CORE
Metadata, citation and similar papers at core.ac.uk
Provided by EEPIS Repository

# RANCANG BANGUN SISTIM ENKRIPSI PENGIRIMAN INFORMASI MENGGUNAKAN ALGORITMA KRIPTOGRAFI KLASIK

Fia Firtin[1],M.Zen Samsono Hadi, ST.Msc[2],Ir.Nanang Syahroni, MKom[2]
Mahasiswa Jurusan Teknologi Telekomunikasi[1], Dosen Pembimbing[2]
Politeknik Elektonika Negeri Surabaya
Institut Teknologi Sepuluh Nopember
Kampus PENS-ITS Keputih Sukolilo Surabaya 60111
Telp (+62)31-5947280, 5946114, Fax. (+62)31-5946114
e-mail : fia@student.eepis-its.edu , fia_kirei78@ymail.com

## Abstrak

Pada lingkungan kompetitif sekarang ini,memungkinkan manusia dapat berkomunikasi dan dapat bertukar informasi/data secara jarak jauh. Antar kota, Negara maupun antar benua bukan suatu kendala lagi dalam melakukan komunikasi dan pertukaran data. Seiring dengan itu tuntutan akan sekuritas (keamanan) terhadap kerahasiaan informasi yang saling dipertukarkan tersebut semakin meningkat. Oleh karena itu dikembangkanlah cabang ilmu yang mempelajari tentang cara-cara pengamanan data atau dikenal dengan istilah Kriptografi.

Seperti halnya sebuah sistem pengamanan data yang dibuat pada proyek akhir ini, proses enkripsi menjadi pendukung didalam nya. Didalam proses enkripsi terdapat sebuah proses dimana data akan disandikan berupa huruf random, dan proses itu dinamakan proses plaintext-ciphertext. Sedangkan pada sisi penerima pesan akan mengalami sebuah proses deskripsi, dimana data random akan diubah ke data sebenarnya atau bisa disebut dengan proses ciphertext-plaintext. Dengan menggunakan metode vigenere cipher, maka diperlukannya sebuah kunci untuk memperoleh sebuah ciphertext. Dimana kunci ditentukan oleh panjang huruf dari plaintext yang diinputkan.

Hasil dari penelitian ini adalah pengiriman data melalui client menuju server dengan mengenkripsikannya sehingga data yang sampai pada server akan langsung tersandikan. Pada sisi server, data yang tersandikan tersebut akan diubah menjadi plaintext kembali melalui proses dekripsi

**Kata Kunci** : Algoritma,Vigenere Cipher, Socket Programming, C Programming.

## *ABSTRACT*

In today's competitive environment, enabling people to communicate and exchange information / data remotely. Between cities, countries and between continents is not an obstacle anymore in the communication and data exchange. Along with that the demand for securities (security) to the confidentiality of information exchanged on the rise. Therefore it is developing branch of science that studies on ways of data security or cryptography known.

Just as a data security system created at the end of this project, the encryption process to be advocates in him. In the process of encryption there is a process by which data is encrypted in the form of random letters, and the process is called the plaintext-ciphertext. While on the side of the receiver will experience a process description, in which random data is converted to actual data or can be called with the ciphertext-plaintext. By using the method vigenere cipher, then the need for a key to obtain a ciphertext. Where the lock is determined by the length of the plaintext letters are entered.

The result of this study issending data through the client to the server with encryption system so that the data to the server will be directly encoded. On the server, the encrypted data will be converted into the plaintext back through the process description

***Key** : cryptography, algorithms, C programming, vigenere cipher, socket programming*

# I. PENDAHULUAN

## 1.1 Latar Belakang

Masalah keamanan dan kerahasiaan merupakan salah satu aspek penting dari suatu pengiriman data, pesan, informasi. Pengiriman suatu data, pesan, informasi membutuhkan tingkat keamanan yang tinggi. Dengan berkembang nya teknologi informasi yang berkembang pesat saat ini, dimana setiap orang akan dengan mudah mendapatkan informasi, data ataupun pesan. Berbagai cara dilakukan orang untuk mendapatkan data ataupun informasi tersebut. Mulai dari cara yang mudah sampai pada cara-cara yang rumit, cara yang tidak selayaknya dilakukan. Dan berbagai cara pula orang berusaha untuk melindungi pesan, data, informasi tersebut agar tidak diketahui oleh orang yang tidak mempunyai wewenang atas pesan, data, atau informasi tersebut.

Ilmu yang mempelajari tentang proses pengamanan data adalah kriptografi. Secara umum ada 2 macam jenis kriptografi, yaitu kriptografi klasik dan kriptografi modern. Kriptografi klasik adalah suatu algoritma yang menggunakan satu kunci untuk mengamankan data. Dua kunci utama yang biasa digunakan adalah substitusi dan transposisi(permutasi). Sedangkan kriptografi modern adalah algoritma yang lebih komplek daripada algoritma kriptografi klasik, hal ini disebabkan algoritma ini menggunakan computer. Algoritma yang digunakan penulis adalah algoritma kriptografi klasik.

