RANCANG BANGUN SISTEM KEAMANAN DATABASE DENGAN METODE KRIPTOGRAFI (Studi Kasus PT. SUMBER SOLUSI KOMUNIKASI BANDUNG)

Ardi Taryanto
Program Studi Manajemen Informatika, Politeknik Piksi Ganesha
ardipiksi@yahoo.com

ABSTRACT

This research was aimed to find out and analyze information systems procurement of goods at PT. Sources Communication Solutions as a solution to data security problems. Security systems use classical cryptographic methods by means of chipher substitution, is that each character in the plaintext will be replaced with another letter based on a particular method or formula so that it cannot be understood by other parties

The research method used is a qualitative descriptive method. While the data collection techniques are carried out by means of observation and literature study.

The concept of system design refers to data processing of procurement of goods both from inputting to reporting. So that this application design is expected to become an information system with better data security and a solution for the company.

Keywords : Information System, Data Security, and Cryptography

PENDAHULUAN

Kebutuhan akan suatu informasi yang cepat dan akurat ditunjang dengan pengolahan data yang cepat dan akurat, maka tidak salah bila sistem yang komputerisasi merupakan alat yang tepat untuk pengolahan data menjadi suatu informasi. Seiring dengan semakin ketatnya persaingan dalam dunia bisnis, keberadaan sistem yang terkomputerisasi menjadi sangat penting. Hal itu dikarenakan pengolahan data secara komputerisasi dapat memberikan kontribusi yang besar untuk kinerja suatu perusahaan. Karena menggunakan sistem yang terkomputerisasi dapat lebih efektif dan efesien dibanding dengan proses pengolahan secara manual, sehingga informasi yang dihasilkan lebih optimal dan juga dapat memajukan perusahaan kearah yang lebih baik.

Dengan kemajuan teknologi di bidang komputer, kemajuan itu diikuti pula dengan sisi buruknya dari teknologi itu sendiri, salah satunya adalah rawannya keamanan data, masalah kerahasian data menjadi salah satu aspek penting dalam suatu sistem informasi, dalam hal ini sangat penting dengan pentingnya suatu informasi tersebut dikirim dan diterima oleh orang yang berkepentingan, dengan kata lain tidak akan berguna atau bermanfaat suatu informasi yang apabila ditengah jalan informasi tersebut disadap atau dibajak oleh orang lain yang tidak berkepentingan.

Ada beberapa cara melakukan pengamanan data salah satunya adalah dengan metode kriptografi. Dalam kriptografi, data yang diproses atau diolah disamarkan sedemikian rupa sehingga meskipun data itu bisa dibaca maka tidak akan dan bisa dimengerti oleh pihak yang tidak berkepentingan. Dalam keamanan data, kriptografi mempunyai sejarah yang sangat panjang dari zaman sebelum masehi sampai sekarang ini.

Maksud dari penelitian ini adalah meningkatkan keamanan database sistem dengan meggunakan metode kriptografi di PT. Sumber Solusi Komunikasi Bandung. Sedangkan kegiatan ini bertujuan antara lain untuk mengetahui dan menganalisis sistem informasi pengadaan barang dan membuat solusi keamanan baru yang lebih efektif dan efisien.

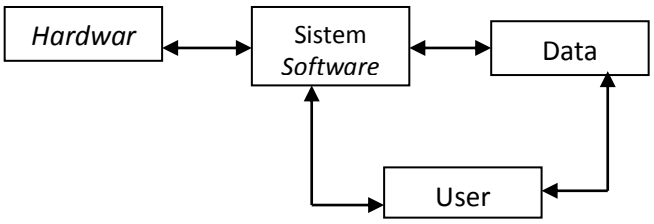
Metode yang digunakan dalam penelitian berdasarkan metode ilmiah dengan cara observasi (*observation*) pendekatan untuk mendapatkan data primer dengan cara mengamati langsung obyek datanya, wawancara (*interview*) pendekatan komunikasi (*communication approach*) yang berhubungan langsung dengan sumber data, dan studi pustaka (*library*) mengumpulkan data-data dan informasi yang berasal dari buku-buku, dokumen dan internet

STUDI LITERATUR

Definisi Sistem Informasi

Pengertian sistem informasi menurut Al-Bahra Bin Ladjamudin (2005:13), "Sistem informasi adalah suatu sistem yang dibuat oleh manusia yang terdiri dari komponen-komponen dalam organisasi untuk mencapai suatu tujuan yaitu menyajikan informasi".

