SIMULASI PENGEMBANGAN KUNCI ALGORITMA MENGGUNAKAN MULTI KUNCI DESKRIPSI

Fathoni Mahardika[1]
[1]*Dosen Manajemen Informatika, STMIK Sumedang*
fathoni@stmik-sumedang.ac.id

ABSTRAK

Tujuan penelitian ini adalah mengetahui kekurangan dan kelebihan algoritma yang menggunakan satu kunci. Selanjutnya dapat membentuk algoritma kunci kriptografi dengan menggunakan banyak kunci deskripsi.Dan dapat mengetahui sejauh mana keamanan yang menggunakan algoritma dengan menggunakan banyak kunci deskripsi.Metode Peneltian ini adalah menggunakan metodologi prototype. Dengan menggunakan metode ini penulis meelakukan tahapan yaitu pengumpulan kebutuhan ,perancangan ,Building prototype ,Evaluasi ,Refining,evaluasi dan Enginer product . Dengan melakukan penelitian ini didapatkan beberapa persamaan sebagai dasar dari algoritma yang digunakan.Dan telah di uji coba terhadap sistem informasi keuangan di kamous STMIK Sumedang.Kesimpulan penerapan algoritma ini juga mampu membentuk dimana algoritma simetris menjadi asimetris. Dengan menggunakan algortima ini di daptkan tiga kunci pada setiap user.Dengan menggunakan algoritma ini juga di dapatkan hasil dimana kriptografi bergantung pada kuncinya.

Kata Kunci :*pengembangan, algoritma, kunci, kriptografi, multi, kunci, deskripsi*

PENDAHULUAN

Kemajuan teknologi komputer sangat berpangaruh terhadap perkembangan zaman pada era modern seperti ini.Pada saat ini komputer sudah merambah ke semua aspek kehidupan manusia baik itu di bidang pendidikan, perkantoran, militer, kepolisian.Komputer juga sering di jadikan sebagai media penyimpanan data. Bahkan data-data penting suatu organisasi sering disimpan di media penyimpanan komputer.

Dengan kemampuan komputer sebagai media penyimpan data-data penting, banyak organisasi baik swasta maupun pemerintahan yang menggunakan komputer sebagai media penyimpannan data.Namun karena persaingan antar organisasi sering sekali terjadi pencurian data yang dilakukan oleh organisasi yang bersaing. Selain karena alasan persaingan organisasi masih banyak alasan yang mendasari pencurian data yang dilakukan seperti kepentingan individu, alasan ekonomi dan dendam yang meliputi banyak bidang seperti aspek politik, pemerintahan, kepolisian, milter, kesehatan, pendidikan.

Masalah keamanan data merupakan salah satu aspek terpenting dari sebuah system informasi .Masalah keamanan sering kali kurang mendapat perhatian dari para perancang dan pengelola sistem imformasi.Karena hal yang demikian itulah sering sekali pencurian data mudah dilakukan dan sering dilakukan oleh pihak tertentu yang memiliki tujuan tertentu.

Banyak contoh dari fenoma yang terjadi kasus pencurian data, diantaranya:

a. Wikileaks: mengungkapkan dokumen-dokumen rahasia negara dan perusahaan kepada publik melalui situs web.
b. Kasus penyadapan percakapan ponsel.
c. Penyadapan yang dilakukan antara Negara

Kasus pencurian data sebenarnya bukan hal yang baru, sebelum adanya komputer pencurian data sudah dilakukan, oleh sebab itu dilakukan pengemanan sebuah pesan atau data 4000 tahun yang lalu yang diperkenalkan oleh orang-orang mesir untuk mengirim pesan ke pasukan militer yang berada di lapangan dan supaya pesan itu tidak dapat dibaca oleh pihak musuh.