Dalam kriptografi terdapat dua konsep utama yakni enkripsi dan dekripsi. Enkripsi adalah proses dimana informasi/data yang hendak dikirim diubah menjadi bentuk yang hampir tidak dikenali sebagai informasi awalnya dengan menggunakan algoritma tertentu. Dekripsi adalah kebalikan dari enkripsi yaitu mengubah kembali bentuk tersamar tersebut menjadi informasi awal.

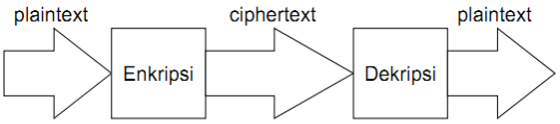
Dalam kriptografi, data yang dikirimkan melalui jaringan akan disamarkan sedemikian rupa sehingga kalaupun data itu bisa dibaca maka tidak bisa dimengerti oleh pihak yang tidak berhak. Data yang akan dikirimkan dan belum mengalami penyandian dikenal dengan isitilah plaintext, dan setelah disamarkan dengan suatu cara penyandian, maka plaintext ini akan berubah menjadi ciphertext.

# II. TEORI PENUNJANG

## 2.1 Kriptografi

Kriptografi (cryptographi) berasal dari BahasaYunani: “cryptos” artinya “secret” (rahasia), sedangkan “graphein” artinya “writing” (tulisan). Sehingga kriptografi berarti “secret writing” (tulisan rahasia). Jadi kriptografi didefinisikan sebagai ilmu dan seni untuk menjaga kerahasiaan pesan dengan cara menyandikannya kebentuk yang tidak dapat dimengerti lagi maknanya.

Secara umum kriptografi merupakan teknik pengamanan informasi yang dilakukan dengan cara mengolah informasi awal (plainteks) dengan suatu kunci tertentu menggunakan suatu metode enkripsi tertentu sehingga menghasilkan informasi baru (chipertext) yang tidak dapat dibaca secara langsung. Chipertext tersebut dapat dikembalikan menjadi informasi awal (plainteks) melalui proses deskripsi. Urutan proses kriptografi secara umum dapat dilihat pada gambar 2.1



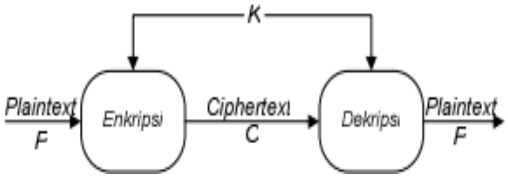

**Gambar 2.1** Mekanisme Enkripsi dan Deskripsi

Terdapat dua jenis algoritma kriptografi berdasar jenis kuncinya :

1. Algoritma Simetri (konvensional)
2. Algoritma Asimetri (kunci public)

### 2.1.1 Algoritma Simetri

Algoritma simetri disebut juga sebagai algoritma konvensional adalah algoritma yang menggunakan kunci enkripsi yang sama dengan kunci dekripsinya. Yang termasuk algoritma kunci simetri adalah OTP, DES, RC2, RC4, RC5, RC6, IDEA, Twofish, Magenta, FEAL, SAFER, LOKI, CAST, Rijndael (AES), Blowfish, GOST, A5, Kasumi dan lain-lain.




**Gambar 2.2** Kriptografi Konvensional.

Orang sering menggunakan notasi matematika untuk mempermudah penulisan dan analisis, sehingga kriptografi modern selalu berhubungan dengan matematika. Dengan pesan asal P dan kode rahasia C yang diperoleh dari enkripsi dengan kunci K, kita dapat dituliskan sebagai berikut :

**C = Ek (P)**

Pada proses dekripsi, dilakukan operasi sebaliknya, dan dapat dituliskan sebagai berikut :

**P = Dk (P)**

### 2.1.2 Algoritma Asimetrik

Algoritma asimetrik (juga disebut algoritma kunci public) didesain sedemikian sehingga kunci yang digunakan untuk enkripsi berbeda dari kunci yang digunakan untuk dekripsi.Enkripsi dengan kunci public Ke dinyatakan sebagai berikut :

**EKe (M) = C**

**DKd (C) = M**

## 2.2 Tujuan Kriptografi

4 aspek yang terdapat pada kriptografi:

1. *Confidentiality* (kerahasiaan)
   Layanan yang ditujukan untuk menjaga pesan agar tidak dapat dibaca oleh pihak-pihak yang tidak berhak.
2. *Authentication* (otentikasi)
   Penerima pesan dapat memastikan keaslian pengirimnya. Penyerang tidak dapat berpura-pura sebagai pengirim atau penerima pesan.
3. *Integrity*(integritas)
   Penerima harus dapat memeriksa apakah pesan telah dimodifikasi ditengah jalan atau tidak. Seorang penyusup seharusnya tidak dapat memasukkan tambahan ke dalam pesan, mengurangi atau mengubah pesan selama data berada di perjalanan.
4. *Nonrepudiation* (nirpenyangkalan)
   Pengirim tidak dapat mengelak bahwa dia telah mengirim pesan, penerima juga tidak dapat mengelak bahwa dia telah menerima pesan tersebut.

