Journal of Computer System and Informatics (JoSYC)
Volume 1, No. 1, November 2019, Page 9 - 14
ISSN 9999-9999 (media online)

Perancangan Aplikasi Messanger Dengan Menerapkan Caesar Shift Berbasis Secret Sharing

Bayu Syahputra

Prodi Teknik Informatika STMIK Budi Darma, Medan, Indonesia
Jalan Sisingamangaraja No. 338, Medan, Indonesia
Email: sahputra19@gmail.com

Abstrak−Dampak yang ditimbulkan dari chatting mungkin tidak disadari sama sekali. Selain memudahkan dalam berkomunikasi sebagai dampak positif yang manusia dapatkan, terdapat pula dampak negatif yang manusia dapatkan sebagai akibat menggunakan chatting ini. Kerahasiaan dan keamanan saat melakukan pertukaran data adalah hal yang sangat penting dalam komunikasi data, baik untuk tujuan keamanan bersama, maupun untuk privasi individu. kemajuan komunikasi tersebut maka banyak orang yang ingin menyadap komunikasi antara satu dengan orang lain yang menyebabkan banyak informasi atau percakapan disadap tanpa sepengetahuan pemilik informasi tersebut. Ada beberapa cara melakukan pengamanan data yang melalui suatu saluran data internet, salah satu diantaranya adalah kriptografi. Data yang sangat rahasia akan disamarkan sedemikian rupa sehingga kalaupun data itu bisa dibaca maka tidak dapat dimengerti oleh pihak yang tidak berhak. Data yang akan dikirimkan dan belum mengalami penyandian, maka plaintext ini akan berubah menjadi ciphertext. Salah satunya algoritma yang dapat mengamankan data penulis bahas adalah Algoritma Caesar Shift.

Kata Kunci: Enkripsi, Dekripsi, Caesar Shift

Abstract−The impact of chatting may not be realized at all. In addition to facilitating communication as a positive impact that humans get, there are also negative impacts that humans get as a result of using this chat. Confidentiality and security when exchanging data is very important in data communication, both for shared security purposes, and for individual privacy. the progress of the communication so many people who want to tap communication between one person and another that causes a lot of information or conversation is tapped without the knowledge of the owner of the information. There are several ways to secure data through an internet data channel, one of which is cryptography. Highly confidential data will be disguised in such a way that even if the data can be read it cannot be understood by unauthorized parties. Data to be sent and not yet encoded, then this plaintext will change to ciphertext. One of the algorithms that can secure the data discussed by the author is the Caesar Shift Algorithm.

Keywords: Encryption, Decryption, Caesar Shift

1. PENDAHULUAN

Pada chatting banyak macam pembincangan atau komunikasi melalui jaringan, namun umumnya yang dimaksud adalah obrolan antara seseorang dengan orang lain atau kelompok menggunakan perangkat lunak seperti aplikasi Instant Messanging (IM), Inter Relay Chat (IRC), Aplikasi Chatting merupakan salah satu dari perkembangan teknologi. Dengan kecanggihan teknologi saat ini, fungsi aplikasi chatting tidak hanya sebagai alat komunikasi biasa, tetapi manusia juga sangat mengirimkan foto dan lain-lainnya.

Dampak yang ditimbulkan dari chatting mungkin tidak disadari sama sekali. Selain memudahkan dalam berkomunikasi sebagai dampak positif yang manusia dapatkan, terdapat pula dampak negatif yang manusia dapatkan sebagai akibat menggunakan chatting ini. Kerahasiaan dan keamanan saat melakukan pertukaran data adalah hal yang sangat penting dalam komunikasi data, baik untuk tujuan keamanan bersama, maupun untuk privasi individu. Mereka yang menginginkan agar datanya tidak diketahui oleh pihak-pihak yang tidak berkepentingan selalu menyiasati cara mengamankan informasi yang akan dikomunikasikannya. Perlindungan terhadap kerahasiaan datapun meningkat, salah satu caranya dengan menyandikan data atau enkripsi.

Dengan kemajuan komunikasi tersebut maka banyak orang yang ingin menyadap komunikasi antara satu dengan orang lain yang menyebabkan banyak informasi atau percakapan disadap tanpa sepengetahuan pemilik informasi tersebut. Ada beberapa cara melakukan pengamanan data yang melalui suatu saluran data internet, salah satu diantaranya adalah kriptografi. Dalam kriptografi, data yang sangat rahasia akan disamarkan sedemikian rupa sehingga kalaupun data itu bisa dibaca maka tidak dapat dimengerti oleh pihak yang tidak berhak. Data yang akan dikirimkan dan belum mengalami penyandian, maka plaintext ini akan berubah menjadi ciphertext. Salah satunya algoritma yang dapat mengamankan data penulis bahas adalah Algoritma Caesar Shift.