Kebutuhan akan kriftografi pada saat ini sangat tinggi. Dengan berkembangan teknologi digital yang semakin pesat dan semakin banyaknya keamanan informasi menjadi hal utama untuk menggunakan suatu sistem komputer.Hal ini diperkuat dengan mudahnya masuk kedalam suatu jaringan tertentu sehingga akses jaringan tidak lagi aman. Kriptografi adalah jawaban dari pengaman informasi walau jaringan

tersebut sudah tidak lagi aman karena kriptografi menjaga kerahasian isi dari informasi tersebut, Pada hal ini kriptografi ditempatkan sebagi pengaman paling dasar dari informasi tersebut.Kriftografi di Negara maju seperti Amerika merupakan aspek penting dalam perkembangan teknologinya setiap tahunnya sering dilakukan lomba algortima pembuatan kriftografi. Hal ini dilakukan untuk mengupgrade sistem keamanan data dengan mengoptimalkan kriptografi. Dengan mengupgrade kriptografi tersebut dengan diharapkan pengaman data akan terjaga,karena para pencuri datapun selalu mengincar dari algortima kriptografi yang digunakan untuk memecahkan algoritma tersebut. Selanjutnya jika algoritma tersebut sudah diketahui akan mudah untuk melakukan pencurian data tersebut., itulah yang mendasari kenapa kriptografi harus sering diupgrade.

Algoritma kriptografi merupakan langkah-langkah yang dilakukan secara logis bagaimana menyembunyikan pesan dari orang-orang yang tidak berhak atas pesan tersebut sehingga kerahasiaan informasi dari pengirim ke penerima dapat dijaga.Namun dari sekian rumitnya perhitungan algortima kriptografi akan membutuhkan waktu dan tenaga yang tidak sedikit untuk membentuk algortima tersebut. Algortima kriptografi yang memiliki kunci *public* dan kunci *private* yang berbeda jika dilakukan perhitungan pada kunci *public*akan menghasilkan satu kunci *private*.jadi dalam algoritma kriptografi satu kunci *public* akan menghasilkan satu kunci *private*.

Pada dasarnya setiap algoritma kriptografi yang dibuat akan meghasilkan satu kunci enkripsi untuk satu kunci deskripsi. Hal ini dilakukan untuk menjaga kemanan dalam pembacaan pesan.Duplikasi kunci deksripsi yang menjadi ancaman jika terjadi penggandaan kunci deskripsi.Namun jika dilhat dari segi efektifitasnya jika satu kunci enkripsi meghasilkan satu kunci deskrpisi bisa kurang efektif, jika dihadapkan dalam suatu kondisi yang dimana dibutuhkan banyak kunci deskrpsi. Misalnya satu pengirim akan mengrimkan pesan terhadap banyak N penerima pesan, maka pengirim haruslah memeliki sebanyak N kunci enkripsi.

Sebagai contoh misalnya dalam susunan organisasi, dimana *owner* yang posisi paling atas akan memiliki banyak anak buah di bawahnya. Jika *owner* memiliki pesan yang berbeda-beda pada anak buahnya . Dari pemasalahan diatas menggunakan algoritma yang umumnya, maka*owner* harus memiliki kunci enkripsi sebanyak anak buah yang dimilikinya. Untuk mengatasi hal tersebut dibutuhkan pegembangan kunci kriptografi, dimana pada pembangkitan kunci bisa membuat 1 kunci *public* dengan menghasilkan banyak kunci *private* dengan tanpa megurangi nilai kerahasian sebuah kunci dan keamanan kunci serta data tersebut.maka dengan hal tersebut dilakukanlah ***Pengembangan Algoritma Kunci Kriptografi Dengan Menggunakan Multi Kunci Deskripsi.***

