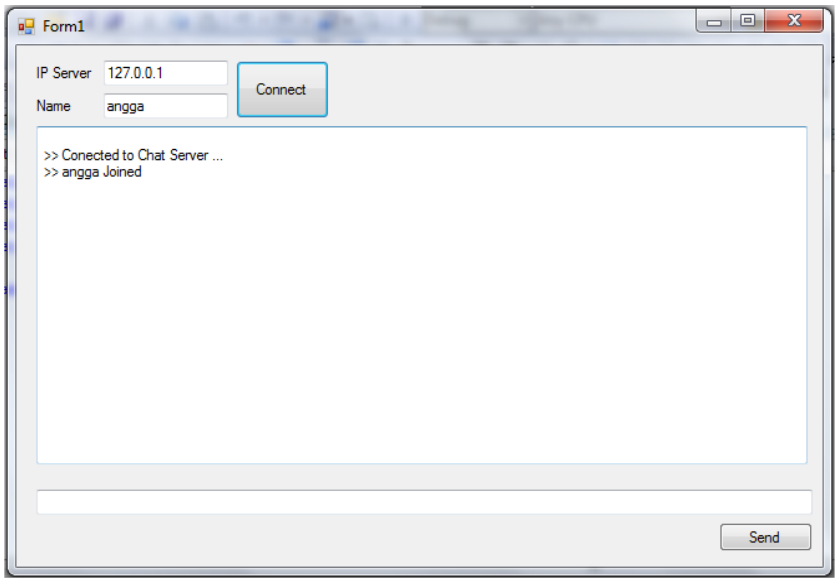
Ketika seorang user (client) melakukan koneksi ke chat server, program akan membuka koneksi ke port yang diberikan, sehingga server perlu membuka socket pada port tersebut dan "mendengarkan" koneksi yang datang. Socket sendiri merupakan gabungan antara host-adress dan port adress. Dalam hal ini socket digunakan untuk komunikasi antara client dan server. Pada saat socket client, informasi alamat socket server dilewatkan sebagai argumen dan socket client akan otomatis mencoba meminta koneksi ke socket server. Pada saat permintaan koneksi client sampai pada server, maka server akan membuat suatu socket biasa. Socket ini yang nantinya akan berkomunikasi dengan socket pada sisi client. Setelah itu socket server dapat kembali melakukan listen untuk menunggu permintaan koneksi dari client lainnya seperti yang ditunjukkan pada gambar 3.3. Langkah ini umumnya hanya dilakukan jika aplikasi server mengimplementasikan multithreading. Langkah – langkah dasar di server :

a. Membuat socket dengan perintah *socket*()
b. Mengikatkan socket kepada sebuah alamat network dengan perintah *bind*()
   Menyiapkan socket untuk menerima koneksi yang masuk dengan perintah *listen*()
b Menerima koneksi yang masuk ke server dengan perintah *accept*()
e. Melakukan komunikasi (mengirim dan menerima data), dengan menggunakan perintah *write*() dan *read*() .



Gambar 5. Tampilan chat server

3.2.2 Aplikasi chat user



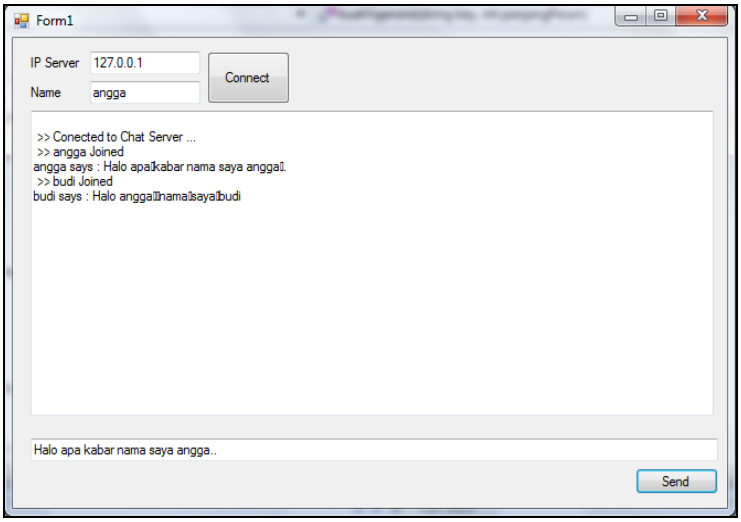
Gambar 6. Tampilan aplikasi chat

Interfaces diatas menggunakan IP server 127.0.0.1 dan port 8888 untuk dapat membangun sebuah socket untuk berkomunikasi ke server. Langkah-langkah pada program client adalah :

