IMPLEMENTASI KRIPTOGRAFI KLASIK PADA KOMUNIKASI BERBASIS TEKS

M. Miftakul Amin[1]

[1] Jurusan Teknik Komputer, Politeknik Negeri Sriwijaya Palembang
Jalan Srijaya Negara, Bukit Besar, Palembang 30139
Telp. 0711 – 353414 Fax. 0711 – 355918
website : http://polsri.ac.id

[1] miftakul_a@polsri.ac.id

Abstrak: Kemajuan di bidang komunikasi data dan jaringan komputer telah memungkinkan ribuan orang untuk melakukan komunikasi dengan beragam teknologi perangkat keras dan perangkat lunak. Di sisi lain terdapat ancaman yang membayangi kemajuan tersebut, yaitu aspek keamanan data dan informasi. Sistem keamanan data diperlukan untuk melindungi data dan informasi yang ditransmisikan melalui jaringan komunikasi. Salah satu mekanisme untuk menyediakan layanan keamanan data adalah teknik kriptografi. Dalam kriptografi, data yang dikirimkan melalui jaringan akan disamarkan sedemikian rupa dengan teknik enkripsi sehingga kalaupun data itu bisa dibaca maka tidak bisa dimengerti oleh pihak yang tidak berhak. Data yang akan dikirimkan dan belum mengalami penyandian dikenal dengan istilah *plaintext*, dan setelah disamarkan dengan suatu cara penyandian, maka *plaintext* ini akan berubah menjadi *ciphertext*. Sebelum adanya komputer, kriptografi dilakukan dengan algoritma berbasis karakter. Terdapat sejumlah algoritma yang tercatat dalam sejarah kriptografi, algoritma-algoritma tersebut sering diistilahkan dengan algoritma kriptografi klasik. Pada penelitian ini diimplementasikan kriptografi klasik sebagai metode untuk melakukan proses enkripsi dan dekripsi data teks yang dikirimkan melalui aplikasi *chat*. Dari proses pengujian diperoleh bahwa proses enkripsi dan dekripsi dapat menjaga kerahasiaan data.
Kata Kunci: kriptografi klasik, aplikasi *chat*

***Abstract:** Progress in the field of data communications and computer networks has enabled thousands of people to communicate with a variety of technology hardware and software. On the other hand there is a threat that overshadows the progress, namely the security aspects of data and information. Data security system is needed to protect the data and information that is transmitted over a communications network. One mechanism for providing data security services are cryptographic techniques. In cryptography, the data that is sent over the network will be disguised in such a way encryption techniques so that the data can be read even if it can not be understood by unauthorized parties. Data to be transmitted and has not experienced known as The term plaintext encryption, and after camouflaged with an encryption method, then it will turn into a plaintext ciphertext. Before the advent of computers, cryptography is done with a character-based algorithms. There are a number of algorithms that are recorded in the history of cryptography, algorithms are often termed classical cryptography algorithms. In this study classical cryptography implemented as a method to perform the encryption and decryption of data that is sent via text chat application. Of the testing process is obtained that the encryption and decryption process to maintain the confidentiality of the data.*
***Keywords:** classical cryptography, chat application*

I. PENDAHULUAN

Komunikasi di era teknologi informasi tidak lagi harus dilakukan dengan cara bertemu langsung atau bertatap muka. Komunikasi dapat dilakukan dengan beragam bantuan baik perangkat keras maupun perangkat lunak. Salah satu bentuk komunikasi yang sering dilakukan adalah menggunakan teks. Dengan berkirim pesan melalui teks, pesan dapat sampai dari sisi pengirim ke sisi penerima. Pengiriman informasi melalui teks dapat dilakukan dengan fasilitas *e-mail*, *chatting*, sms, dan bentuk komunikasi lain berbasis teks.

Salah satu bentuk komunikasi berbasis teks yang banyak digunakan di *social media* adalah aplikasi *chatting*. Layanan web seperti *facebook* dan *yahoo* juga menyediakan fasilitas *chatting* untuk berkirim pesan dengan menggunakan jaringan internet.