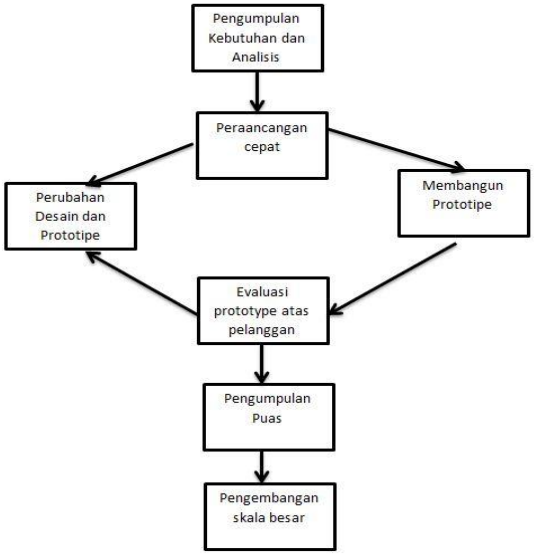
RUMUSAN MASALAH

Dari latar belakang yang telah di jelaskan ,maka yang dapat diambil perumusan masalah yaitu bagaimana membentuk algoritma kunci kriptografi yang efektif dimana satu kunci enkripsi yang akan menghasilkan banyak kunci deskripsi yang aman.

METODOLOGI

Metodologi Pengembangan Model yang digunakan adalah Model *Prototype*Metodologi pengembangan model *Prototype* adalah suatu proses mencari sesuatu secara sistematis dalam waktu yang relatip lama dengan menggunakan metode ilmiah serta aturan yang berlaku.

Analisis data dilakukan secara kualitatif maupun kuantitatif dengan tujuan untuk memperoleh masukan dan gambaran jelas yang secara skematik dapat digambarkan pada gambar 1 :



Gambar 1. Metodologi Pengembangan Model

Prototyping adalah salah satu pendekatan dalam rekayasa perangkat lunak yang secara langsung mendemonstrasikan bagaimana sebuah perangkat lunak atau komponen-komponen perangkat lunak akan bekerja dalam lingkungannya sebelum tahapan konstruksi actual.Langkah kerja model *Prototype* dari gambar diatas adalah:

a. *Requiremen Gathering & Refinement* atau pengumpulan kebutuhan dan menganalisi kebutuhan
b. *Quick* Desain atau perancangan dilakukan cepat dan rancangan mewakili semua aspek penelitian algoritma yang diketahui, dan rancangan ini menjadi dasar *Prototype*.
c. *Building Prototype* tahap ini akan membangun sebuah versi *Prototype* yang dirancang kembali dimana masalah-masalah tersebut diselesaikan.
d. Evaluasi *Prototype* pada tahap ini terjadi evaluasi oleh pengguna terhadap model yang dikembangkan guna memenuhi algoritma yang dihasilkan.
e. *Refining Prototype* tahap ini akan merubah rancangan dan prortotyppe yang sudah di analisa
f. Apabila terjadi kesalahan atau kekurangan maka di ulangi ke langah evaluasi *Prototype*.
g. *Enginer* product selanjutnya pada tahap selanjutnya dibuatkan kembali *software* yang telah di perbaiki.

PEMBAHASAN

Pendefinisian Sistem

Algoritma yang akan dipakai merupakan pengembangan yang dapat digunakan oleh lebih satu orang pengguna. Dengan menggunakan sistem multiuser dapat menggunakan satu kunci master namun dapat digunakan oleh banyak operator dengan password yang berbeda-beda.

Algortima ini menggunakan 2 operasi matematika pada saat melakukan pengembangan kunci yaitu :

a. Modulus digunakan untuk menemukan nilai pengurang pada nilai yang telah dipilih sebagai kunci penerima pesan . (disimbolkan dengan “b”)
b. Divisor digunakan untuk menemukan nilai pembagi pada nilai yang telah dipilih dengan kata lain nilai div ini merupakan berbading terbalik dengan nilai yang dipilih. (disimbolkan dengan “c”)

Selain menggunakan operasi matematika algoritma ini juga memilki 3 nilai,yaitu:

a. Nilai pilihan merupakan nilai acak yang digunakan sebagai kunci yang akan diberikan kepada user atau dengan kata lain adalah kunci ke-1. (disimbolkan dengan : a)
b. Nilai proses yaitu dua bilangan yang didapatkan setelah melakukan operasi div dan mod yang. Nilai proses ini juga adalah kunci ke-2 dan kunci ke-3. (disimbolkan dengan : b, c)
c. Kunci master merupakan kunci utama yang merupakan pusat dari semua kunci yang dibagi.(disimbolkan dengan :e)

