KOMBINASI ALGORITMA RSA DAN ALGORITMA CIPHER TRANSPOSISI UNTUK KEAMANAN DATABASE

Ajib Susanto[1], Rico Tritanto[2]
[1]Staf Pengejar Fakultas Ilmu Komputer
Universitas Dian Nuswantoro Semarang

Abstract

Cryptography is a solution or method of securing the data precisely to preserve confidentiality and authenticity of data. It is also able to enhance the security aspects of a data or information. The aim of the method is the confidential information which is sent via a network, can not be known or used by someone else.
Cryptographic provides two aspects of information security, first is the protection of the confidential data/information, counterfeiting and undesired alteration of information. RSA algorithm is an asymmetric encryption algorithm, in other word this algorithm uses the same key for both encryption and decryption process. Transposition cipher algorithm encrypts the plain text by removing small pieces of the message around. By using a combination of the RSA algorithm and Transposition Cipher algorithm, it will be able to improve the security of the data file storage in a database.

Keywords : RSA Algorithm, Transposition Cipher, cryptography.

Pendahuluan

Kemajuan di bidang teknologi informasi telah memungkinkan seseorang untuk melakukan komunikasi dan transaksi bisnis secara *on-line*. Kegiatan-kegiatan tersebut tentu saja akan menimbulkan resiko apabila informasi yang sensitif dan berharga itu diakses oleh orang-orang yang tidak berhak. Dengan berpindahnya data dari titik A ke titik B di internet, data itu akan melalui beberapa titik lain selama perjalanan dan membuka kesempatan bagi pihak lain untuk memotong, membaca, merusak, atau merubah tujuan data.[1]

Proses enkripsi ini sangat diperlukan terhadap data yang bersifat rahasia. Dengan proses ini data akan dicetak dengan menggunakan algoritma enkripsi dan kunci tertentu sehingga sangat sulit untuk dapat dimengerti oleh orang lain yang tidak berhak. Untuk itu kerahasiaan kunci sangat diperlukan bagi keberhasilan proses. Proses enkripsi merupakan proses untuk meng-*encode* data dalam bentuk yang hanya dapat dibaca oleh sistem yang mempunyai kunci untuk membaca data. Proses enkripsi dapat dengan menggunakan *software* atau *hardware*. Hasil enkripsi disebut *cipher*. *Cipher* kemudian didekripsi dengan *device* (alat) dan kunci yang sama tipenya (sama *hardware*/*software* serta sama kuncinya).[2]

Dalam teknologi web, autentifikasi digunakan sebagai sarana untuk mengakses halaman web yang bersifat rahasia dan terbatas. Salah satu metode yang paling banyak digunakan adalah dengan memakai user-id dan password yang dimasukkan pada form login. Selain murah dan tidak memerlukan perangkat tambahan, penggunaan user-id dan password juga nyaman. User hanya perlu menghapal user-id dan password kemudian dapat melakukan login dimanapun.[3]

Namun demikian penggunaan user-id dan password bukannya tanpa kelemahan. User sering kali memilih user-id dan password yang pendek dan lemah sehingga mudah dicuri dengan teknik brute force.[3] Selain itu format standar dari form login akan mengirimkan user-id dan password dari client ke server dalam format plaintext atau teks asli. Dalam format ini, sangat mudah bagi para hacker untuk mendapatkan data user-id dan password yang valid dan dapat digunakan pada form login yang dimaksud.[4]

Untuk menjaga agar user-id dan password tidak mudah dibaca oleh hacker diperlukan proses pengamanan data user-id dan password tersebut. Alternatif proses pengamanan yang ditawarkan adalah dengan melakukan enkripsi di sisi client sebelum data dikirimkan ke server melalui internet.

Dengan demikian yang dikirimkan melalui jaringan internet adalah ciphertext. Format chipertext juga dapat melindungi user-id dan password dari pencurian dengan teknik brute force.[5] Selanjutnya pada sisi server dilakukan dekripsi kembali data sehingga didapatkan data asli.

