
PERANCANGAN SISTEM KEAMANAN DATA *INVENTORY* BARANG DI TOKO NANDA BERBASIS *WEB* MENGGUNAKAN METODE *KRIPTOGRAFI VIGENERE CIPHER*

Joni Karman¹, Ahmad Nurhasan²

¹Program Studi Sistem Informasi, Universitas Bina Insan, Lubuklinggau

²Program Studi Informatika, Universitas Bina Insan, Lubuklinggau

Email : ¹jonikarman@univbinainsan.ac.id, , ²hasan.ahmad451@gmail.com

Abstrak

Masalah yang ada pada penelitian ini adalah sistem pencatatan stok barang bangunan pada Toko Nanda masih rentan terhadap kehilangan data, karena sistem pencatatan stok barang pada toko ini masih manual, yaitu dengan cara mengumpulkan nota-nota setiap pembelian nya. Di era modern seperti sekarang ini sudah seharusnya Toko Nanda menggunakan teknologi yang ada sebagai media pengamanan data tersebut. Penelitian ini menggunakan metode pengumpulan data, dengan cara pengamatan langsung pada objek yang diteliti (Observasi), melakukan tanya jawab langsung pada sumber (Interview), dokumentasi dan perpustakaan. Hasil penelitian ini menghasilkan sebuah aplikasi keamanan data *inventory* barang berbasis *web*, dengan menggunakan bahasa pemrograman PHP, dan database menggunakan MySQL, sedangkan untuk keamanan data nya menggunakan metode *kriptografi vigenere cipher*, dan dapat disimpulkan bahwa aplikasi ini dapat membantu Toko Nanda dalam mengamankan data serta dapat mengetahui jumlah stok barang yang tersedia.

Kata Kunci :Keamanan Data, *Inventory*,*Kriptografi*, *Vigenere Cipher*,

Abstract

The problem that exists in this study is the system of recording the stock of building goods in Toko Nanda is still vulnerable to data loss, because the system of recording the stock of goods in this store is still manual, namely by collecting the notes for each purchase. In the modern era, as now, Nanda Store is supposed to use existing technology as a means of securing the data. This study uses data collection methods, by direct observation of the object under study (Observation), conducting question and answer directly to the source (Interview), documentation and library. The results of this study resulted in a web-based inventory data security application, using the PHP programming language, and a database using MySQL, while for data security it uses the vigenere cipher cryptographic method, and it can be concluded that this application can help the Nanda Store in securing data and can find out the amount of available stock.

Keywords: *Data Security*, *Inventory*,*Kriptografi*, *Vigenere Cipher*,

I. PENDAHULUAN

Keamanan data menjadi hal yang sangat penting pada saat ini karena untuk setiap pengambilan keputusan, kebijakan harus berdasarkan data. Banyak data yang berisikan informasi penting dan terbatas untuk diketahui pihak yang terkait saja. Faktor keamanan data menjadi sangat penting dan harus diperhatikan. Salah satu cara untuk meningkatkan keamanan data diperlukan *kriptografi* dengan metode *enkripsi*[1].

Kriptografi pada awalnya dijabarkan sebagai ilmu yang mempelajari bagaimana menyembunyikan pesan. Namun pada pengertian modern *kriptografi* adalah ilmu yang bersandarkan pada teknik matematika untuk berurusan dengan keamanan informasi seperti kerahasiaan, keutuhan data dan otentikasi entitas. Jadi pengertian *kriptografi* modern adalah tidak saja berurusan hanya dengan penyembunyian pesan namun lebih pada sekumpulan teknik yang menyediakan keamanan informasi[2].

Vigenere cipher adalah salah satu algoritma *kriptografi* klasik yang diperkenalkan pada abad 16 atau kira-kira pada tahun 1586. Algoritma *kriptografi* ini dipublikasikan oleh seorang diplomat dan juga kriptologis yang berasal dari Prancis, yaitu Blaise de Vigenere, namun sebenarnya algoritma ini telah digambarkan sebelumnya pada buku *La Cifra del Sig.* Giovan Batista Belaso, sebuah buku yang ditulis oleh Giovan Batista Belaso, pada tahun 1553.