Aplikasi *chatting* banyak dilakukan karena penggunaannya yang relatif mudah, serta dalam keadaan yang sibuk masih tetap dapat memanfaatkan aplikasi tersebut. Penggunaan layanan seperti *yahoo messenger* atau *facebook messenger* membutuhkan koneksi internet secara terus menerus. Pada kenyataannya tidak semua komputer yang ada baik di kantor maupun rumah mempunyai koneksi ke internet. Pada kebanyakan komputer yang ada di perkantoran sebagian masih terhubung dalam jaringan *Local Area Network* (LAN). Sehingga perlu adanya sebuah layanan aplikasi *chatting* yang dapat berjalan dalam sebuah jaringan.

Pesan yang dikirimkan antar pengguna aplikasi *chatting* perlu diberikan layanan keamanan data, sehingga hanya orang-orang yang memiliki otoritas saja yang dapat mengetahui isi pesan yang disampaikan tersebut. Walaupun komunikasi dilakukan dalam mode *offline* hanya melalui jaringan LAN tetapi tidak menutup kemungkinan jalur komunikasi tersebut disusupi oleh *cracker* yang dapat mengakses pesan yang ditransmisikan. Perlu dibuat mekanisme supaya pesan yang dikirimkan dapat terjaga kerahasiaannya.

Dengan demikian permasalahan yang akan dimunculkan dalam penelitian ini adalah:

1. Bagaimana membangun sebuah aplikasi *chatting* dengan memanfaatkan jaringan *Local Area Network* (LAN)?
2. Bagaimana teknik mengamankan pesan pada aplikasi *chatting* sehingga dapat menjamin kerahasiaan pesan yang dikirimkan?

II. TINJAUAN PUSTAKA

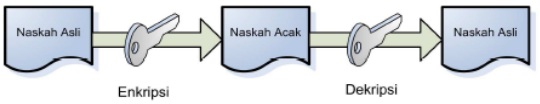
Kriptografi (*Cryptography*) berasal dari bahasa Yunani, terdiri dari dua suku kata yaitu *kripto* dan *graphia*. *Kripto* artinya menyembunyikan, sedangkan *graphia* artinya tulisan. Kriptografi adalah ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi, seperti kerahasian data, keabsahan data, integritas data, serta autentikasi data. Tetapi tidak semua aspek keamanan informasi dapat diselesaikan dengan kriptografi [1].

Kriptografi dapat pula diartikan sebagai ilmu atau seni untuk menjaga keamanan pesan. Ketika suatu pesan dikirim dari suatu tempat ke tempat lain, isi pesan tersebut mungkin dapat disadap oleh pihak lain yang tidak berhak untuk mengetahui isi pesan tersebut. Untuk menjaga pesan, maka pesan tersebut dapat diubah menjadi sebuah kode yang tidak dapat dimengerti pihak lain [2].

Enkripsi adalah sebuah proses penyandian yang melakukan perubahan sebuah kode (pesan) dari yang bisa dimengerti (*plaintext*) menjadi sebuah kode yang tidak bisa dimengerti (*chipertext*). Sedangkan proses kebalikannya untuk mengubah *cipertext* menjadi *plaintext* disebut dekripsi. Proses enkripsi dan deskripsi memerlukan suatu mekanisme dan kunci tertentu [3]. 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 [4]. Dekripsi menggunakan kunci dekripsi mendapatkan kembali data asli. Proses enkripsi dilakukan

menggunakan suatu algoritma dengan beberapa parameter. Biasanya algoritma tidak dirahasiakan, bahkan enkripsi yang mengandalkan kerahasiaan algoritma dianggap sesuatu yang tidak baik. Rahasia terletak di beberapa parameter yang digunakan, jadi kunci ditentukan oleh parameter.

Algoritma kriptografi klasik memiliki ciri diantaranya berbasis karakter dan menggunakan kunci simetri. Dalam kriptografi klasik, teknik enkripsi yang digunakan adalah enkripsi simetris dimana kunci dekripsi sama dengan kunci enkripsi seperti dapat dilihat pada Gambar 1.