Jaringan internet adalah suatu bentuk jaringan komunikasi antar user komputer dimana jaringan internet merupakan system yang terbuka dan informasi yang lewat di dalamnya dapat dengan mudah disadap dan diawasi. Pada umumnya, aplikasi komunikasi yang tersedia memiiiki ukuran yang kecil dan mengabaikan faktor keamanan di dalam komunikasi data. Oleh karena itu, user dihadapkan pada resiko akan terancamnya hak *privacy* atas informasi yang mereka rniliki.[6]

Menurut *G. J. Simons*, keamanan informasi adalah bagaimana kita dapat mencegah penipuan (cheating) atau, paling tidak, mendeteksi adanya penipuan di sebuah sistem yang berbasis informasi, dimana informasinya sendiri tidak memiliki arti fisik.

Beberapa cara telah dikembangkan untuk menangani masalah keamanan ini, salah satu teknik mengamankan data pada database adalah dengan algoritma penyandian data atau yang biasa disebut dengan kriptografi. Kriptografi merupakan bagian dari suatu cabang ilmu matematika (*cryptology*) yang dapat dimanfaatkan untuk kepentingan keamanan pesan.[1]

Proses enkripsi data informasi dilakukan secara real time dengan menggunakan dua algoritma yang berbeda dan key enkripsi dapat dibuat berbeda-beda satu user dengan yang lainnya sehingga sulit untuk diterjemahkan oleh pihak yang tidak berkepentingan.[7]

Dari hasil analisis keamanan tersebut, data pada database dapat diamankan dengan penerapan teknologi enkripsi dengan algoritma RSA dan algoritma Cipher Transposisi. RSA termasuk algoritma kunci asimetris sedangkan Cipher Transposisi termasuk algoritma kriptografi klasik. Sebagai algoritma kunci publik, RSA mempunyai dua kunci, yaitu kunci public dan kunci pribadi. Kunci publik boleh diketahui oleh siapa saja, dan digunakan untuk proses enkripsi. Sedangkan kunci pribadi hanya pihak - pihak tertentu saja yang boleh mengetahuinya, dan digunakan untuk proses dekripsi.

Tinjauan Pustaka

Kriptography

Kriptografi telah dikenal dan dipakai cukup lama sejak kurang lebih tahun 1900 sebelum masehi pada prasasti-prasasti kuburan. Kriptografi sendiri berasal dari kata "*Crypto*" yanng berarti rahasia dan "*graphy*" yang berarti tulisan. Jadi, dapat dikatakan kriptografi adalah tulisan yang tersembunyi. Dengan adanya tulisan yang tersembunyi ini, orang orang yang tidak mengetahui bagaimana tulisan tersebut disembunyikan tidak akan mengetahui bagaimana cara membaca maupun menerjemahkan tulisan tersebut. William Stallings mendefinisikan kriptografi sebagai "*the art and science of keeping messages*"

Kriptografi mempunyai peranan penting dalam dunia komputer. Hal ini disebabkan karena banyaknya informasi rahasia yang disimpan dan dikirimkan melalui media-media computer. Informasi-informasi ini biasanya berisikan dokumen-dokumen penting dan data keuangan dari suatu instasi yang tidak ingin dibaca oleh orang yang tidak berhak atas informasi tersebut. Oleh karena itu ilmu kriptografi setiap saat selalu dikembangkan oleh orang untuk dapat menjaga fasilitas-fasilitas tersebut.

Kata kriptografi berasal dari bahasa Yunani. Dalam bahasa Yunani, kriptografi terdiri dari dua buah kata yaitu *cryptos* dan *graphia*. Kata *crypto* berarti rahasia sedangkan *graphia* berarti tulisan. Berarti secara umum makna dari kata kriptografi adalah tulisan rahasia. Dan artinya sebenarnya dari kriptografi adalah ilmu yang mempelajari tentang bagaimana menjaga kerahasiaan suatu pesan, agar isi pesan yang disampaikan tersebut aman sampai ke penerima pesan.[8] Dalam kamus Bahasa Inggris Oxford pengertian kriptografi adalah sebagai berikut :