Cara kerja dari *Vigenere cipher* ini mirip dengan *Caesar cipher*, yaitu mengenkripsi plaintext pada pesan dengan cara menggeser huruf pada pesan tersebut sejauh nilai kunci pada deret alphabet. *Vigenere cipher* adalah salah satu algoritma kriptografi klasik yang menggunakan metode substitusi abjad majemuk. Substitusi abjad-majemuk mengenkripsi setiap huruf yang ada menggunakan kunci

yang berbeda, tidak seperti *Caesar cipher* yang menerapkan metode substitusi abjad-tunggal yang semua huruf di suatu pesan dienkripsi menggunakan kunci yang sama[3].

Toko Nanda adalah salah satu toko yang ada di kota Lubuklinggau. Toko ini menjual berbagai macam jenis kebutuhan alat-alat bangunan seperti semen, besi, cat dan lain sebagainya. Selain menjual bahan-bahan bangunan, toko nanda juga menjual barang-barang kebutuhan sehari hari atau bisa di sebut juga sebagai toko manisan. Pada saat ini keamanan sistem pencatatan stok barang bangunan pada Toko Nanda masih rentan terhadap kehilangan data, karena sistem pencatatan stok barang pada toko ini masih manual, yaitu dengan cara mengumpulkan nota-nota setiap pembelannya. Untuk menjaga keamanan dan kerahasiaan data yang ada maka diperlukan sebuah sistem keamanan data dengan menggunakan metode kriptografi, agar data dalam database aman dari orang-orang yang tidak berkepentingan. Penyimpanan data atau informasi yang telah memiliki keamanan akan sulit dicuri atau tidak mudah dibaca oleh orang-orang yang tidak bertanggung jawab.

Dari permasalahan yang ada, maka dapat disimpulkan bahwa Toko Nanda memerlukan suatu sistem keamanan untuk menjaga kerahasiaan data atau informasi yang ada agar terhindar dari hal-hal yang tidak diinginkan. Untuk merealisasikan hal tersebut maka penulis bermaksud melakukan penelitian yang berjudul "*Perancangan Sistem Keamanan Data Inventori Barang di Toko Nanda Berbasis Web Menggunakan Metode Kriptografi Vigenere*".

II. TINJAUAN PUSTAKA

2.1 Perancangan

Perancangan adalah suatu proses pemilihan dan pemikiran yang menghubungkan fakta-fakta berdasarkan asumsi-asumsi yang berkaitan dengan masa datang dengan menggambarkan dan merumuskan kegiatan-kegiatan tertentu yang diyakini diperlukan untuk mencapai tujuan-tujuan tertentu dan menguraikan bagaimana pencapaiannya [4].

2.2 Sistem

Sistem didefinisikan sebagai sekumpulan prosedur yang saling berkaitan dan saling terhubung untuk melakukan suatu tugas bersama-sama. Secara garis besar, sebuah sistem informasi terdiri atas tiga komponen utama. Ketiga komponen tersebut mencakup *software*, *hardware*, dan *brainware*. Ketiga komponen ini saling berkaitan satu sama lain[5].

2.3 Keamanan Data

Keamanan data menjadi hal yang sangat penting pada saat ini karena untuk setiap pengambilan keputusan, kebijakan harus berdasarkan data. Banyak data yang berisikan informasi penting dan terbatas untuk diketahui pihak yang terkait saja. Faktor keamanan data menjadi sangat penting dan harus diperhatikan. Salah satu cara untuk meningkatkan keamanan data diperlukan kriptografi dengan metode enkripsi[1].

2.4 Kriptografi

Kriptografi pada awalnya dijabar - kan sebagai ilmu yang mempelajari bagaimana menyembunyikan pesan. Namun pada pengertian modern kriptografi adalah ilmu yang bersandarkan pada teknik matematika untuk berurusan dengan keamanan informasi seperti kerahasiaan, keutuhan data dan otentikasi entitas. Jadi pengertian kriptografi modern adalah tidak saja berurusan hanya dengan penyembunyian pesan namun lebih pada

sekumpulan teknik yang menyediakan keamanan informasi [2].