Gambar 1. Proses Enkripsi dan Dekripsi

Salah satu algoritma klasik adalah *Caesar chipper*. Dalam kriptografi klasik, secara umum dapat dikelompokkan dalam dua model yaitu menggunakan tekik substitusi dan transposisi [6]. Teknik substitusi dilakukan dengan mengganti salah satu karakter yang ada dalam sebuah teks menggunakan karakter yang lain. Teknik yang termasuk dalam kategori substitusi adalah kriptografi Caesar. Teknik yang digunakan adalah dengan memetakan karakter A-Z ke dalam deretan *index numeric* seperti Gambar 2.

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 2. Pemetaan Karakter

Algoritma *Caesar chipper* melakukan pergeseran karakter sebagai kunci (k) dengan rentang nilai k sebesar 1 – 25, yang secara matematis dijabarkan dalam bentuk:

Untuk proses enkripsi

$$C = E(k,p) = (p + k) \, mod \, 26 \qquad (1)$$

Sedangkan untuk melakukan proses dekripsi

$$P = D(k,c) = (C - k) \, mod \, 26 \qquad (2)$$

Dari sudut pandang aplikasi, koneksi antar komputer yang terbentuk adalah koneksi dari *socket* ke *socket*. *Socket* adalah dua buah nilai yang mengidentifikasi setiap *endpoint* sebuah alamat IP dan sebuah nomor port [5]. Untuk dapat berkomunikasi antara dua komputer, masing-masing port harus dalam kondisi terbuka. Tahapan dalam melakukan koneksi antara komputer *client* dan *server* dapat dijabarkan sebagai berikut .

1) *Server* membuat sebuah *socket* dengan menggunakan karakter unik (misalnya dengan penentuan alamat IP dan nomor *port*), yang dapat diidentifikasi dan ditemukan oleh *client*, pada saat ini *server* telah memasuki kondisi *listening*. Kondisi *listening* adalah keadaan di mana *server* dalam kondisi siap untuk menerima permintaan servis dari *client*.
2) *Client* membuat *socket*, mencari nama atau alamat *socket server* dan kemudian "menyambungkannya" untuk menginisialisasi sebuah komunikasi.
3) Setelah inisialisasi dilakukan maka *client* dan *server* sudah bisa saling mengirimkan data dan menerima data.

Dalam pengembangan sistem yang akan dibangun digunakan bahasa pemrograman Basic, merupakan bahasa pemrograman yang banyak digunakan oleh programmer pemula. Bahasa ini mudah digunakan dan tidak banyak ketentuan yang mengikat, dibandingkan bahasa prosedural seperti Bahasa C atau Pascal. Pada Visual Basic perancangan aplikasi dimulai dari mendefinisikan tujuan program, merancang keluaran sebagai

media komunikasi dengan pengguna, dan menuliskan kode programnya [7].

Pemrograman dengan *Visual Basic* banyak menggunakan istilah obyek. Obyek-obyek digunakan pada *layer* untuk melakukan pengaturan properti terhadap obyek yang digambarkan. Pada saat program dijalankan, dituliskan metode-metode terhadap obyek tersebut sesuai dengan tujuan program. Untuk membuat sebuah program aplikasi dengan *Visual Basic*, dimulai dengan membuat *form* terlebih dahulu, kemudian dibuat *file* dan modul lain. Setelah komponen dipadukan dan kode selesai ditulis, dilanjutkan dengan membuat proyek menjadi *file* yang dapat dieksekusi [8].