## 2.3 Vigenere Cipher

Sandi Vigenere adalah metode menyandi teks alphabet dengan menggunakan deretan sandi Caesar berdasarkan hurufhuruf pada kata kunci. Sandi Vigenere merupakan bentuk sederhana dari sandi polialfabetik. Kelebihan sandi ini dibanding sandi Caesar dan sandi monoalfabetik lainnya adalah sandi ini tidak begitu rentan terhadap metode pemecahan sandi yang disebut analisis frekuensi. Giovan Batista Belaso menjelaskan metode ini dalam buku La cifra del. Sig. Giovan Batista Nelaso (1553) dan disempurnakan oleh diplomat Perancis Blaise de Vigenere pada tahun 1586. Pada abad ke19 banyak orang yang mengira vigenere adalah penemu sandi ini, sehingga sandi ini dikenal sebagai “sandi Vigenere”.

Sandi ini dikenal dengan luas karena cara kerjanya mudah dimengerti dan dijalankan dan bagi para pemula sulit dipecahkan. Pada saat kejayaannya, sandi ini dijuluki le chiffre indenchiffrable (bahasa perancis: “sandi yang tak terpecahkan”). Metode pemecahan sandi ini baru ditemukan pada abadke19. Pada tahun 1854, Charles Babbage menemukan cara untuk memecahkan sandi vigenere. Metode ini dinamakan tes Kasiski karena Friedrich Kasiskilah yang pertama mempublikasikannya.

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.

**Tabel 2.1** Tabel Kriptografi Vigenere Cipher.

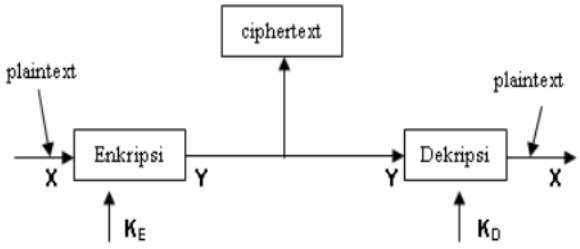
| | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| A | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | 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 |

## 2.4 Enkripsi dan Deskripsi

Proses penyandian pesan dari plaintext ke ciphertext dinamakan enkripsi / *enchipering* . Sedangkan proses mengembalikan pesan dari chipertext ke plaintext dinamakan deskripsi /

dechipering. Proses enkripsi dan deskripsi ini dapat diterapkan pada pesan yang dikirim ataupun pesan yang disimpan.

Algoritma Kriptografi dari setiap kriptografi klasik selalu terdiri dari dua bagian yaitu enkripsi dan dekripsi. Secara sederhana proses kriptografi dapat digambarkan sebagai berikut :




**Gambar 2.3** Kriptografi secara umum.

Operasi enkripsi dan dekripsi dijelaskan secara umum sebagai berikut :

Y Eκe = (enkripsi)

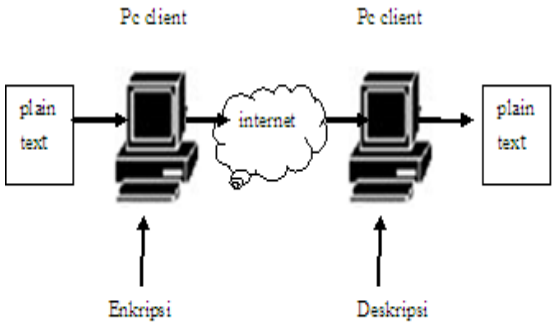
X Dκd = (dekripsi)

Ada dua cara yang paling dasar pada kriptografi klasik. yaitu adalah Transposisi dan Subsitusi :

- Transposisi adalah mengubah susunan huruf pada plaintext sehingga urutannya berubah. Contoh yang paling sederhana adalah mengubah suatu kalimat dengan menuliskan setiap kata secara terbalik.
- Substitusi yaitu setiap huruf pada plaintext akan digantikan dengan huruf lain berdasarkan suatu cara atau rumus tertentu.