Maka dari pendifinisan di atas di dapat persamaan sebagai berikut :

Diketahui:

a mod e =b

a div e = c

maka:

i. a = (e.c) +b
   e.c = a-b
ii. e = $\frac{a-b}{c}$ berlaku jika a ≥ e
iii. c = $\frac{a-b}{e}$
iv. b = a-(e.c)

Perilaku Sistem

a. Fungsi pembangkit kunci

Skenario yang dapat dibuat untuk fungsi level pembangkit kunci adalah :

Tabel 1. Fungsi Level Pembangkit Kunci

Identifikasi	
Nomor	PN-key-01
Nama	Pembangkit Kunci
Tujuan	Menghasilkan kunci deskripsi dan enkripsi master.
Aktor	Administrator
Skenario Utama	
Aksi Aktor	**Reaksi Sistem**
1. Memasukan nilai kunci master.	2. system akan mengubah nilai decimal yang di inputkan menjadi bilangan biner
	3. nilai binner yang dhasilkan akan disimpan di database

	sebagai kunci utama
Kondisi Akhir	Akan meghasilkan kunci master

b. Fungsi pengembang kunci

Skenario yang dapat dibuat untuk fungsi level pengembang kunci adalah:

Tabel 2. Fungsi Level Pengembang Kunci

Identifikasi	
Nomor	PN-key-02
Nama	pengembang kunci
Tujuan	Menghasilkan kunci lebih dari satu .
Aktor	Administrator , operator
Skenario Utama	
Aksi Aktor	**Reaksi Sistem**
1. opretor memasukan nilai plihannya (kunci ke-1/a).	2. nilai tersebut akan dikirim kepada admin.
3. Administrator akan memvalidasi nilai tersebut kedalam nilai master.	kunci akan di formulasikan dengan nilai pilihan operator yang sudah di validasi dengan menggunkan mod dan div kepada nilai master menghasilkan 2 nilai yaitu “b “ dan “c”.
6. operator akan mendapatkan nilai yang dimasukan dan nilai”b” sebagai kuncinya.	Nilai “b” akan disimpan kedalam database dan nilai “c” akan dimiliki oleh operator.
Kondisi Akhir	Akan meghasilkan key yang berbeda-beda.

c. Fungsi enkripsi data

Skenario yang dapat dibuat untuk fungsi level enkripsi data adalah :

Tabel 3. Fungsi Level Eknripsi Data

Identifikasi	
Nomor	PN-key-03
Nama	enkripsi data
Tujuan	Mengubah plain text menjadi chipper text.
Aktor	Operator
Skenario Utama	
Aksi Aktor	**Reaksi Sistem**
1.user memasukan data-data plaintext	2. merubah data-data kedalam bentuk ascii
3.user memasukan kunci ke-1 dan kunci ke-2	4. Sistem akan meload nilai kunci ke-3 atau nilai c.
	5 Sistem akan mengubah plaintext kedalam chipertext dengan menggunakan kombinasi kunci ke-1, kunci ke-2, kunci ke-3.
	5.hasil enkripsi (chipper text) akan disimpan kedalam database.
Kondisi Akhir	Akan mengahsilkan chipertext.

d. Fungsi deskripsi

Skenario yang dapat dibuat untuk fungsi level deskripsi adalah :

Tabel 4. Fungsi Level Deskripsi Data

Identifikasi	
Nomor	PN-key-04
Nama	Deskripsi data
Tujuan	Merubah chipertext ke palin text
Aktor	Operator, Administrator
Skenario Utama	
Aksi Aktor	**Reaksi Sistem**
1.operator memasukan kuncinya masing-masing a dan	2. system meload database untuk memanggil nial b dan kunci pada setiap a
	3. System merubah kunci a menjadi kunci master e
5.opearator memasukan data chipertext .	System merubah data chippertext kedalam ascii
	System merubah data chipper text ke plaintext
	System merubah m(palin text) dari ascii ke dalam alphabetic
Kondisi akhir	Menghasilkan plaintext