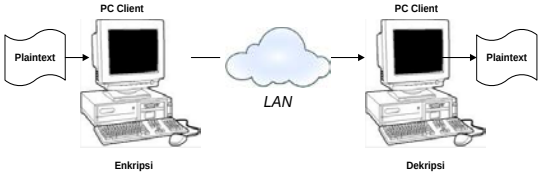
Penelitian dengan tema komunikasi berbasis teks (*chatting*) telah banyak dilakukan, diantaranya penelitian yang dilakukan oleh Setiawan [9] yang telah mengembangkan aplikasi *chatting* menggunakan jaringan LAN. Aplikasi dapat digunakan oleh beberapa orang secara serentak (*multiuser*) dan didalamnya juga terdapat fasilitas untuk berkirim *file* sehingga menjadi komunikasi antara *user* dapat berjalan lebih efektif. Sisi lemah dari aplikasi ini adalah masih belum adanya fasilitas *history* yang mencatat isi informasi komunikasi yang telah dilakukan sehingga dapat dibuka kembali pada sesi komunikasi berikutnya. Penelitian yang dilakukan Zakaria [10] juga telah mengembangkan teknologi komunikasi *chatting* menggunakan media komputer dan *handphone* melalui koneksi Bluetooth. Dalam sistem yang dikembangkan telah terdapat fasilitas *history* yang menyimpan informasi komunikasi yang telah berlangsung sebelumnya.

Penelitian tentang penyandian data pernah dilakukan oleh Hasugian [11] yang mengembangkan teknik penyandian *hill cipher* pada penyimpanan basis data. Informasi yang tersimpan di dalam basis data dibagi menjadi beberapa blok kemudian dilakukan proses enkripsi. Sistem dikembangkan dengan bahasa pemrograman *Visual Basic* 6 untuk proses penyandian di dalam basis data. Penggunaan kriptografi klasik lainnya juga pernah dilakukan oleh Fairuzabadi [12] dan Sasongko [13] yang telah mengembangkan sistem keamanan data menggunakan bahasa pemrograman Delphi dan bahasa C/C++. Penelitian ini lebih mengedepankan aspek pemrograman dengan memetakan formula matematis ke dalam bahasa pemrograman.

Dalam penelitian ini yang dilakukan adalah mengembangkan sebuah aplikasi *chatting* dengan menggunakan teknik kriptografi klasik. Sehingga informasi yang dikirimkan oleh *user* yang saling berkomunikasi di dalam sistem dapat terjaga kerahasiaan datanya.

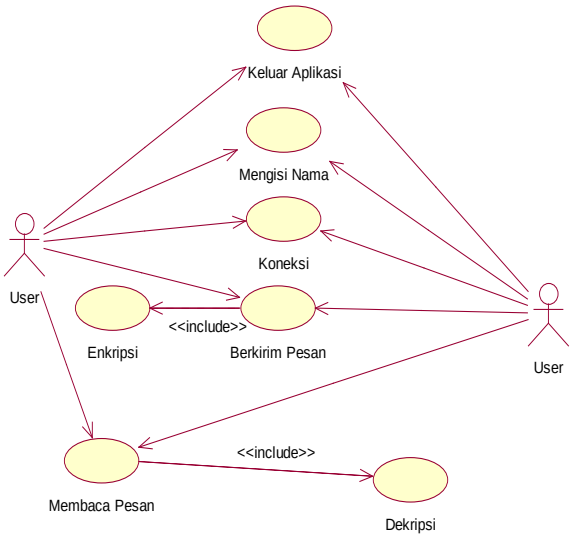
III. METODE PENELITIAN

Dalam proses komunikasi berbasis teks yang dikembangkan, pesan dikirim dalam bentuk teks yang telah dienkripsi (*chipertext*), ketika pesan sampai pada sisi penerima pesan dikemas dalam pesan yang telah didekripsi (*plaintext*) seperti dapat dilihat pada Gambar 3. Pesan tersebut dikirimkan melalui jaringan *Local Area Network* (LAN). Sistem ini merupakan aplikasi *chat* sederhana yang pengiriman datanya pesan telah dienkripsi menggunakan algoritma *Caesar chipper*. Sistem ini mengizinkan 2 orang *user* untuk berkomunikasi melalui TCP/IP.



Gambar 3. Rancangan Sistem Yang Dibangun

Secara umum layanan yang ada di dalam aplikasi yang dibangun dapat dilihat pada Gambar 4, terdapat fasilitas untuk mengisi nama dan melakukan koneksi ke jaringan LAN. Pada saat melakukan proses pengiriman pesan, selalu melibatkan enksripsi yang didalamnya terdapat metode/fungsi untuk melakukan enkripsi. Dan pada proses pembacaan pesan selalu menggunakan *use case* dekripsi untuk mengembalikan kembali pesan yang telah dienkripsi sehingga terbaca oleh sistem.