2.5 Vigenere

Vigenere cipher adalah salah satu algoritma kriptografi klasik yang diperkenalkan pada abad 16 atau kira-kira pada tahun 1586. Algoritma kriptografi ini dipublikasikan oleh seorang diplomat dan juga kriptologis yang berasal dari Prancis, yaitu Blaise de Vigenere, namun sebenarnya algoritma ini telah digambarkan sebelumnya pada buku *La Cifra del Sig. Giovan Batista Belaso*, sebuah buku yang ditulis oleh Giovan Batista Belaso, pada tahun 1553.

Cara kerja dari *Vigenere cipher* ini mirip dengan *Caesar cipher*, yaitu mengenkripsi plainteks pada pesan dengan cara menggeser huruf pada pesan tersebut sejauh nilai kunci pada deret alphabet. *Vigenere cipher* adalah salah satu algoritma kriptografi klasik yang menggunakan metode substitusi abjad majemuk. Substitusi abjad-majemuk mengenkripsi setiap huruf yang ada menggunakan kunci yang berbeda, tidak seperti *Caesar cipher* yang menerapkan metode substitusi abjad-tunggal yang semua huruf di suatu pesan dienkripsi menggunakan kunci yang sama.

Model matematika dari enkripsi pada algoritma *Vigenere cipher* ini adalah seperti berikut :

$$C_i = E_k(M_i) = (M_i + K_i) \text{ mod } 26$$

Dan model matematika untuk deskripsi adalah :

$$M_i = D_k(C_i) = (C_i - K_i) \text{ mod } 26$$

Keterangan :

C : cipherteks

M : Plainteks

K : Kunci

Contoh dari penerapan algoritma *Vigene cipher* adalah jika kita memiliki sebuah plainteks yang ingin di enkripsi :

MAKALAH KRIPTOGRAFI

Dan kita menggunakan kunci :
TUGAS

Maka plainteks akan dienkrpsi dengan cara :

Plainteks : MAKALAH KRIPTOGRAFI

Kunci: TUGASTU GASTUGASTUG

Cipherteks : FUQADTB

QRAINUGJTZO

Huruf pada kunci akan dikonveksi menjadi sebuah nilai, misalnya A=0, B=1, sampai dengan Z=25. Setelah itu prosesnya sama seperti caessar cipher dimana setiap huruf plainteks akan digeser sejauh nilai kunci yang posisinya bersesuaian[3].

2.6 Penelitian Relevan

Beberapa penelitian yang menjadi referensi penelitian ini adalah :

1. Penelitian yang dilakukan oleh Efrandi, Asnawati, Yupiyanti program studi teknik informatika fakultas ilmu computer universitas dehasen Bengkulu dengan judul *aplikasi kriptografi menggunakan algoritma vigenere cipher*. Jurnal media infotama vol. 10 no. 2, September 2014. Semua informasi dikirim dengan bebas melalui suatu jaringan dengan tingkat keamanan yang relative rendah. Untuk itulah peranan teknologi keamanan informasi benar-benar dibutuhkan. Salah satu cara yang bisa digunakan adalah menyandikan (mengenkrpsi) informasi atau data rahasia yang dikirim, sehingga walupun pihak yang tidak berkepentingan dapat membaca informasi tersebut, pihak tersebut tetap sulit bahkan tidak dapat memahami isi informasi tersebut.
2. Penelitian yang dilakukan oleh Alfa Vionita, Dyah Purboningsih Pendidikan Matematika (Pasca sarjana, Universitas Negeri Yogyakarta) dengan judul *Penggunaan Metode Enkrpsi Vigenere dan MD5 dalam*

Proses Pengamanan Pesan. Seminar nasional matematika dan pendidikan matematika 2016. Pengiriman *e-mail* sangat ekonomis karena tidak memerlukan biaya banyak untuk ongkos dijalan. *E-mail* juga dapat mengunggah data dengan kapasitas yang lebih besar dibandingkan dengan aplikasi yang lain. Namun selain itu semua ada beberapa kekurangan saat mengirim *e-mail* salah satunya yaitu tentang keamanan proses pengiriman yaitu penyadapan, penipuan, atau bahkan pencurian akun pengguna *e-mail* untuk digunakan hal-hal yang merugikan pengguna. Maka diperlukan suatu sistem yang dapat mengamankan pesan tersebut agar sampai kepada penerima pesan secara utuh.