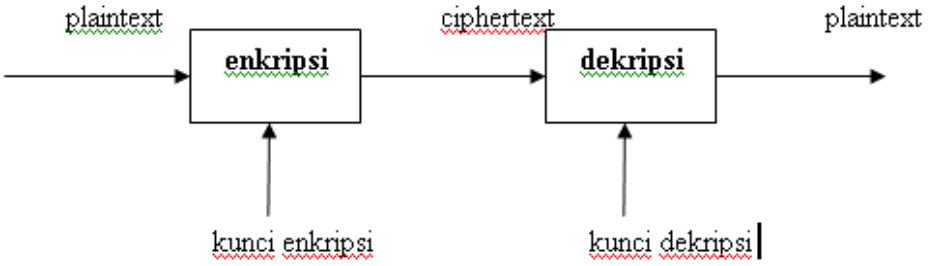
> "Sebuah teknik rahasia dalam penulisan, dengan karakter khusus, dengan menggunakan huruf dan karakter di luar bentuka aslinya, atau dengan metode-metode lain yang hanya dapat dipahami oleh pihak-pihak yang memproses kunci, juga semua hal yang ditulis dengan cara seperti ini".

Jadi secara umum dapat diartikan sebagai seni menulis atau memecahkan chipper.

Secara umum, kriptografi merupakan teknik pengamanan informasi yang dilakukan dengan mengolah informasi awal (plainteks) dengan suatu kunci tertentu menggunakan suatu metode enkripsi tertentu sehingga menghasilkan suatu informasi baru (chiperteks) yang tidak dapat dibaca secara langsung. Chiperteks tersebut dapat dikembalikan menjadi informasi awal (plainteks) melalui proses dekripsi.

Data-data tersebut diamankan dengan sedemikian rupa oleh pengirim sehingga orang lalin tidak dapat mengenali data tersebut. Hal ini lebih dikenal dengan nama proses enkripsi. Data atau pesan yang asli sering disebut sebagai plaintext dan data yang telah dienkripsi disebut sebagai chipertext ata menurut terminologi yang lebih tepat enchiper.

Data yang telah dienkripsi disebut chipertext karena data asli (plaintext) telah mengalami proses di dalam sebuah algoritma kriptografi atau lebih dikenal dengan nama chiper. Kebalikannya, proses merubah pesan yang telah dienkripsi (chipertext) menjadi pesan asli (plaintext) disebut sebagai proses dekripsi atau dechiper. Perkembangan kriptografi memang sangat pesat. Para ahli kriptografi (cryptographers) terus menerus menciptakan algoritma-algoritma kriptografi yang baru.



Gambar 1. Urutan proses kriptografi

Algoritma RSA

Ide pertama dari public key cryptosystem didasarkan dari sebuah paper yang berjudul "*New directions in cryptography*" [9], yang kemudian membuahkan sebuah hasil karya teknis ilmiah, yang dituliskan oleh Rivest, Shamir, dan Adleman [10]. Kemudian, di bulan Februari 1978, mereka mempublikasikan papernya [11] yang berjudul "*A Method for Obtaining Digital Signatures and Public-Key Cryptosystems*".

Algoritma RSA adalah sebuah block cipher algorithm (algoritma yang bekerja per blok data), di mana plaintext dan ciphertext-nya adalah bilangan bulat (integer) antara 0 dan n-1 untuk sebuah n tertentu [12]. Algoritma ini bekerja dengan menghitung eksponen dari pesan (atau plaintext) dalam operasi modulo n (modulo = sisa pembagian). Jadi, sebelum sebuah plaintext dikirimkan, plaintext tersebut harus dipangkatkan dengan sebuah bilangan, yang biasa disebut sebagai e (e = public key). Kemudian, di sisi penerima, pesan tersandi (atau ciphertext) tersebut harus dipangkatkan dengan kunci miliknya sendiri, yang biasa dikenal sebagai d, untuk memperoleh kembali pesan yang dikirimkan. Semua perhitungan dikerjakan pada operasi modulo n.

Algoritma RSA merupakan salah satu algoritma kunci publik yang sampai saat ini paling banyak dikenal. Salah satu sifat dari sistem kripto dengan kunci publik adalah : *D(E(m)) = E(D(m))* dengan *E* adalah proses enkripsi, *D* adalah proses dekripsi dan m adalah message data. Sifat ini yang nantinya sebagai dasar untuk merancang system pengamanan data yang mampu menjamin keaslian dan kerahasiaan data.