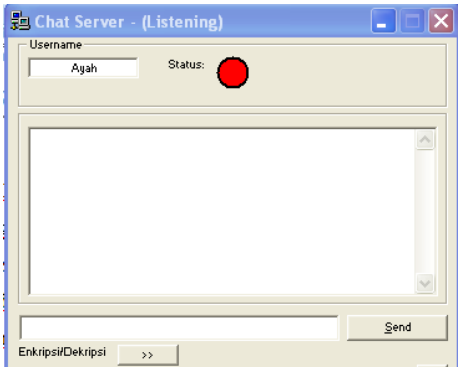


Gambar 4. Use Case Diagram Sistem

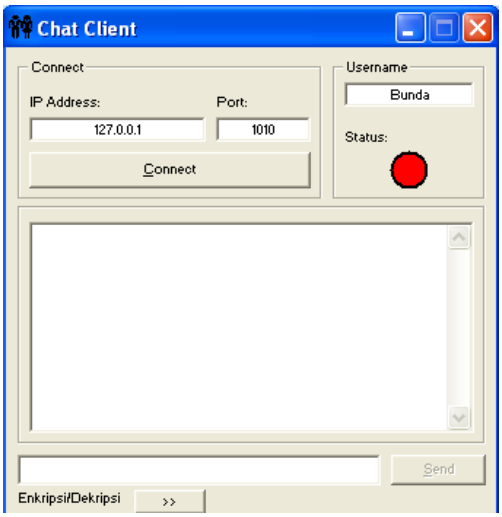
IV. HASIL DAN PEMBAHASAN

Penelitian ini menghasilkan perangkat lunak yang dibangun dalam lingkungan *client/server* dengan model *visual/desktop application.*

Aplikasi yang dibangun menghasilkan 2 buah aplikasi, 1 buah bertindak sebagai *server* dan 1 buah sebagai *client.* Aplikasi *server* menunggu (*listening*) permintaan komunikasi dari *client.* Demikian juga *client* harus proaktif untuk memulai komunikasi. Pada awal kedua aplikasi diaktifkan masing-masing terdapat indikator lampu berwarna merah, yang menandakan bahwa komunikasi antara *client* dan *server* belum terbentuk seperti dapat dilihat pada Gambar 5.