2. METODE PENELITIAN

2.1 Kriptografi

Kriptografi berasal dari bahasa Yunani. Menurut bahasa tersebut kata “Kriptografi” dibagi menjadi dua, yaitu kripto dan graphia. Kripto berarti *secret* (rahasia) dan Graphia berarti *writing* (tulisan). Menurut terminologinya, kriptografi adalah ilmu dan seni untuk menjaga keamanan pesan ketika pesan dikirim dari suatu tempat ke tempat yang lain Kriptografi merupakan seni dan ilmu untuk menjaga keamanan data dengan metode tertentu, dan pelakunya disebut *cryptographer*. Kriptografi disebut sebagai ilmu karena didalamnya terdapat metode (rumusan) yang digunakan, dan dikatakan sebagai seni karena karena dalam membuat suatu teknik kriptografi itu sendiri

merupakan ciri tersendiri dari sipembuat dan memerlukan teknik khusus dalam mendisainnya. Sedangkan *cryptanalysis* adalah suatu ilmu dan seni memecahkan ciphertext menjadi plaintext tanpa melalui cara yang seharusnya dan orang yang melakukannya disebut *cryptanalyst* [1].

2.2 Metode Caesar Shift

Caesar Shift atau sering di sebut dengan Caesar Cipher mungkin adalah contoh terbaik dari cipher alphabet-majemuk manual. Algoritma ini dipublikasikan oleh diplomat (sekaligus seorang kriptologis) perancis, meskipun Giovan Batista Belaso telah menggambarkannya pertama kali pada tahun 1553 sepeti ditulis di dalam bukunya La Cifra del Sig. Caesar Shift dipublikasikan pada tahun 1586, tetapi algoritma tersebut baru dikenal luas 200 tahun kemudian yang oleh penemunya cipher tersebut dinamakan Caesar Shift. Cipher ini berhasil dipecahkan oleh Babbage dan Kasiski pada pertengahan abad 19. Caesar Shift digunakan oleh tentara Konfiderasi (Confederate Army) pada perang sipil Amerika (American Civil war) [4].

Caesar Shift sangat dikenal karena mudah dipahami dan diimplem entasikan. Cipher menggunakan bujursangakar Vigenere untuk melakukan enkripsi seperti ditunjukkan pada (Tabel 2.1). Kolom paling kiri dari bujursangkar menyatakan huruf-hurf kunci, sedangkan baris paling atas menyatakan huruf-huruf plainteks. Setiap baris dalam bujursangkar menyatakan huruf-huruf cipherteks yang diperoleh dengan Caesar cipher, yang mana jumlah pergesaran huruf plainteks ditentukan nilai numerik huruf kunci tersebut (yaitu, A = 0, B = 1, C = 2,…, Z = 25).

Karena hanya ada 26 huruf abjad, maka pergeseran huruf yang mungkun dilakukan adalah dari 0 sampai 25. Secara umum, untuk pergeseran huruf sejauh k (dalam hal ini k adalah kunci enkripsi dan dekripsi). Rumus Kriptografi Menurut Caesar, secara umum dituliskan sebagai berikut :

$$Ci=E(Pi) = (Pi+k) \bmod 26 \quad (1)$$
$$Pi=D(Ci) = (Ci-k) \bmod 26 \quad (2)$$

Keterangan :
Pi : Plaintext
Ci : Ciphertext
E : Proses Enkripsi
D : Proses Dekripsi
k : pergeseran huruf sesuai dengan kunci yang dikehendaki.

2.3 Internet

Internet adalah jaringan antar komputer yang saling dihubungkan. Media penghubung tersebut bisa melalui kabel, kanal satelit maupun frekwensi radio, sehingga komputer-komputer yang terhubung tersebut dapat saling berkomunikasi. Setiap komputer yang terhubung dengan jaringan tersebut, diberikan sebuah nomor yang unik, dan berkomunikasi satu sama lainnya dengan bahasa kompunikasi yang sama. Bahasa komunikasi yang sama ini disebut protokol. Protokol yang digunakan di internet adalah TCP/ IP (Transmission Control Protocol/ Internet Protocol).

3. ANALISA DAN PEMBAHASAN

Pada bagian ini, akan dijelaskan tentang fasilitas yang disediakan oleh perangkat lunak ini. Selain itu juga akan dijelaskan bagaimana cara kerja proses enkripsi transposisi dalam program yang disediakan pada perangkat lunak ini. Enkripsi digunakan untuk menyandikan data-data atau informasi sehingga tidak dapat dibaca oleh orang yang tidak berhak. Dengan enkripsi, data kita disandikan (encrypted) dengan mengunakan sebuah kunci (key). Untuk membuka (men-decrypt) data tersebut, juga digunakan kunci yang dapat sama dengan kunci untuk mengenkripsi (privat key).