Sistem informasi sendiri memiliki jumlah komponen tertentu yang terdiri dari beberapa komponen yang berbeda yaitu: manusia, data, *hardware*, dan *software*. Sebagai suatu sistem informasi, setiap komponen tersebut berinteraksi satu dengan yang lainnya membentuk satu kesatuan untuk mencapai sasaran, komponen sistem informasi dapat dilihat pada gambar berikut ini:



Gambar 1 Komponen Sistem Informasi
Sumber : Analisis dan Desain Sistem Informasi, Andi Offset , 1999

Kode ASCII

Beberapa aplikasi menggunakan data yang bukan hanya bilangan tetapi juga huruf dari alfabet dan karakter khusus lainnya. Data semacam ini disebut dengan data alfanumerik dan mungkin dapat ditunjukkan dengan kode numerik. Jika bilangan-bilangan dimasukkan dalam data, maka bilangan tersebut juga dapat ditunjukkan dengan kode khusus. Set karakter alfanumerik secara khusus mencakup 26 huruf alfabet (termasuk huruf besar dan huruf kecil), angka dalam digit sepuluh desimal, dan sejumlah simbol seperti +, =, *, $, …, dan!. Dua kode alfabet yang paling umum dipakai adalah ASCII (American Standard Code for Information Interchange) dan EBCDIC (Extended Binary Coded Decimal Interchange Code).

Data Base

Pengertian data base atau basis data yaitu "kumpulan dari item–item yang saling berhubungan satu dengan yang lainnya yang diorganisasikan berdasarkan sebuah skema atau struktur tertetu, tersimpan di hardware komputer dan software untuk melakukan manipulasi untuk kegunaan tertentu".

Jogiyanto (1999:711) mendefinisikan bahwa basis data merupakan kumpulan dari data yang saling berhubungan satu dengan yang lainnya, tersimpan diperangkat keras komputer dan digunakan perangkat lunak untuk memanipulasi"

Kriptografy

Kriptografi berasal dari bahasa Yunani, crypto dan graphia. Cypto 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 tampat lain. Kriptografi mempunyai sejarah yang sangat menarik dan panjang. Kriptografi sudah digunakan 4000 tahun yang lalu, diperkenalkan oleh orang – orang Mesir lewat hieroglyph. Jenis tulisan ini bukanlah bentuk standar untuk menulis pesan. Tujuan dari kriptografi adalah keamanan data yang dapat dijabarkan sebagai berikut:

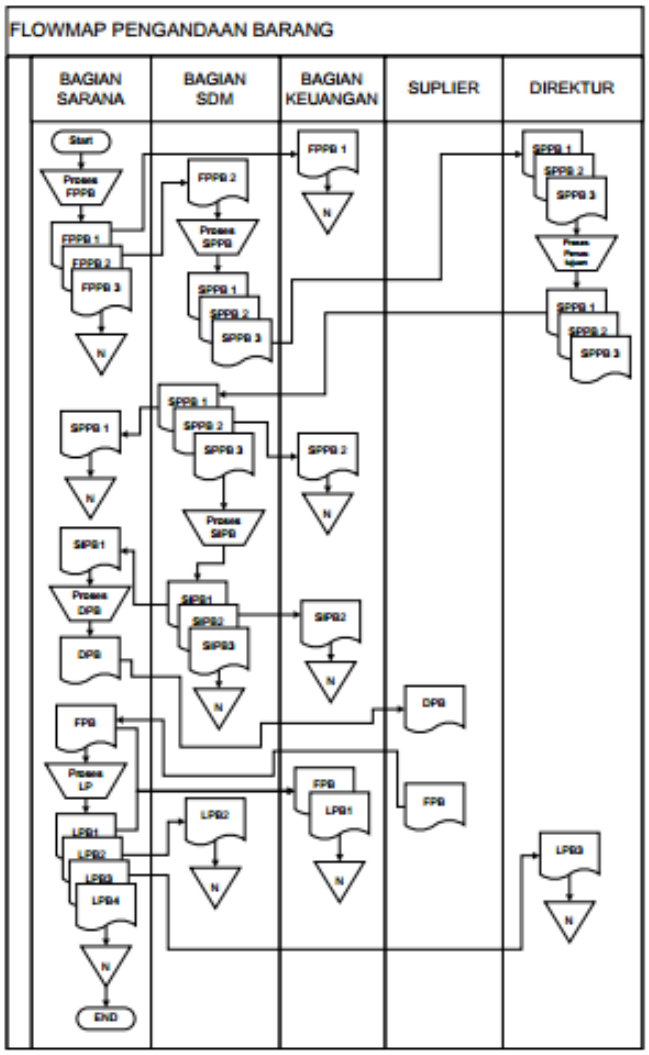
a) Kerahasiaan atau *Confidentiality* adalah menjaga agar informasi atau pesan yang ada tidak dapat dibaca oleh pihak – pihak yang tidak berhak. Di dalam kriptografi, hal ini direalisasikan dengan menyandikan pesan cyphertext.
b) Integritas Data yaitu menjamin bahwa pesan masih asli atau belum pernah dimanipulasi oleh pihak yang tidak berhak selama proses pengiriman.
c) Otentikasi atau Authentication yaitu mengidentifikasi tentang kebenaran pihak – pihak yang berkomunikasi. Hal ini berkaitan erat dengan keaslian sumber pesan.
d) Anti Penyangkalan atau Non Repudiation yang bertujuan mencegah pihak yang mengirim pesan melakukan penyangkalan terhadap pesan yang dikirimkannya

ANALISIS DAN PERANCANGAN

A. Analisis

Salah satu tahapan analisis sistem yaitu tahapan yang memberikan gambaran tentang sistem yang sedang berjalan. Penjelasan kegiatan hasil analisis sistem didiskripsikan dalam bentuk flowmap berikut :

Keterangan Flowmap Pengadaan Barang :
FPPB : Formulir Permohonan Pengadaan Barang
SPPB : Surat Persetujuan Pengadaan Barang
SIPB : Surat Izin Pengadaan Barang
DPB : Daftar Pemebelian Barang
FPB : Faktur Pembelian Barang
LPB : Laporan Pengadaan Baran

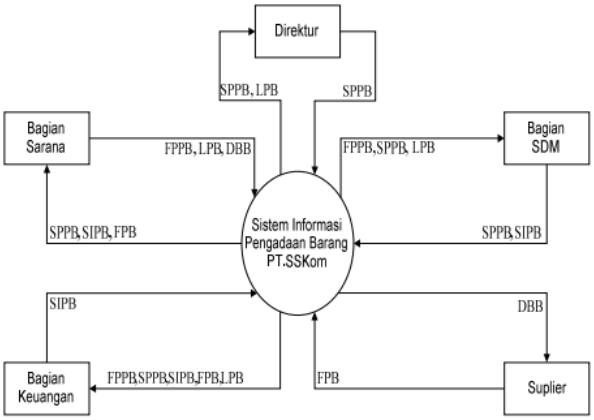


Gambar 2 Flowmap Pengadaan barang

B. Perancangan

Setelah tahap analisa sistem selesai dilakukan, maka analisa sistem telah mendapatkan gambaran jelas yang harus dikerjakan. Langkah selanjutnya adalah masuk pada tahap perancangan sistem *(system desain).*Tahap desain sistem mempunyai dua tujuan utama, yaitu untuk memenuhi kebutuhan pemakai sistem dan memberi gambaran yang jelas dan rancangan bangun yang lengkap kepada pemrograman komputer dan ahli teknik lainnya yang terlibat.