III. METODOLOGI PENELITIAN

3.1 Metode Pengumpulan Data

3.1.1 Data Primer

Metode pengumpulan data yang dilakukan dalam penelitian ini adalah sebagai berikut:

- 1) Pengamatan (*Observasi*)
- 2) Wawancara (*Interview*)
- 3) Dokumentasi

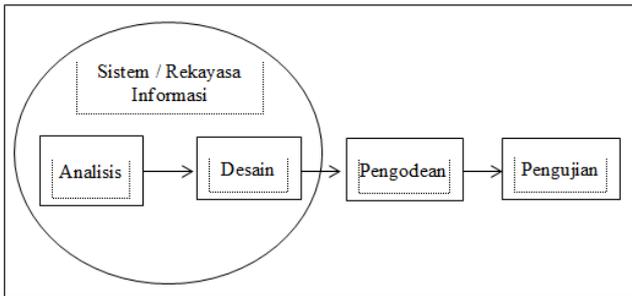
3.1.2 Data Sekunder

Data Sekunder ini dilakukan dengan pengambilan dan pengumpulan data serta memahami baik dari bahan-bahan kuliah, buku-buku relevan yang masih berhubungan dengan judul penulis teliti, serta dari hasil penjelajahan (*Browsing*) di *internet* yang berhubungan dengan penelitian ini.

3.2 Metode Pengembangan Sistem

Dalam mengembangkan sistem, penulis menggunakan metode *waterfall*. Alasan kenapa menggunakan sistem ini karena metode ini memiliki langkah-langkah yang sesuai dengan rancangan penulis. Dimana dalam pengembangan ini

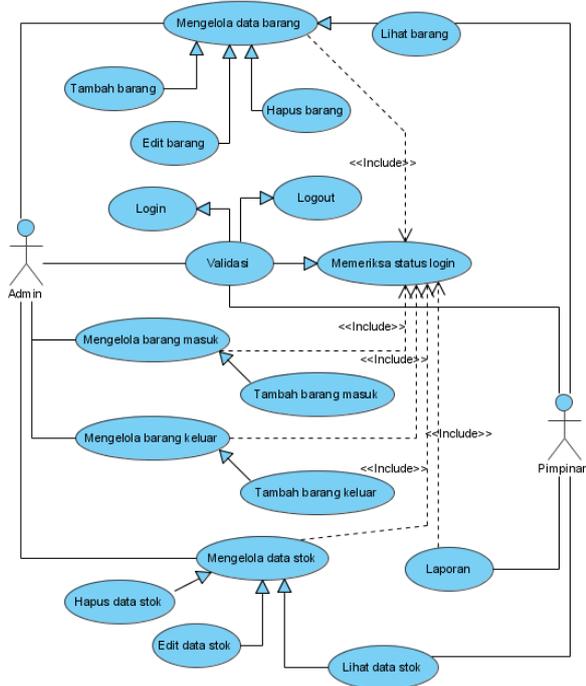
penulis merancang sebuah sistem secara bertahap dimulai dari analisis, desain, pengodean, dan pengujian.



Gambar 1. Metode Waterfall

3.3 Desain Sistem

3.3.1 Use case Diagram



Gambar 2. Use case Diagram

3.3.2 Rancangan Sistem

1. Halaman Admin

a. Halaman Data Barang

HEADER				
Data Barang	Barang Masuk	Barang Keluar	Data Stok	Logout
+Tambah Data+				
No	Kode	Nama Barang	Ukuran	Aksi
FOOTER				

Gambar 3. Halaman Barang

b. Halaman Barang Masuk

HEADER					
Data Barang	Barang Masuk	Barang Keluar	Data Stok	Logout	
+Tambah Data+					
No	Kode	Nama Barang	Ukuran	Tanggal	Jumlah
FOOTER					