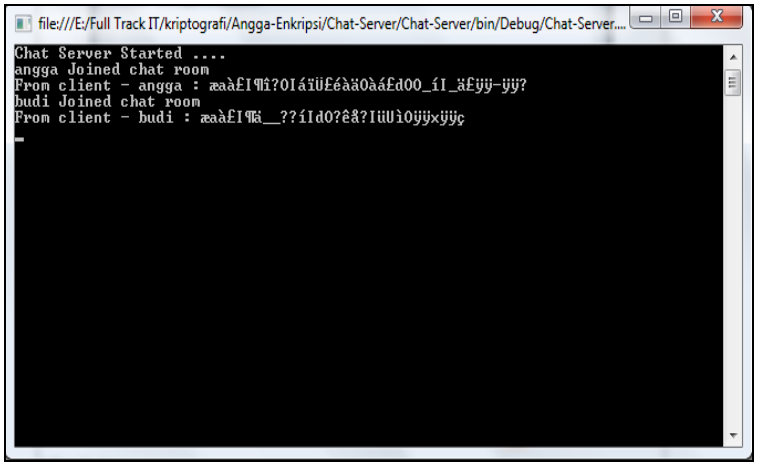
a. Membuat socket dengan perintah *socket*().
b. Mengikat socket pada sebuah alamat jaringan dengan perintah *bind ()*.
c. Menyiapkan socket untuk menerima koneksi yang masuk dengan perintah *listen()*.
d. Menerima koneksi yang masuk ke server dengan perintah *accept()*.
e. Melakukan komunikasi (Mengirim dan menerima data) dengan menggunakan perintah *write()* dan *read()*.

3.3 Enkripsi pesan pada aplikasi

Setiap pesan yang dikirimkan oleh user pada saat memasuki server maka dilakukan enkripsi pada pesan tersebut. Jalur komunikasi socket pada aplikasi ini telah ditambahkan metode enkripsi yaitu kombinasi antara vigenere dan transposisi. Gambar 3.5 dan 3.6 menunjukkan tampilan pertukaran pesan pada sisi user dan pada sisi server.



Gambar 7. Tampilan user saat bertukar pesan



Gambar 8. Enkripsi pesan di server

Enkripsi merupakan proses mengubah pesan asli menjadi pesan sandi. Berikut ini potongan program enkripsi dengan metode vigenere cipher.

```
string hasil = "";

        //BUAT KEY DALAM ARRAY

        string[] keyArray = new
string[key.Length];
        for (int i = 0; i < key.Length; i++)
        {
           keyArray[i] = key.Substring(i, 1);
        }

        //JIKA PANJANG KEY LEBIH BESAR
DARI PESAN
        if (panjangPesan < key.Length)
        {
           for (int i = 0; i < panjangPesan; i++)
           {
              hasil += keyArray[i];
           }
        }

        //JIKA PANJANG KEY LEBIH KECIL
DARI PESAN
        if (panjangPesan > key.Length)
        {
           int counter = 0;
           for (int i = 0; i < panjangPesan; i++)
           {
              if (i % key.Length == 0)
              {
                 counter = 0;
              }
              else
              {
                 counter++;
              }
              hasil += keyArray[counter];
           }
        }
        return hasil;
```

kemudian cipher text yang dihasilkan dari metode vigenere, kembali dilakukan pengenkripsian dengan metode transposisi dengan potongan program seperti dibawah ini.

```
string transposisi = "", tampung = "";
        int pKey3 = key3.Length, pTeks =
teks.Length;
        int[] aturanTransposisi = new
int[pKey3];
        int j = 0, index = 0;

        //buat array pemetaan transposisi
        for (int i = 0; i < key3.Length; i++)
        {
           aturanTransposisi[i] =
Convert.ToInt32(key3.Substring(i, 1));
        }

        //buat tambahan/padding karakter
        if (pTeks % pKey3 != 0)
        {
           int pPadding = ((pTeks / pKey3) + 1)
* pKey3;//mencari padding agar menjadi
kelipatan panjang key 3
           tampung = teks.PadRight(pPadding,
(char)255);//menambah karakter agar menjadi
kelipatan panjang key 3
        }
        else
        {
           tampung = teks;
        }

        //proses transposisi
        for (int i = 0; i < tampung.Length; i++)
        {
           if (i % pKey3 == 0)
           {
              j = 0;
              index++;//untuk kendali blok blok
yg masing2 sepanjang key3
           }
           transposisi = transposisi +
tampung.Substring((aturanTransposisi[j] - 1) +
((index - 1) * pKey3), 1);//
           j++;
        }
        return transposisi;
```