1) Diagram Konteks Perancangan

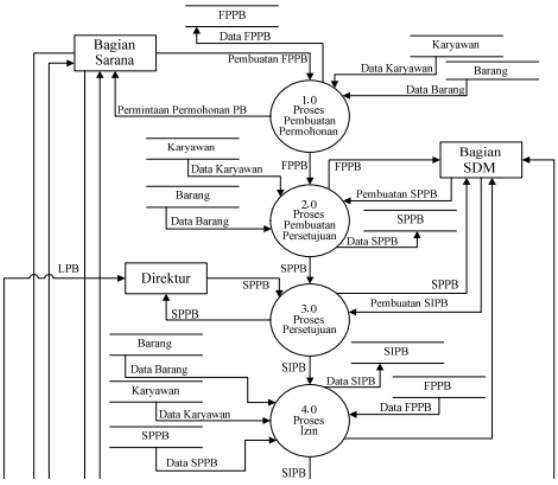


Gambar 4 Diagram Konteks Sistem informasi Pengadaan Barang

Keterangan :
FPPB : Formulir Permohonan Pengadaan Barang
SPPB : Surat Persetujuan Pengadaan Barang
SIPB : Surat Izin Pengadaan Barang
DBB : Daftar Belian Barang
FPB : Faktur Pembelian Barang
LPB : Laporan Pemebelian Barang

2) Data Flow Diagram (DFD)

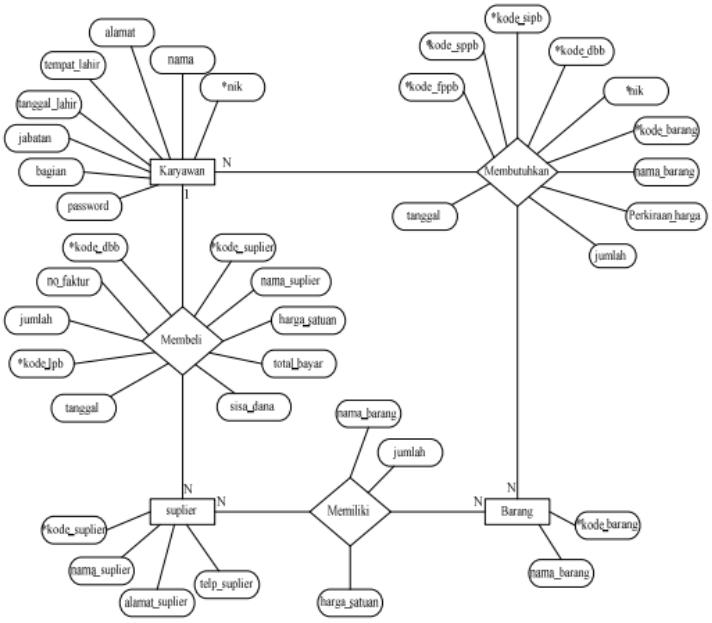
Dalam pengembangan sistem yang terstruktur dan untuk mengembangkan arus data dalam sistem yang jelas. Berikut data flow diagram sistem informasi Pengadaan Barang.



Gambar 6 Data Flow Diagram Rancangan Sistem

3) Rancangan ERD

Komponen utama pembentuk ERD yaitu entitas dan relasi, sehingga dalam hal ini diagram E-R merupakan komponen – komponen himpunan entitas dan himpunan relasi yang dideskripsikan lebih jauh melalui atribut – atribut (properti) yang menggambarkan seluruh fakta dari sistem yang ditinjau.