Gambar 4. Halaman Barang Masuk

c. Halaman Barang Keluar

HEADER					
Data Barang	Barang Masuk	Barang Keluar	Data Stok	Logout	
+Tambah Data+					
No	Kode	Nama Barang	Ukuran	Tanggal	Jumlah
FOOTER					

Gambar 5. Halaman Barang Keluar

d. Halaman Stok Barang

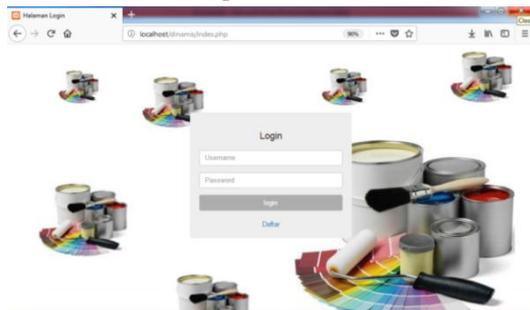
HEADER				
Data Barang	Barang Masuk	Barang Keluar	Data Stok	Logout
No	Kode	Nama Barang	Stok	Aksi
FOOTER				

Gambar 6. Halaman Stok Barang

IV. HASIL DAN PEMBAHASAN

Berdasarkan hasil analisis dan pembahasan yang telah dilakukan, maka dihasilkan sebuah aplikasi *inventory* barang dengan keamanan data menggunakan metode kriptografi *vigenere* berbasis *web* sehingga dapat dijadikan media untuk mengamankan kerahasiaan data dari pihak-pihak yang tidak bertanggung jawab.