untuk setiap program chat, juga diberikan perintah untuk melakukan dekripsi pesan saat server mengirmkan balik pesan melalui jalur socket yang dibuat. Dibawah ini merupakan potongan program untuk melakukan proses dekripsi pada kombinasi kedua metode tersebut

```
string hasil = "";
            char temp,
tempVigenere;
            int decTemp,
decTempVigenere;
            teks =
buatTransposisiBack(key3,
teks);//mengembalikan transposis
sebelum dikenai vigenere dan
cesar
            string vigenere =
buatVigenere(key2, teks.Length);
            for (int i = 0; i <
teks.Length; i++)
            {
                tempVigenere =
Convert.ToChar(vigenere.Substrin
g(i, 1));
                decTempVigenere
= (int)tempVigenere;
                temp =
Convert.ToChar(teks.Substring(i,
1));
                decTemp =
(int)temp - key1 -
decTempVigenere;
                hasil +=
(char)decTemp;
            }
            return hasil;

string transposisi = "";
            int pKey3 =
key3.Length, pTeks =
teks.Length;
            string[ ]
transposisiBack = new
string[ pTeks] ;
            int[ ]
aturanTransposisi = new
int[ pKey3] ;
            int j = 0, index =
0;

            //buat array
pemetaan transposisi
            for (int i = 0; i <
key3.Length; i++)
            {

aturanTransposisi[ i] =
Convert.ToInt32(key3.Substring(i
, 1));
            }

            //proses transposisi
back dalam bentuk array
```

```
            for (int i = 0; i <
pTeks; i++)
            {
                if (i % pKey3 ==
0)
                {
                    j = 0;
                    index++;
                }

transposisiBack[ (aturanTransposi
si[ j] - 1) + ((index - 1) *
pKey3)] = teks.Substring(i,
1);//mengisi array tranposisi
back dengan teksnya.
                j++;
            }
```

```
            //proses pengabungan
array transposisi back ke string
biasa
            for (int i = 0; i <
pTeks; i++)
            {
                transposisi =
transposisi +
transposisiBack[ i];
            }

            string charnya =
((char)255).ToString();
            return
transposisi.Replace(charnya,
"");//menghilangkan padding
```

4. Simpulan

Setelah melalui tahap demi tahap perancangan dan penerapan program enkripsi data dengan kombinasi metode vigenere dan transposisi pada aplikasi chatting, maka dihasilkan kesimpulan yaitu :

1. Implementasi program enkripsi data dengan metode vigenere dan transposisi dapat menigkatkan keamanan pengiriman pesan ke server.
2. Kombinasi dengan metode transposisi membuat metode vigenere menjadi lebih sulit untuk di pecahkan karena cipher text yang dihasilkan di awal akan dilakukan pengenkripsian kembali dengan merubah letak posisi karakter menggunakan cara transposisi.

Daftar Pustaka

[1] Sadikin, Rifki. 2012. Kriptografi untuk Keamanan Jaringan dan Implementasinya dalam Bahasa Java. Penerbit Andi, Yogyakarta.

[2] Ariyus, Dony., 2008, Pengantar Ilmu Kriptografi: Teori, Analisis, dan Implementasi. Penerbit Andi, Yogyakarta.

[3] Munir, Rinaldi., 2006, Kriptografi. Penerbit Informatika, Bandung..

[4] Ahmad Rosyadi, Jurusan Teknik Elektro, Universitas Diponegoro Semarang, "IMPLEMENTASI ALGORITMA KRIPTOGRAFI AES UNTUK ENKRIPSI DAN DEKRIPSI EMAIL", TRANSIENT, VOL. 1, NO. 3, SEPTEMBER 2012, ISSN: 2302-9927, 64

[5] Sukrisno, Ema Utami, Jurusan Teknik Informatika STMIK AMIKOM Yogyakarta," IMPLEMENTASI STEGANOGRAFI TEKNIK EOF DENGAN GABUNGAN ENKRIPSI RIJNDAEL, SHIFT CIPHER DAN FUNGSI HASH MD5", Seminar Nasional Teknologi 2007 (SNT 2007) ISSN : 1978 – 9777, Yogyakarta, 24 November 2007.

[6] Putu H. Arjana, Tri Puji Rahayu,Yakub, Hariyanto., "IMPLEMENTASI ENKRIPSI DATA DENGAN ALGORITMA VIGENERE CHIPER". Seminar Nasional Teknologi Informasi dan Komunikasi 2012 (SENTIKA 2012) ISSN: 2089-9815 Yogyakarta, 10 Maret 2012.

[7] Erna Kumalasari Nurnawati, Seminar, ANALISIS KRIPTOGRAFI MENGGUNAKAN ALGORITMA VIGENERE CIPHERDENGAN MODE OPERASI CIPHER BLOCK CHAINING(CBC), Nasional Aplikasi Sains dan Teknologi 2008 – IST AKPRIND Yogyakarta,

[8] Ignatius Ronaldo Galman Kurniawan, VIGENERE CIPHER UNTUK AKSARA KOREA (HANGUL), Makalah IF3058 Kriptografi Sem I Tahun 2011/2012