Performasi Algortima tergantung kedalam beberapa faktor yaitu:

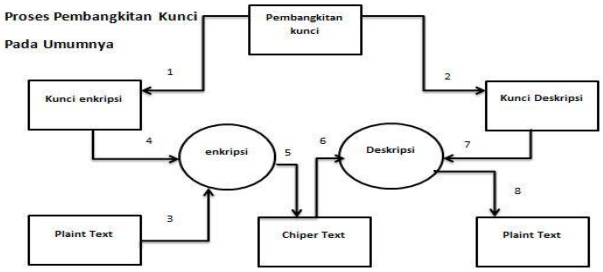
a. Nilai kunci master , Nilai ini di anjurkan merupakan bilangan prima yang memiliki

nilai besar hal ini digunakan untuk menghasilkan keragaman dari nilai kunci user.

b. Nilai input yang dipilih oleh operator. Setiap nilai yang dipilih tidak boleh sama karena akan mengabitkan duplikasi kunci.
c. Fungsi atau formulasi yang dipilih untuk merubah nilai master menjadi sebuah formulasi yang komplek.

Formulasi Pembangkitan Kunci Algoritma Yang Sudah Berjalan

Berikut dibawah ini formulasi pengembangan kunci algoritma yang sudah berjalan :



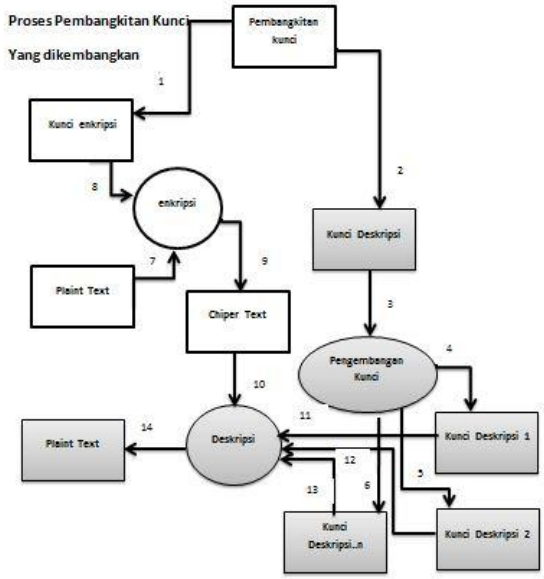
Gambar 2. Formulasi Kunci Algoritma

Keterangan

1. Proses pembangkitan kunci enkripsi.
2. Proses pembentukan kunci deskripsi.
3. Plain text yang akan dienkripsi masuk kedalam proses enkripsi.
4. Kunci enkripsi menuju ke proses enkripsi.
5. Plaint text yang di ubah menjadi chipper text.
6. Proses deskripsi dimana chipper text di masukan kedalam proses deskirpisi.
7. Kunci deskripsi yang dulu dihasilkan dimasukan kedalam proses deskripsi
8. Menghasilkan plaintext tyang telah di deskripsikan

Formulasi Yang Akan Dibuat

Dari formula yang sudah berjalan tadi, penulis akan mengembangkan algoritma seperti dibawah :



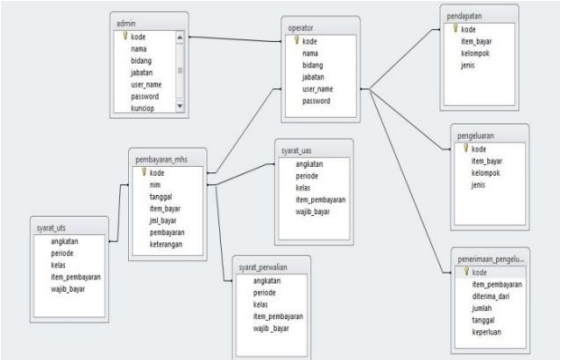
Gambar 3. Formulasi Algoritma yang Dibuat