## III. PERANCANGAN SISTEM

Sistem pengiriman informasi yang dienkripsi dan di deskripsikan dapat dilihat pada gambar 3.1 dibawah ini




**Gambar 3.1** sistem yang dibangun

Sistem ini merupakan aplikasi chat sederhana yang pengiriman datanya akan melalui proses pengenkripsian terlebih dahulu dimana metode enkripsi yang dipakai adalah vigenere cipher. Program ini akan mengizinkan 2 pihak untuk saling chat satu sama lain melalui koneksi TCP/IP. Vigenere chat ini akan dibuat dalam bahasa C pada Linux.

Ilustrasi pemakaian program ini dapat dimisalkan seperti ini : Misalkan Tisy dan Ajeng ingin menggunakan vigenere chat untuk mengamankan percakapan mereka sehingga tidak disadap oleh orang lain. Satu pihak diantara mereka berdua setuju bertindak sebagai client dan pihak yang lain menjadi server. Pertama-tama server harus menyediakan port yang harus dibuka sehingga mengizinkan client dapat membuat koneksi dengan server.

## IV. PENGUJIAN DAN ANALISA

Pada tahap pengujian ini, penulis akan menguji aplikasi vigenere chat yang telah dibuat. Pengujian dibagi menjadi 2 tahap yaitu

### 4.1 PENGUJIAN PENGENKRIPSIAN MENGGUNAKAN KUNCI YANG SAMA

Pengujian tahap ini dilakukan dengan menjalankan 2 aplikasi vigenere chat yang telah dibuat.

| Enkripsi | Ciphertext | Deskripsi | berhasil | gagal |
|---|---|---|---|---|
| Surabaya | RTAQZAZXZ | SURABAKM | - | √ |
| jaKArtA | IZJZQSZ | JAKARTM | - | √ |
| BANDUNG | AZMCTMF | BANDUZS | - | √ |
| medan | LDCZM | MEDAN | √ | - |
| kota surabaya | JNSZ | KOTA | - | √ |

**Gambar 4.1** Hasil enkripsi yang dikirimkan ke server

Pada tabel diatas , proses yang berhasil membawa informasi dengan benar adalah pada enkripsi medan. Faktor yang mempengaruhi keberhasilan pengiriman karena, pada sisi server, program deskripsinya hanya terdapat untuk huruf kecil saja. Selain itu juga, pada saat data enkripsi diberi spasi, maka yang terbaca pada sisi server sesudah dideskripsi hanya berupa kata awalnya saja. Seperti terlihat pada tabel diatas, pada kata “kota Surabaya” , pada sisi server hanya terbaca KOTA nya saja.

### 4.2 PENGUJIAN PENGENKRIPSIAN DENGAN KUNCI YANG SAMA, DENGAN NILAI DATA < = > DENGANKUNCI

| Enkripsi | Ciphertext | Deskripsi | Keterangan |
|---|---|---|---|
| surabaya | KUPATAWA | SURABAJN | data > kunci |
| data | VARA | DATA | data = kunci |
| ya | QA | YA | data < kunci |

**Gambar 4.2** Enkripsi kunci yang sama dengan nilai data yang < = > dengan kunci

Pada pengujian yang kedua ini, yaitu pengujian berdasarkan nilai data yang lebih besar dari kunci (>), lebih kecil dari kunci (<), dan sama dengan kunci (<). Terlihat bahwa, 2 data telah berhasil mengirimkan datanya secara benar.

## V. KESIMPULAN

Pada penelitian kali ini, penulis mencoba untuk membuat suatu aplikasi pertukaran informasi sederhana dimana lalu lintas datanya diamankan dengan metode enkripsi klasik yaitu vigenere cipher. Namun metode vigenere cipher ini sekarang sudah obsolete(kuno) karena sudah terdapat metode pemecahannya yaitu dengan metode kasiski. Oleh karena itu penulis menyarankan agar algoritma pengenkripsian yang digunakan kedepannya pada fitur pengiriman informasi ialah metode pengenkripsian modern seperti DES atau RSA yang jauh lebih powerful. Dan bukan hanya diaplikasikan pada sistim Linux saja, tetapi dapat diaplikasikan pada selular.

## DAFTAR PUSTAKA


[1]M. Zen Samsono Hadi *"Modul Praktikum 10 Datagram Socket"* Politeknik Elektronika Negeri Surabaya, 2009.

[2]M.Zen Samsono Hadi *"Modul Praktikum 9 Stream Socket Program"* Politeknik Elektronika Negeri Surabaya, 2009.

[3] Abd. Hallim, dkk ,"Pembuatan Perangkat Lunak Media Pembelajaran Kriptografi Klasik", Proyek Akhir PENS-ITS,2010.

[4] Phillip I Wilson, Maria Gracia, "A Modified Version of the Vigenere Algorithm", IEEE,2006.