Gambar 6 Entity Relationships Diagram (ERD)

4) Rancangan Keamanan Database

Ada banyak macam cara untuk pengamanan data salah satunya dengan kriptografi.Kriptografi berasal dari bahasa Yunani, crypto dan graphia. Cypto 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 tampat lain. Rancangan keamanan database dengan kriptografi ini berfungsi untuk menghindari orang yang tidak berhak yang ingin mengetahui isi data dari database, sehingga bilapun orang yang tidak berhak itu dapat membuka dan melihat isi data dari database maka orang yang tidak berhak itu tidak akan mudah untuk mengerti dari isi data pada database.

Pada tahapan ini penulis merancang keamanan database mengunakan kriptografi klasik dengan cara chipher substitusi, chipher substitusi yaitu setiap karakter pada plaintext akan digantikan dengan huruf lain berdasarkan suatu cara atau rumus tertentu. Adapun rumus/algoritma untuk proses Enkripsi data yang digunakan sebagai berikut :

$$C = E(P) = (P + K + P_i) \bmod 256$$

Dan rumus/algoritma untuk proses Deskripsi data yang digunakan sebagai berikut :

$$P = D(C) = (C – K – C_i) \bmod 256$$

Dengan ketentuan dimana C adalah Chipertext, E adalah Enkripsi, P adalah Plaintext, dan K adalah pergeseran karakter sesuai dengan yang telah ditentukan. Dengan rumus/algoritma diatas dapat digambarkan proses enkripsi pada tabel berikut.

Tabel 1 Proses Enkripsi

Plaintext	A	B	C	D	E	F	G	H	I	J	P_i
Pergeseran	4+1	4+2	4+3	4+4	4+5	4+6	4+7	4+8	4+9	4+10	4+*i*
Chipertext	F	H	J	L	N	P	R	T	V	X	C_i

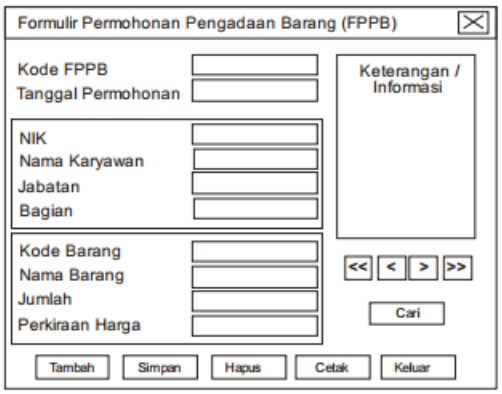
Dan untuk proses dekripsi dapat digambarkan pada tabel berikut

Tabel 2 Proses Dekripsi

Chipertext	F	H	J	L	N	P	R	T	V	X	C_i
Pergeseran	4 - 1	4 - 2	4-3	4-4	4-5	4-6	4-7	4-8	4-9	4-10	4-*i*
Plaintext	A	B	C	D	E	F	G	H	I	J	P_i

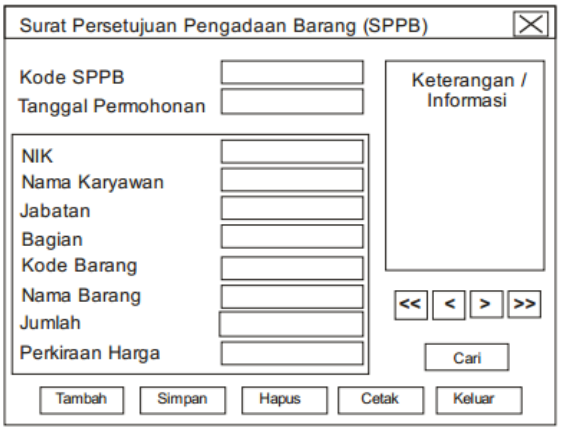
Jadi pada rancangannya ini membuat data yang ada dalam database terenkripsi sehingga untuk melihat deskripsi datanya diharuskan untuk masuk/login ke dalam program.