Keterangan

1. Proses pembangkitan kunci enkripsi.
2. Proses pembentukan kunci deskripsi.
3. Dilakukan pengembangan kunci deskripsi dengan algoritma dimana kunci desripsi bisa di perbanyak.
4. Menghasilkan kunci desripsi ke-1
5. Menghasilkan kunci deskirpsi ke-2
6. Menghasilkan kunci deskripsi ke-n
7. Plain text yang akan dienkripsi masuk kedalam proses enkripsi.
8. Kunci enkripsi menuju ke proses enkripsi.
9. Plaint text yang di ubah menjadi chipper text.
10. Proses deskripsi dimana chipper text di masukan kedalam proses deskirpisi.
11. Kunci deskripsi ke -1 dimasukan kedalam proses deskripsi.
12. Kunci deskripsi ke -2 dimasukan kedalam proses deskripsi
13. Kunci deskripsi ke -n dimasukan kedalam proses deskripsi
14. Menghasilkan plaintext tyang telah di deskripsikan

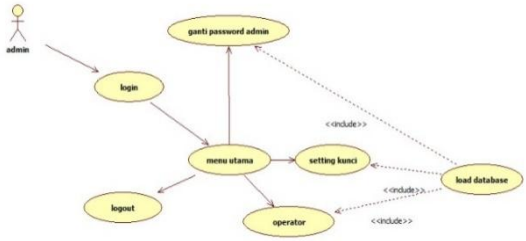
Perancangan Basis Data

Rancangan dan relasi Tabel Pada gambar di bawah merupakan gambaran relasi tabel pada sistem yang berjalan dimana pada setiap tabel terhubung.



Gambar 4. Perancangan Basis Data

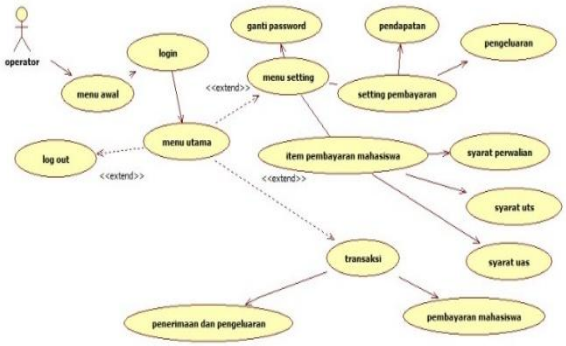
Unified Modelling Leanggue (UML)
Use Case Diagram
a. Admin



Gambar 5. Use Case Diagram Admin

Pada gambar diatas admin(actor) akan login terlebihi dahulu sebelum ke menu utama. Selanjutnya admin dapat meamilih tiga pilihan apakan itu ganti password admin atau setting kunci atau juga setting operator.

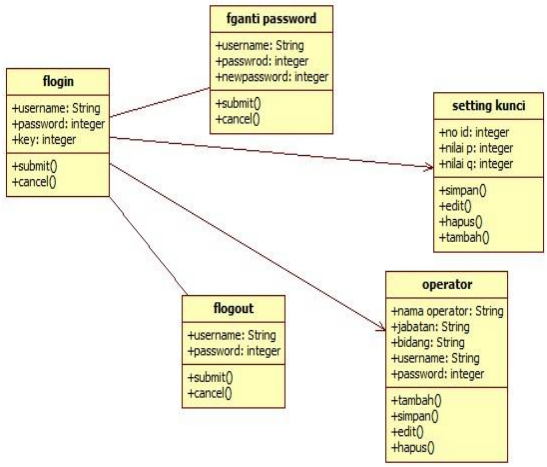
b. Operator



Gambar 6. Use Case Diagram Operator

Operator (actor) masuk kedalam menu awal operator selanjutnya login untuk masuk ke menu utama dan bisa melakukan pemilihan menu baik itu menu setting, item pembayaran maupun transaksi. Jika operator akan keluar dari menu operator maka dapat memilih logout.