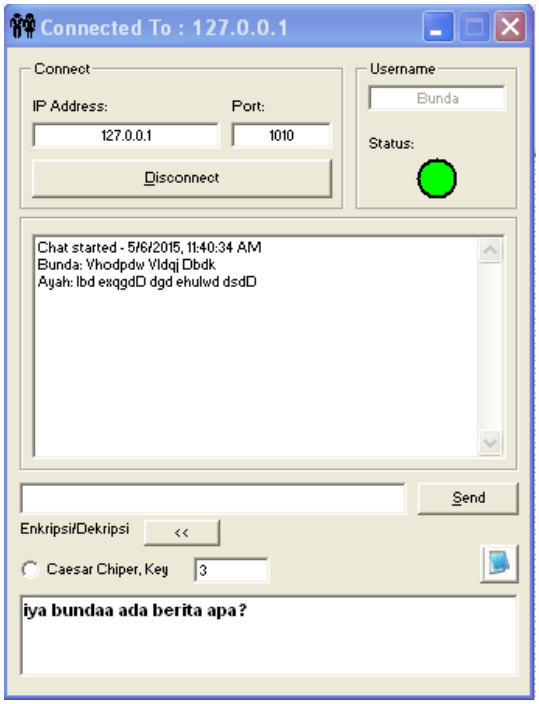
(a) Posisi *server* menunggu *request*



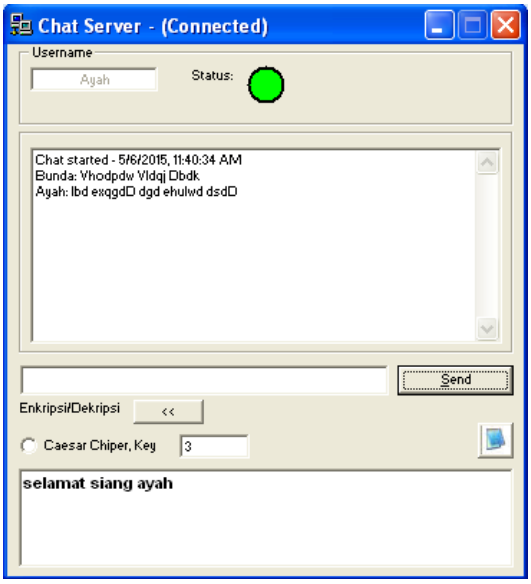
(b) Posisi *client* pertama kali aktif

Gambar 5. Posisi Aplikasi *Client* dan *Server* Pada Saat Diaktifkan Pertama Kali.

Setelah komunikasi terbentuk kedua lampu indikator pada masing-masing aplikasi akan berwarna hijau yang menandakan bahwa komunikasi telah terbentuk. Teks yang terkirim pada aplikasi akan dienkripsi menggunakan algoritma *Caesar Chipper* dengan pergeseran sebanyak 3 karakter. Seperti dapat dilihat pada Gambar 6. Di bagian bawah dari panel aplikasi terdapat teks yang terbaca (*plaintext*) sehingga setiap kali sesi berkirim pesan dilakukan otomatis akan didekripsi sehingga terbaca pada sisi penerima. Pada proses komunikasi secara *runtime* dapat diubah parameter pergeseran kunci dari algoritma *Caesar chipper* pada Gambar 6 terlihat menggunakan pergeseran kunci sebanyak 3.



(a) Teks Pada Aplikasi *Client*



(b) Teks Pada Aplikasi *Server*

Gambar 6. Pola Pengiriman Teks

Pada bagian bawah dari aplikasi *client* dan *server* juga terdapat satu buah *file* teks yang berisi hasil dari proses berkirim pesan dalam bentuk *plaintext*. Sehingga setelah semua sesi komunikasi berbasis teks telah selesai dilakukan dapat dilihat secara menyeluruh komunikasi yang telah terjadi. Hasil sesi percakapan disimpan dalam satu buah *file* teks sehingga dapat dibuka dengan mudah menggunakan aplikasi *text editor* seperti Notepad.

Beberapa pengujian yang dilakukan dari sisi aplikasi menggunakan metode *black box* dapat dijabarkan pada Tabel 1. Pengujian *black box* (*black box testing*) adalah salah satu metode pengujian perangkat lunak yang berfokus pada sisi fungsionalitas, khususnya pada *input* dan *output* aplikasi (apakah sudah sesuai dengan apa yang diharapkan atau belum). Tahap pengujian atau *testing* merupakan salah satu tahap yang harus ada dalam sebuah siklus pengembangan perangkat lunak (selain tahap perancangan atau desain).

Tabel 1. Pengujian *Black Box* Aplikasi *Chatting*

No.	Skenario Pengujian	*Test Case*	Hasil yang diharapkan	Hasil Pengujian	Simpulan
1	Mengisi-kan nama sebagai identitas user yang menggunakan aplikasi dan melakukan koneksi	Nama: -	Sistem akan memberikan respon bahwa proses koneksi untuk mulai komunikasi dapat dilakukan setelah user mengisikan nama.	Sesuai harapan	Valid
2	Mengosong-kan semua isian data pesan, kemudian menkan tombol Send.	Pesan: -	Sistem akan menolak proses pengiriman pesan dengan memuncul-kan informasi bahwa “Pesan Masih Kosong”	Sesuai harapan	Valid
3	Menginputka n pesan yang akan dikirim-kan kepada penerim. Pesan yang dikirim-kan adalah sapaan ‘selamat siang’. Ketika pesan sampai pada sisi penerima akan dienkripsi menjadi ‘vhodpdw vldqj’	Pesan: selamat siang	Sistem akan melakukan enkripsi pesan mengguna-kan algoritma Caesar chipper dengan pergeseran kunci sebanyak k=3	Sesuai harapan	valid