5) Rancangan Form Formulir Permohonan Pengadaan Barang (FPPB



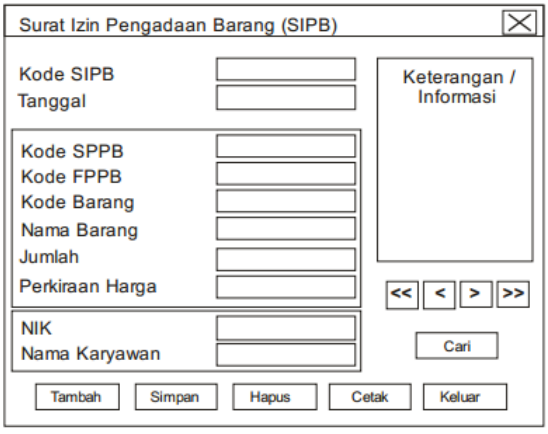
Gambar 7 Rancangan Tampilan FPPB

6) Rancangan Form Surat Persetujuan Pengadaan Barang (SPPB



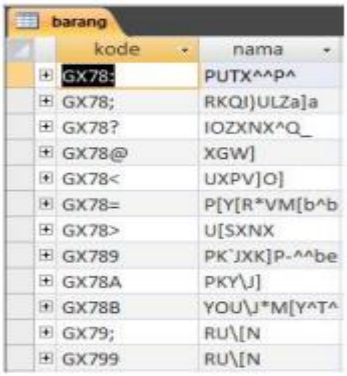
Gambar 8 Rancangan Tampilan SPPB

7) Rancangan Form Surat Izin Pengadaan Barang (SIPB)



Gambar 9 Rancangan Tampilan SIPB

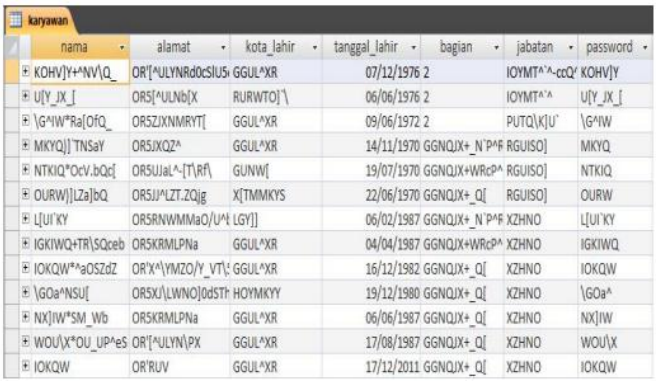
8) Tampilan Enkripsi Data Barang
Hasil dari proses enkripsi pada form data barang, hasil enkripsi ini dapat dilihat pada database, adapun hasil enkripsi data barang dapat dilihat pada gambar berikut ini:


barang

kode	nama
GX78:	PUTX^^P^
GX78;	RKQI)ULZa]a
GX78?	IOZXNX^Q_
GX78@	XGW]
GX78<	UXPV]O]
GX78=	P[Y[R*VM[b^b
GX78>	U[SXNX
GX789	PK`JXK]P-^^be
GX78A	PKY\J]
GX78B	YOU\J*M[Y^T^
GX79;	RU\[N
GX799	RU\[N

Gambar 10 Tampilan Enkripsi Data Barang

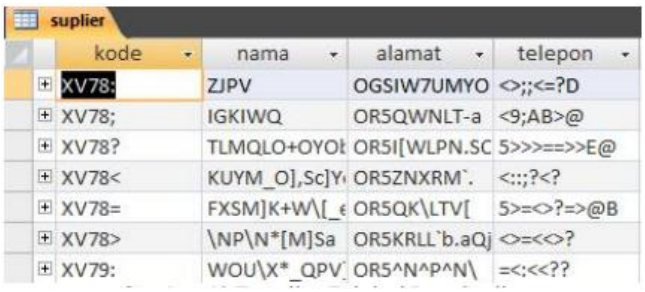
9) Tampilan Enkripsi Data Karyawan
Hasil dari proses enkripsi pada form data karyawan dapat dilihat pada database, sedangkan hasil enkripsi data karyawan dapat dilihat pada gambar berikut ini