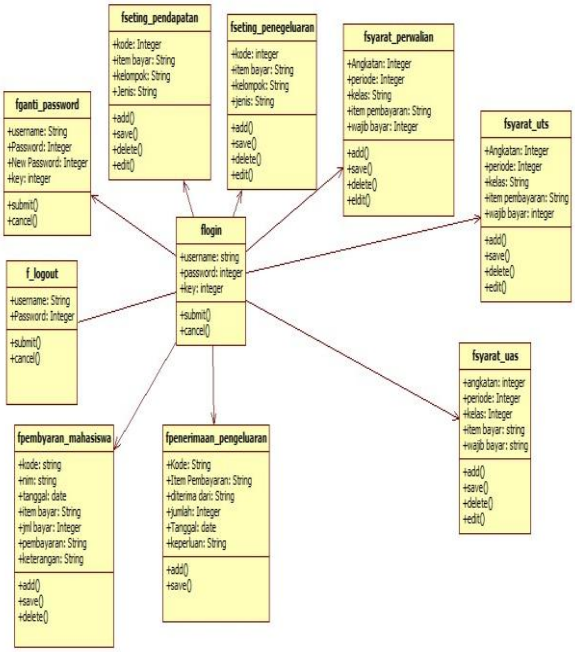
Class Diagram
a. Class Diagram Admin



Gambar 7. Class Diagram Admin

Class Diagram ini menjelaskan bagaimana keterhubungan masing-masing class yang bisa di akses oleh admin dimana setiap fieldnya saling berkaitan.

b. Class Diagram Operator



Gambar 8. Class Diagram Operator

Pada class diagram ini operator terdapat beberapa atribut pada setiap classnya yang dapat dioprasikan oleh operator. Namun untuk melakukan operasi-operasi pada class yang lain, operator harus melakukan login terlebih dahulu.

IMPLEMENTASI

Pada tahapan ini merupakan lanjutan dari tahap *form*ulasi, pada tahap analisis akan diimplementasikan dan menguji desain yang digunakan yang digunakan dan menguji sistem yang telah diterapkan dengan menggunakan bahasa pemograman php dan html. Implementasi ini merupakan sebuah simulasi interface terhadap pengguna untuk membuktikan algoritma yang dikembangkan. Interfacenya seperti berikut.

Penulis melakukan simulasi pada aplikasi Sistem Informasi Akademik, proses pembayaran mahasiswa.

Transaksi Pembayaran Mahasiswa

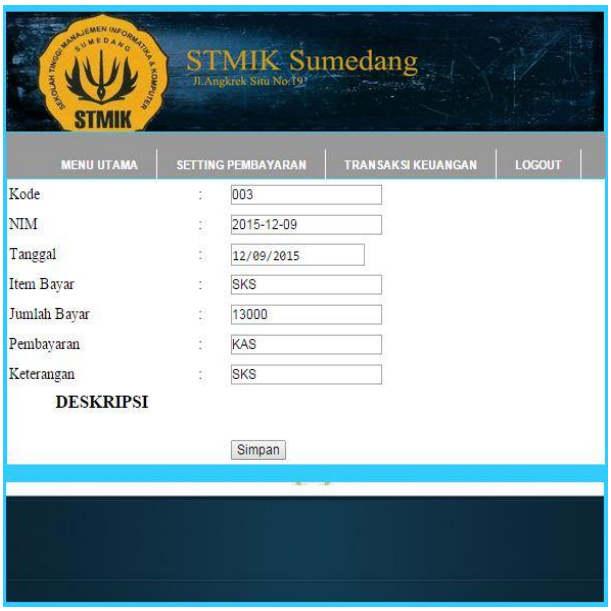
a. Index

Gambar 9. Index

b. Tambah Data

Gambar 10. Tambah Data

c. Deskripsi Data



Gambar 11. Deskripsi Data

KESIMPULAN

Berdasarkan uraian dari penjelasan sebelumnya tentang pengembangan algoritma kunci kriptografi dan telah di uji dengan pembuktian matematika ataupun dengan penerapan kepada sistem di STMIK Sumedang yang telah di hostingkan dengan nama domain www.mutikey.esy.es. Dengan menggunakan model prototype pada pengembangan model dengan menentukan algoritma kunci kriptografi dan melakukan observasi terhadap objek yang diteliti yang di jadikan sebagai sampel penelitian dengan mewancarai pembuatan software dan telah diuji menggunakan white box. Dimana pada proses enkripsi dan deskripsi menggunakan algoritma kunci sederhana yaitu Caesar chipper text yang di kombinasikan dengan algoritma pengembangan kunci yang. Maka dapat di ambil kesimpulan tentang algoritma yang di kembangkan.yaitu :