1. Halaman Admin
a. Halaman *Login*



Gambar 7. Halaman *Login*

b. Halaman Data Barang



Gambar 8. Halaman Barang

c. Halaman Barang Masuk



Gambar 9. Halaman Barang Masuk

d. Halaman Barang Keluar



Gambar 10. Halaman Barang Keluar

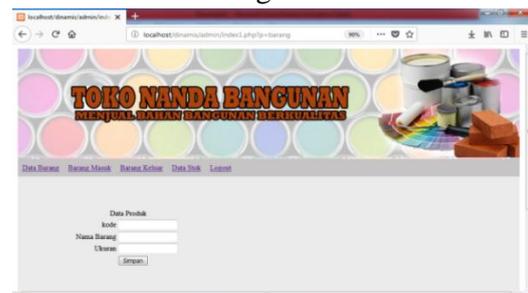
e. Halaman Stok



Gambar 11. Halaman Data Stok

2. Halaman *Input Admin*

a. Tambah Barang



Gambar 12. Halaman Tambah Barang

b. Tambah Barang Masuk



Gambar 13. Halaman Tambah Barang Masuk

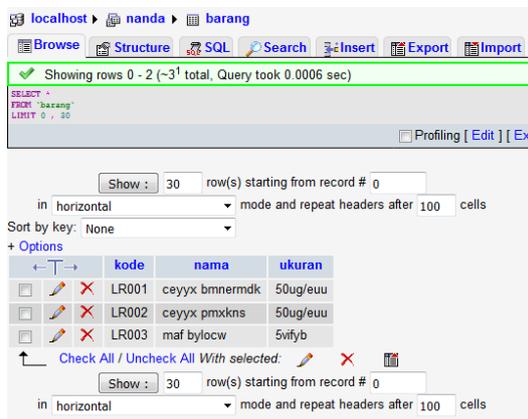
c. Tambah Barang Keluar



Gambar 14. Halaman Tambah Barang Keluar

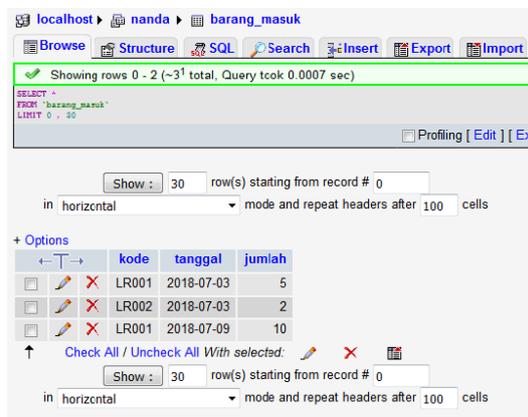
3. Tampilan Database Yang Terenkripsi

a. Tabel Barang



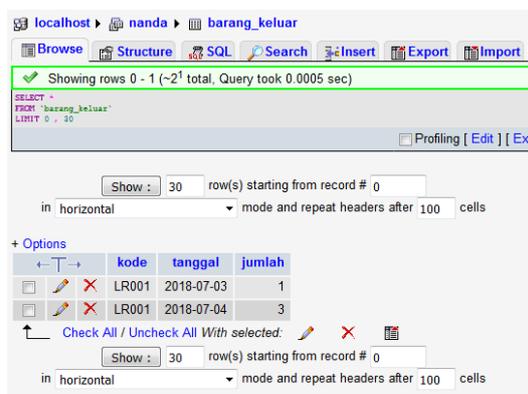
Gambar 15. Tabel Barang

b. Tabel BarangMasuk



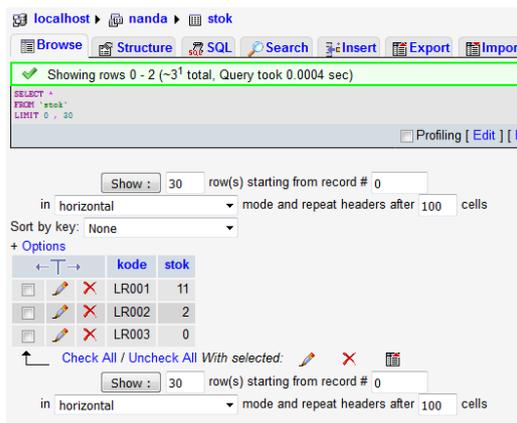
Gambar 16. Tabel Barang Masuk

c. Tabel Barang Keluar



Gambar 17. Tabel Barang Keluar

d. Tabel Stok



Gambar 18. Tabel Stok

V. KESIMPULAN

Berdasarkan pembahasan yang telah dijelaskan, maka peneliti mengambil kesimpulan yaitu dengan adanya perancangan sistem ini diharapkan :

1. Mampu menjadi media operasional bagi toko Nanda baik itu proses barang masuk maupun barang keluar.
2. Mempermudah dalam mengetahui jumlah stok barang pada toko.
3. Mampu menjaga keamanan dan kerahasiaan data yang ada.

VI. SARAN

Adapun saran yang diberikan untuk penelitian selanjutnya yaitu sebagai berikut :

1. Dapat mengkombinasikan beberapa metode kriptografi yang berbeda.
2. Aplikasi yang tidak hanya untuk mengetahui jumlah stok barang, laporan barang masuk dan barang keluar saja tetapi juga untuk pemasaran agar toko ini lebih dikenal lagi oleh masyarakat luas.

VII. DAFTAR PUSTAKA

- [1] D. A. W. Pratiwi, "Peningkatan Keamanan Data Dengan Metode Cropping Selection Pseudorandom," vol. 4, p. 3, 2016.
- [2] R. Sodikin, *Kriptografi untuk keamanan jaringan*. Yogyakarta: C.V Andi Offset, 2012.
- [3] Y. Efrandi, Asnawati, "Aplikasi Kriptografi Pesan Menggunakan Algoritma Vigenere Cipher," *Apl. Kriptografi Pesan Menggunakan Algoritma Vigenere Cipher*, vol. 10, p. 2, 2014.
- [4] S. I. Rosita Cahyaningtityas, "Perancangan Sistem Informasi Perpustakaan Pada Smp Negeri 3, Kecamatan Tulukan Kabupaten Pacitan," *Peranc. Sist. Inf. Perpustakaan Pada Smp Negeri 3, Kec. Tulukan Kabupaten Pacitan*, vol. 4, p. 2, 2015.
- [5] I. putu A. E. Pratama, *Sistem Informasi dan Implementasinya*. Informatika, 2014.