Dari sisi *content* informasi aplikasi yang dikembangkan juga dilakukan pengujian untuk melihat sejauh mana kemampuan *module* kriptografi klasik yang ditanamkan di dalam sistem. Pengujian yang dilakukan adalah dengan menggunakan *input* berupa *plaintext* ataupun *chipertext* untuk melihat *output* yang dihasilkan. Algoritma *Caesar Cipher* menggunakan operasi modulus atau sisa bagi. Operasi pembagian a/n pada bilangan *integer* diinterpretasikan memiliki 2 buah keluaran yaitu hasil bagi (*q/quotion*) dan sisa bagi (*r/remainder*). Relasi keempat bilangan tersebut diekspresikan dalam persamaan [3]:

$$a = q\,x\,n + r \qquad (3)$$

Untuk melihat cara kerja dari algoritma *Caesar cipher* dapat digunakan formula 1) dan formula 2) untuk proses enkripsi dan dekripsi. Sebagai contoh jika terdapat sebuah *plaintext* "SELAMAT SIANG", maka proses enkripsi dan dekripsi dapat dilakukan dengan langkah-langkah seperti pada Tabel 2 dan Tabel 3. Sementara pemetaan karakter dapat dilihat pada Gambar 7.

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 7 Pemetaan Karakter Menjadi *Index Numerik*

Tabel 2 Proses Enkripsi

Plaintext : SELAMAT SIANG
Kunci (k) : 3
Proses Enkripsi

P	*Index*	C = (P+k) mod 26
S	18	(18+3) mod 26 = 21 mod 26 = 21 →V
E	4	(4+3) mod 26 = 7 mod 26 = 7 →H
L	11	(11+3) mod 26 = 14 mod 26 = 14 →O
A	0	(0+3) mod 26 = 3 mod 26 = 3 →D
M	12	(12+3) mod 26 = 15 mod 26 = 15 →P
A	0	(0+3) mod 26 = 3 mod 26 = 3 →D
T	19	(19+3) mod 26 = 22 mod 26 = 22 →W
S	18	(18+3) mod 26 = 21 mod 26 = 21 →V
I	8	(8+3) mod 26 = 11 mod 26 = 11 →L
A	0	(0+3) mod 26 = 3 mod 26 = 3 →D
N	13	(13+3) mod 26 = 16 mod 26 = 16 →Q
G	6	(6+3) mod 26 = 9 mod 26 = 9 →J

Sehingga diperoleh proses enkripsi
Plaintext : SELAMAT SIANG
Ciphertext : VHODPDW VLDQJ

Tabel 3 Proses Dekripsi

Ciphertext : VHODPDW VLDQJ
Kunci (k) : 3
Proses Dekripsi

C	*Index*	P = (C - k) mod 26
V	21	(21-3) mod 26 = 18 mod 26 = 18 →S
H	7	(7-3) mod 26 = 4 mod 26 = 4 →E
O	14	(14-3) mod 26 = 11 mod 26 = 11 →L
D	3	(3-3) mod 26 = 0 mod 26 = 0 →A
P	15	(15-3) mod 26 = 12 mod 26 = 12 →M
D	3	(3-3) mod 26 = 0 mod 26 = 0 →A
W	22	(22-3) mod 26 = 19 mod 26 = 19 →T
V	21	(21-3) mod 26 = 18 mod 26 = 18 →S
L	11	(11-3) mod 26 = 8 mod 26 = 8 →I
D	3	(3-3) mod 26 = 0 mod 26 = 0 →A
Q	16	(16-3) mod 26 = 13 mod 26 = 13 →N
J	9	(9-3) mod 26 = 6 mod 26 = 6 →G

Sehingga diperoleh proses dekripsi
Ciphertext : VHODPDW VLDQJ
Plaintext : SELAMAT SIANG

Proses ujicoba *module* kriptografi klasik *Caesar Cipher* untuk beberapa teks dapat dilihat pada Tabel 4.