a. Algoritma pengembangan kunci yang dikembangkan bisa menjadikan algoritma simetris menjadi algoritma asimetris , Yang mana dengan menggunakan Asimetris dimana kunci enkripsi dan kunci deskripsi yang berbeda akan menambah kekuatan pada keamanan datanya karena kunci terbagi dua yaitu kunci public dan kunci private. Dengan kunci lebih dari satu, namun memiliki kemanan pada setiap pengguna.

b. Kunci yang akan di hasilkan dari pengembangan kunci pada setiap user akan menghasilkan 3 kunci, dimana 1 kunci di simpan di database dan 2 kunci di miliki user.
c. Nilai kunci yang di ajukan tidak boleh lebih dari kunci master. Kunci Master di ajurkan memiliki nilai prima. Dikarenakan jika nilai kunci yang diajukan melibihi nilai kunci master maka nilai modnya akan menjadi nilai kunci yang diajukan dan nilai div nya akan menjadikan nilai 1, Artinya nilai kunci yang diajukan akan sama dengan nilai mod(kunci ke-1 sama dengan kunci ke-2, kunci ke-3 adlah 1). Sedangkan untuk Kunci Master sebagai nilai prima adalah untuk mencegah nilai mod sama dengan 0 dan nilai div sama dengan nilai kunci yang diajukan.
d. Algoritma pengembangan kunci yang dikembangkan menambah efisiensi dari deskripsi dan enkripsi yaitu hanya memerlukan proses enkripsi satu kali untuk banyak user. Selain itu efektivitas dari segi keamanan bisa di tingkatkan, meskipun database dan source code telah diketahui tapi keamana akan terjaga karena keamanan terletak pada kunci. Kerahasian data yang tergantung pada kunci inilah yang sesuai dengan prinsip algoritma modern yang merupakan pandangan algoritma masa depan.

SARAN

Pada pengembangan algoritma kunci kriptografi ini terdapat beberapa saran yang ingin penulis sampaikan,yaitu :

a. Algoritma kunci kriptografi harus dikembangkan lagi untuk menambah kompleksitas fungsi dan menghilangkan ketrgantungan terhadap kunci master.
b. Diharapkan mampu di uji coba dengan algoritma kriptografi yang lainnya tidak hanya menggunakan algoritma kriptografi Caesar chipher text.

DAFTAR PUSTAKA

Ana Wahyuni ,Keamanan Pertukaran Kunci Kriptografi dengan Algoritma Hybrid :Diffie-Hellman dan RSA, Fakultas Ilmu Komputer Universitas AKI

Dony Ariyus,*KRIPTOGRAFI KEAMANAN DATA DAN KOMUNIKASI*,Graha Ilmu,2006

Dr.Ir.Saludin Muis,M.Kom, *PENGANTAR KRIPTOGRAFIK KUANTUM*, graha ilmu,2013

Maman Abdurohman, ST. MT.,*ORGANISASI&ARSITEKTUR KOMPUTER*,informatika,2008

Maureen Linda Caroline ,Metode Enkripsi baru : Triple Transposition Vigènere Cipher (13508049) Program Studi Teknik Informatika Sekolah Teknik Elektro dan Informatika,2011

Renaldi Munir, *Algoritma Dan Pemograman*, informatika,2011

Rifki Sadikin, *Kriftografi untuk keamanan jaringan*, ANDI Yogyakarta,2012

Rosa A.S,M.Shalahudin, Rekayasa Perangkat Lunak, Informatika, 2015