Keamanan dari enkripsi bergantung pada beberapa factor. Pertama, algoritma enkripsi harus cukup kuat sehingga sulit untuk men-decrypt ciphertext dengan dasar ciphertext tersebut. Lebih jauh lagi, keamanan dari algoritma enkripsi bergantung pada kerahasiaan dari kuncinya bukan algoritmanya, yaitu dengan asumsi bahwa adalah sangat tidak praktis untuk men-deycrypt informasi dengan dasar chipper text dan pengetahuan tentang algoritma dekripsi atau enkripsi. Atau dengan kata lain, kita tidak perlu menjaga kerahasiaan dari algoritma tetapi cukup dengan kerahasiaan kuncinya. Dan dekripsi digunakan untuk mengembalikan data-data atau informasi sehingga dapat dibaca oleh orang yang berhak.

3.1 Proses Enkripsi Menggunakan Rumus Kriptografi

Proses pencarian *Ciphertext* pada enkripsi tidak hanya menggunakan bujursangkar. Dapat juga menggunakan rumus sebagai berukut :

$$Ci = E (Pi) = (Pi+k) \bmod 26$$

Contoh :
Diketahui :

Journal of Computer System and Informatics (JoSYC)
Volume 1, No. 1, November 2019, Page 9 - 14
ISSN 9999-9999 (media online)

Kunci = BAYU
Plaintext = SYAHPUTRABD

a. Ci = E (Pi) = (Pi+k) mod 26
= (S+B) mod 26
= (83+66) mod 26
= 84 = T

b. Ci = E (Pi) = (Pi+k) mod 26
= (Y+A) mod 26
= (89+65) mod 26
= 89 = Y

c. Ci = E (Pi) = (Pi+k) mod 26
= (A+Y) mod 26
= (65+89) mod 26
= 89 = Y

d. Ci = E (Pi) = (Pi+k) mod 26
= (H+U) mod 26
= (72+85) mod 26
= 66 = B

e. Ci = E (Pi) = (Pi+k) mod 26
= (P+B) mod 26
= (80+66) mod 26
= 81 = Q

f. Ci = E (Pi) = (Pi+k) mod 26
= (U+A) mod 26
= (85+65) mod 26
= 85 = U

g. Ci = E (Pi) = (Pi+k) mod 26
= (T+Y) mod 26
= (84+89) mod 26
= 82 = R

h. Ci = E (Pi) = (Pi+k) mod 26
= (R+U) mod 26
= (82+85) mod 26
= 76 = L

i. Ci = E (Pi) = (Pi+k) mod 26
= (A+B) mod 26
= (65+66) mod 26
= 66 = B

j. Ci = E (Pi) = (Pi+k) mod 26
= (B+A) mod 26
= (66+65) mod 26
= 66 = B

k. Ci = E (Pi) = (Pi+k) mod 26
= (D+Y) mod 26
= (68+89) mod 26
= 66 = B

Maka hasil Ciphertext : TYYBQURLBBB

3.2 Proses Dekripsi Menggunakan Rumus Kriptografi

Proses pencarian *Plaintext* pada dekripsi tidak hanya menggunakan bujursangkar. Dapat juga menggunakan rumus sebagai berukut :