karyawan

nama	alamat	kota_lahir	tanggal_lahir	bagian	jabatan	password
KOHV]Y+^NV\Q_	OR'[^ULYNRd0cSlU5	GGUL^XR	07/12/1976 2		IOYMT^`^-ccQ'	KOHV]Y
U[Y_JX_[	OR5[^ULNb[X	RURWTO]`\	06/06/1976 2		IOYMT^`^	U[Y_JX_[
\G^IW*Ra[OfQ_	OR5ZJXNMRYT[	GGUL^XR	09/06/1972 2		PUTQ\K]U`	\G^IW
MKYQ]]`TNSaY	OR5JXQZ^	GGUL^XR	14/11/1970	GGNQJX+_N`P^R	RGUISO]	MKYQ
NTKIQ*OcV.bQc[	OR5UJaL^-[T\Rf\	GUNW[	19/07/1970	GGNQJX+WRcP^	RGUISO]	NTKIQ
OURW]]LZa]bQ	OR5JJ^LZT.ZQjg	X[TMMKYS	22/06/1970	GGNQJX+_Q[	RGUISO]	OURW
L[UI`KY	OR5RNWMMaO/U^I	LGY]]	06/02/1987	GGNQJX+_N`P^R	XZHNO	L[UI`KY
IGKIWQ+TR\SQceb	OR5KRMLPNa	GGUL^XR	04/04/1987	GGNQJX+WRcP^	XZHNO	IGKIWQ
IOKQW*^aOSZdZ	OR'X^\YMZO/Y_VT\	GGUL^XR	16/12/1982	GGNQJX+_Q[	XZHNO	IOKQW
\GOa^NSU[	OR5X/\LWNO]0dSTI	HOYMKYY	19/12/1980	GGNQJX+_Q[	XZHNO	\GOa^
NX]IW*SM_Wb	OR5KRMLPNa	GGUL^XR	06/06/1987	GGNQJX+_Q[	XZHNO	NX]IW
WOU\X*OU_UP^eS	OR'[^ULYN\PX	GGUL^XR	17/08/1987	GGNQJX+_Q[	XZHNO	WOU\X
IOKQW	OR'RUV	GGUL^XR	17/12/2011	GGNQJX+_Q[	XZHNO	IOKQW

Gambar 11 Tampilan Enkripsi Data Karyawan

10) Tampilan Enkripsi Data Suplier
Hasil dari proses enkripsi pada form data suplier, hasil enkripsi ini dapat dilihat pada database, adapun hasil enkripsi data suplier dapat dilihat pada gambar berikut ini :


suplier

kode	nama	alamat	telepon
XV78:	ZJPV	OGSIW7UMYO	<>;;<=?D
XV78;	IGKIWQ	OR5QWNLT-a	<9;AB>@
XV78?	TLMQLO+OYOI	OR5I[WLPN.SC	5>>>==>>E@
XV78<	KUYM_O],Sc]Y	OR5ZNXRM`.	<:::?<?
XV78=	FXSM]K+W\[_€	OR5QK\LTV[	5>=<>?=>@B
XV78>	\NP\N*[M]Sa	OR5KRLL`b.aQj	<>=<<>?
XV79:	WOU\X*_QPV	OR5^N^P^N\	=<:<<??

Gambar 12 Tampilan Enkripsi Data Suplier

11) Tampilan Enkripsi Data FPPB
Hasil dari proses enkripsi pada form data


fppb

kode_fppb	tanggal	nik	kode_baran	jumlah	perkiraan_h
KVWJ9:?	24/11/2011	XL78<	GX78@	8	;6789
KVWJ9:@	27/11/2011	XL78<	GX78;	6	86789:
KVWJ9:=	22/11/2011	RP78;	`	6	96789:;
KVWJ9:>	22/11/2011	IQ78:	GX78>	68	76789
KVWJ9:A	27/11/2011	XL78=	GX78>	7	8678
KVWJ9:B	30/11/2011	IQ78:	GX799	6	7;789
KVWJ9:C	06/12/2011	XL78=	GX78<	6	9;789:
KVWJ9:D	07/12/2011	XL78>	GX78?	6	6;789:

FPPB, hasil enkripsi ini dapat dilihat pada database, adapun hasil enkripsi data FPPB dapat dilihat pada gambar berikut ini:

Gambar 13 Tampilan Enkripsi Data FPPB

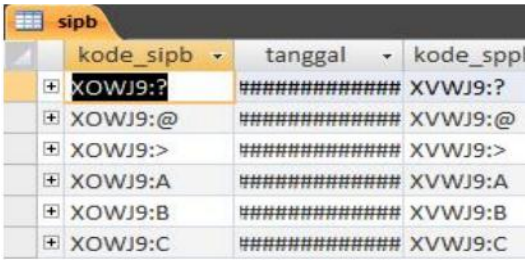
12) Tampilan Enkripsi Data SPPB
Hasil dari proses enkripsi pada form data SPPB, hasil enkripsi ini dapat dilihat pada database, adapun hasil enkripsi data SPPB dapat dilihat pada gambar berikut ini:


sppb

kode_sppb	tanggal	kode_fp
XVWJ9:?	06/12/2011	KVWJ9:?
XVWJ9:@	06/12/2011	KVWJ9:@
XVWJ9:=	22/11/2011	KVWJ9:=
XVWJ9:>	22/11/2011	KVWJ9:>
XVWJ9:A	06/12/2011	KVWJ9:A
XVWJ9:B	06/12/2011	KVWJ9:B
XVWJ9:C	06/12/2011	KVWJ9:C

Gambar 14 Tampilan Enkripsi Data SPPB

13) Tampilan Enkripsi Data SIPB
Hasil dari proses enkripsi pada form data SIPB, hasil enkripsi ini dapat dilihat pada database, adapun hasil enkripsi data SIPB dapat dilihat pada gambar berikut ini


sipb

kode_sipb	tanggal	kode_spp
XOWJ9:?	##########	XVWJ9:?
XOWJ9:@	##########	XVWJ9:@
XOWJ9:>	##########	XVWJ9:>
XOWJ9:A	##########	XVWJ9:A
XOWJ9:B	##########	XVWJ9:B
XOWJ9:C	##########	XVWJ9:C

Gambar 15 Tampilan Enkripsi Data SIPB

PENUTUP

Berdasarkan analisis perancangan sebagai strategi dalam pengembangan sistem keamanan database, maka dapat diambil kesimpulan sebagai berikut :

1. Sistem informasi yang berjalan saat ini menggunakan microsoft office. Namun masukan dan pengolahan data dikatakan manual karena tidak terorganisir dengan baik, dan untuk mengolah data menjadi informasi dibutuhkan waktu yang relatif lama sehingga proses ini kurang efektif dan efisien.
2. Keamanan data kurang optimal, sehingga diperlukan sistem keamanan guna menjaga data-data penting dan rahasia perusahaan agar tidak bisa diakses atau dibaca dan dimanipulasi oleh pihak luar.
3. Rancangan aplikasi sistem keamanan pengadaan barang dengan kriptografi diharapkan menjadi solusi bagi perusahaan.

REFERENSI

Al-Bahra Bin Ladjamudin. ”Analisis dan Desain Sistem Informasi”. Graha Ilmu: Yogyakarta, 2005

Al-Bahra Bin Ladjamudin. ”Rekayasa Perangkat Lunak”. Graha Ilmu : Yogyakarta, 2006

Al Fatta, Hanif. ”Analisis dan Perancangan Sistem Informasi”. ANDI : Yogyakarta, 2007

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

Fathansyah. ”Basis Data”, Bandung: Informatika.2002

Andi. ”Memahami Model Enkripsi dan Security Data”, Yogyakarta: Wahana Komputer. 2003

ANONIMUS, ASCII Table and Extended ASCII Table, www.asciitable.com, 22 Maret 2004

PFLEEGER, CHARLES P., ”Security in Computing”. 2nd Edition. Upper Saddle River: Prentice Hall, 1997