Tabel 4. Pengujian Kriptografi

Enkripsi	*Chipertext*	Dekripsi	Berhasil	Gagal
Selamat siang	vhodpdw vldqj	Selamat siang	✓	
Apa kabar	dsd ndedu	Apa kabar	✓	
Sehat	vhkdw	Sehat	✓	
Yang diperoleh	bdqj glshurohk	Yang diperoleh	✓	
Exotic	harwlf	Exotic	✓	
Zigzag	cljcdj	Zigzag	✓	

V. SIMPULAN

Setelah penelitian ini selesai dilakukan, selanjutnya dapat disimpulkan bahwa untuk membangun aplikasi komunikasi berbasis teks dapat dibangun aplikasi *chatting* menggunakan pemrograman *socket*, dengan arsitektur aplikasi *client/server*. Algoritma *Caesar chipper* dapat digunakan untuk melakukan enkripsi/dekripsi pesan yang dikirimkan dalam aplikasi *chatting*.

Untuk penelitian lanjutan dapat dikembangkan dengan membuat komunikasi *chatting* di dalam sebuah group, sehingga banyak *user* yang dapat bergabung dalam aplikasi untuk berkirim pesan. Dari sisi metode enkripsi dapat ditambahkan beberapa pilihan teknik enkripsi sehingga akan menjadikan aplikasi semakin tangguh untuk menjaga kerahasiaan data.

UCAPAN TERIMA KASIH

Terimakasih kepada seluruh redaksi Jurnal Pseudocode yang telah memberi kesempatan, sehingga tulisan ini dapat dimuat.

REFERENSI

[1] Ariyus, D. (2006). "*Kriptografi Keamanan Data dan Kriptografi*".Yogyakarta: Penerbit Andi Offset.

[2] Maulana, A., R. (2012). "*Penerapan Algoritma WAKE Pada Aplikasi Chatting & Internet Monitor Berbasis LAN*". Yogyakarta : STMIK Amikom Yogyakarta.

[3] Kurniawan, Y. (2004). "*Kriptografi Keamanan Internet dan Jaringan Komunikasi*". Bandung: Penerbit Informatika.

[4] Kromodimoeljo, S. (2009). "*Teori dan Aplikasi Kriptografi*". Jakarta: SPK IT Consulting

[5] Stevens, Richard W. (1998). "*UNIX Network Programming Volume I, Networking APIs: Sockets and XTI*", Prentice-Hall,Inc.

[6] Stalling, W. (2006). "*Cryptography and Network Security Principles and Practice Fifth Edition*". New York: Prentice Hall

[7] Putra, I. (2004). "*Membangun Aplikasi Nyata Dengan Visual Basic 6.0*". Yogyakarta: Penerbit Andi.

[8] Nalwan, A. (2004). "*Membuat Program Profesional Secara Cepat dengan VB*". Jakarta: Penerbit Gramedia

[9] Setiawan, R. (2009). "*Membangun Aplikasi Chatting Berbasis Multiuser Jurnal DASI Vol. 10 No. 1 Maret 2009*". Yogyakarta: STMIK AMIKOM

[10] Zakaria, M. T.; Wijaya, D.S. (2009). "*Aplikasi Chat pada Handphone dan Komputer dengan Media Bluetooth (Bluetooth Chat) Jurnal Teknologi Informasi-Aiti Vol. 6 No. 1 Februari 2009*". Bandung: Universitas Kristen Maranatha

[11] Hasugian, H. A. (2013). "*Implementasi Algoritma Hill Cipher Dalam Penyandian Data jurnal Pelita Informatika Budi Darma Vol. 4 No. 2 Agustus 2013*". Medan: STMIK Budi Darma

[12] Fairuzabadi, M. (2010). "*Implementasi Kriptografi Klasik Menggunakan Borland Delphi, Jurnal Dinamika Informatika Vol. 4 No. 2 September 2010*". Yogyakarta: Universitas PGRI

[13] Sasongko, J. (2005). "*Pengamanan Data Informasi Menggunakan Kriptografi Klasik, Jurnal Teknologi Informasi Dinamik Vol. 10 No. 3 September 2005*". Semarang: Universitas Stikubang

[14] Sadikin, R. (2012). "*Kriptografi Untuk Keamanan Jaringan*". Yogyakarta: Penerbit Andi Offset