$$Pi = D(Ci) = (Ci-k) \bmod 26$$

Contoh :
Diketahui :
Kunci = BAYU
Ciphertext = TYYBQURLBBB

a. Pi = D (Ci) = (Ci-k) mod 26
= (T-B) mod 26
= (84-66) mod 26
= 83 = S

b. Pi = D (Ci) = (Ci-k) mod 26
= (Y-A) mod 26

= (89-65) mod 26
= 89 = Y

c. Pi = D (Ci) = (Ci-k) mod 26
= (Y-Y) mod 26
= (89-89) mod 26
= 65 = A

d. Pi = D (Ci) = (Ci-k) mod 26
= (B-U) mod 26
= (66-85) mod 26
= 72 = H

e. Pi = D (Ci) = (Ci-k) mod 26
= (Q-B) mod 26
= (81-66) mod 26
= 80 = P

f. Pi = D (Ci) = (Ci-k) mod 26
= (U-A) mod 26
= (85-65) mod 26
= 85 = U

g. Pi = D (Ci) = (Ci-k) mod 26
= (R-Y) mod 26
= (82-89) mod 26
= 84 = T

h. Pi = D (Ci) = (Ci-k) mod 26
= (L-U) mod 26
= (76-85) mod 26
= 82 = R

i. Pi = D (Ci) = (Ci-k) mod 26
= (B-B) mod 26
= (66-66) mod 26
= 65 = A

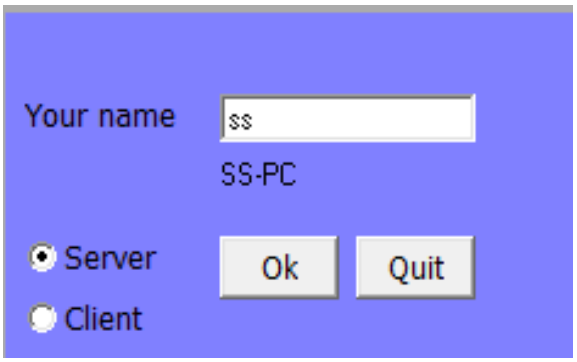
j. Pi = D (Ci) = (Ci-k) mod 26
= (B-A) mod 26
= (66-65) mod 26
= 66 = b

k. Pi = D (Ci) = (Ci-k) mod 26
= (B-Y) mod 26
= (66-89) mod 26
= 68 = D

Maka hasil Plaintext : SYAHPUTRABD

4. IMPLEMENTASI

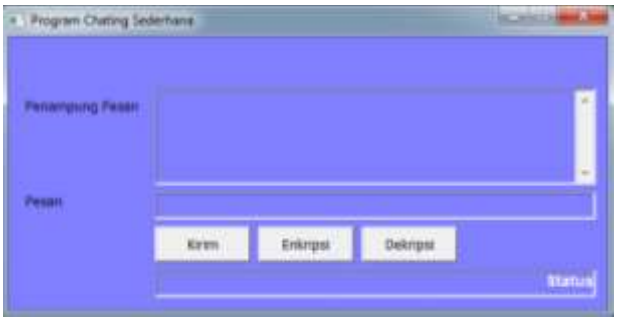
Implementasi dari perangkat lunak mencakup kebutuhan sistem, instalasi, tampilan *output* dari perangkat lunak dan hasil proses eksekusi dari perangkat lunak. Tampilan ini merupakan tampilan koneksi dari perangkat lunak yang berfungsi untuk menghubungkan client dan server. Tampilan form 'koneksi' dapat dilihat pada gambar berikut :



Gambar 1. Tampilan Form Main

Adapun form untuk penampung pesan enkripsi dan dekripsi dapat dilihat pada gambar dibawah ini

Journal of Computer System and Informatics (JoSYC)
Volume 1, No. 1, November 2019, Page 9 - 14
ISSN 9999-9999 (media online)



Gambar 2. Tampilan Penampung Pesan

Tampilan ini berfungsi untuk melakukan proses enkripsi pesan. Tampilan form 'enkripsi' dapat dilihat pada gambar berikut :

Gambar 3. Tampilan Form Enkripsi

Tampilan ini berfungsi untuk menampilkan proses dekripsi pesan. Tampilan form 'Dekripsi" dapat dilihat pada gambar berikut:

Gambar 4. Tampilan Form Dekripsi

5. KESIMPULAN

Setelah menyelesaikan penelitian ini, penulis menarik beberapa kesimpulan, sebagai berikut:

1. Aplikasi ini berhasil mengamankan pesan pengguna pada saat pesan sebelum dikirim ke server.
2. Panjang karakter pesan yang disimpan sebanyak delapan karakter sebagai pesan aslinya.
3. Jumlah block hasil cipherteks berbanding lurus dengan jumlah blok plainteks. Semakin banyak pesan yang dikirim semakin banyak pula jumlah cipherteksnya.

REFERENCES

[1] Ariyus, Dony, "Kriptografi keamanan data dan komuniksi", Penerbit Graha Ilmu, Yogyakarta, 2006.
[2] Ariyus, Dony, "Pengantar Ilmu Kriptografi", Andi offset, Yogyakarta, 2008.
[3] Munir, Rinaldy, "Kriptografi", Institut Teknologi bandung, 2006.
[4] Gunawan Pandia, 2008, "Keamanan data dengan Kriptografi"www.tonews.com/makalah/kriptografi.pdf, Tgl 14-03-2012
[5] www.tonews.com/makalah/kriptografi.pdf, Tgl 14-03-2012
[6] http://thesis.binus.ac.id/pdf/internet.pdf, Tgl 14-03-2012

[7] http://iptkj.web.id/Thread-PENGERTIAN-PHP-dan-MYSQL, Tgl 17-07-2012
[8] http://www.articlecenter.org/pengertian-mysql-my-structure-query-language, Tgl 17-07-2012
[9] http://www.w3function.com/blog/?p=det&idn=23, Tgl 17-07-2012
[10] http://cois.is.uad.ac.id/forum/showthread.php?tid=35, Tgl 17-07-2012