Algoritma RSA adalah algoritma kunci publik yang populer, Algoritma RSA dibuat oleh tiga orang ilmuwan dari MIT(Massachusset Institute of Technology) pada tahun 1976, ilmuwan tersebut adalah Ron Rivest, Adi Shamir, dan Leonard Adleman, nama RSA sendiri diambil dari gabungan nama ketiga penemunya yaitu, (R)ivest (S)hamir (A)dleman. Algoritma ini dinilai aman karena melibatkan proses perhitungan bilangan prima dalam jumlah yang besar, secara garis besar proses enkripsi dengan Algoritma RSA dibagi kedalam dua buah proses, yaitu membangkitkan pasangan kunci dan melakukan enkripsi dengan pasangan kunci tersebut. Algoritma membangkitkan pasangan kunci :

1. Pilih secara acak 2 buah bilangan prima, P dan Q.
2. Hitung nilai n = P.Q, sebaiknya nilai P tidak sama dengan Q agar tidak mudah difaktorkan dengan cara menarik akar pangkat 2 dari n.
3. Hitung ©(n)=(P-1)(Q-1).
4. Pilih kunci publik e yang relatif prima dengan ©(n), relative prima artinya nilai PBB (kuncipublik, ©(n))=1.
5. Buat sebuah kunci privat d dengan menggunakan persamaan *d* = 1+*k*©*n/e* Nilai k adalah salah satu bilangan bulat 1, 2, 3, , i. yang menghasilkan variabel d yang bulat, ketika diproses dengan menggunakan persamaan diatas.

Algoritma Enkripsi :

1) Anggaplah kita telah memiliki pasangan kunci enkripsi e nilai n.(cara mencari nilai e dan n dapat dilihat pada penjelasan di atas).
2) Input sebuah plaintext (*Pj*), setiap karakter pada plaintext(*Pj*) akan diindikasikan sebagai P=P1, P2, P3,..., Pj.
3) Cari ciphertext(*Cj*) dengan cara :

*C*1 = *Pe*
1 *modn*
*C*1 = *Pe*
2 *modn*
....
Cj = *Pe*
j modn

Proses dekripsi dari RSA tidakjauh berbeda dengan proses enkripsinya, hanya perlu merubah nilai fariabel e menjadi fariabel d dimana d merupakan kunci dekripsi, sehingga persamaan dekripsinya menjadi , hal penting yang perlu diketahui dari algoritma RSA adalah proses matematika yang terlibat seperti pencarian bilangan prima, PBB([param1],[param2]) atau Pembagi Bersama Terbesar(greatest common divisor), dan Totient Euler(©(n)). PBB digunakan untuk mencari nilai pembagi bilangan bersama terbesar, sebagai contoh:

PBB(27,36) : Faktor(25)= 1, 3, 9, 27 Faktor(36) = 1, 2, 3, 4, 9, 12, 18, 36

Faktor pembagi bersama 25 dan 36 adalah 1, 3, 9. Maka PBB(25,36) = 9. Tottient Euler (©(n)) menyatakan jumlah bilangan bulat yang relatif prima terhadap n, relatif prima memiliki arti PBB(n, m) =1, dimana dalam kasus ini *n* = *P.Q* dan m adalah bilangan bulat.

Transpotition Cipher

Cipherteks diperoleh dengan mengubah posisi huruf di dalam plainteks. Dengan kata lain, algoritma ini melakukan *transpose* terhadap rangkaian huruf di dalam plainteks. Nama lain untuk metode ini adalah permutasi, karena *transpose* setiap karakter di dalam teks sama dengan mempermutasikan karakter-karakter tersebut.

Contoh 1:
Misalkan plainteks adalah FAKULTAS TEKNOLOGI INFORMASI
Enkripsi :

FAKULT
ASTEKN
OLOGII
NFORMA
SIZZZZ

Cipherteks : (baca secara vertikal)

FAONSASLFIKTOOZUEGRZLKIMZTNIA
FAON SASL FIKT OOZU EGRZ LKIM ZTNI AZ

Dekripsi: Bagi panjang cipherteks dengan kunci.(Pada contoh ini, 30 / 6 = 5)

FAONS
ASLFI
KTOOZ
UEGRZ
LKIMZ
TNIAZ

Plainteks: (baca secara vertikal) FAKULTAS TEKNOLOGI INFORMASI
Contoh 2:
Plainteks: TEKNOLOGI INFORMASI
Bagi menjadi blok-blok 8-huruf. Jika < 8, tambahkan huruf palsu.
Cipherteks:

GEKONLOTAINOFRMIFIACBDES

Pembahasan

Analisa algoritma RSA

Prinsip kerja algoritma RSA terletak pada sulitnya memfaktorkan bilangan yang besar menjadi faktor-faktor prima. Pemfaktoran dilakukan adalah untuk mendapatkan kunci privat. Selama

bilangan tersebut tidak dapat difaktorkan selama itu pula keamanana algoritma RSA dan algoritma Cipher Transposisi terjamin. Dalam algoritma RSA terdapat beberapa besar-besaran yang penting, yaitu sebagai berikut:

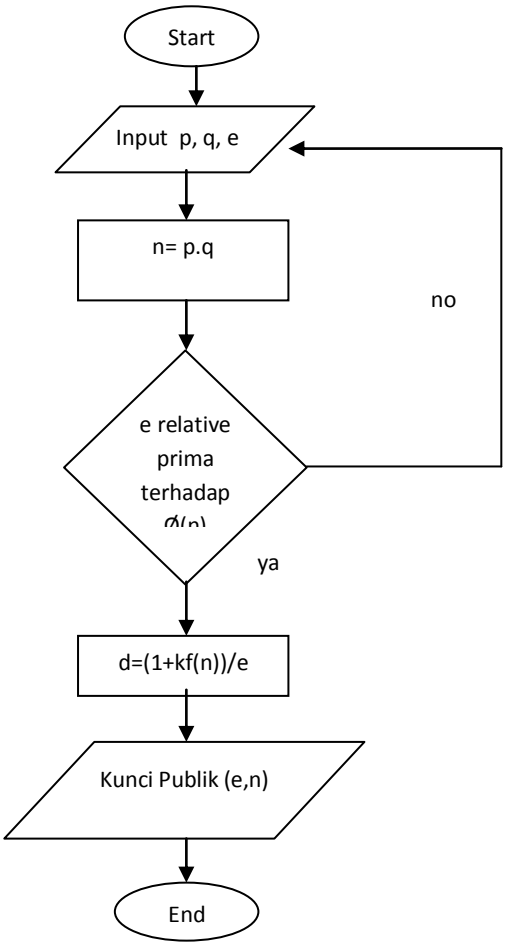
a) p dan q merupakan bilangan prima yang diambil secara acak, atau untuk lebih bagusnya dipilih oleh orang yang akan menerima pesan.Sifat dari kedua bilangan ini adalah rahasia, dimana hanya pengirim pesan dan penerima pesan saja yang mengetahui.
b) n=p.q. sifat dari n ini adalah tidak rahasia, yang berarti bisa diketahui oleh publik.
c) Q(n)=(p-1)(q-1). Sifat dari bilangan ini adalah rahasia.
d) e(kunci enkripsi). Kunci enkripsi bersifat tidak rahasia.
e) d(kunci dekripsi). Kunci dekripsi bersifat tidak rahasia.
f) m(plainteks). Plainteks merupakan informasi awal yang bersifat rahasia.
g) c(chiperteks). Chiperteks merupakan informasi yang telah dienkripsi yang bersifat tidak rahasia.[17]

Langkah pertama dalam algoritma RSA ini adalah membangkitkan pasangan kunci (kunci publik, dan kunci privat). Sebagaimana yang telah kita ketahui kunci publik bersifat tidak rahasia dan boleh diketahui oleh semua orang, sedangkan kunci privat bersifat rahasia dan hanya orang berhak terhadap informasi tersebut saja yang dapat mengetahuinya. berikut adalah langkah-langkah dalam membangkitkan pasangan kunci:

a) Pertama pilih 2 buah bilangan prima secara acak. Bilangan itu diberi besaran p dan q.
b) Hitung nilai n= p.q
c) Hitung Q(n)=(p-1)(q-1)
d) Pilih kunci publik yang disimbolkan dengan e.Syarat dari pemulihan kunci ini adalah e harus relatif prima terhadap Q(n).
e) Membangkikan kunci privat dengan persamaan d=1+kQ(n)/e

Hasil algoritma di atas adalah:

1. Kunci publik adalah pasangan (e,n).
2. Kunci privat adalah pasangan (d,n).

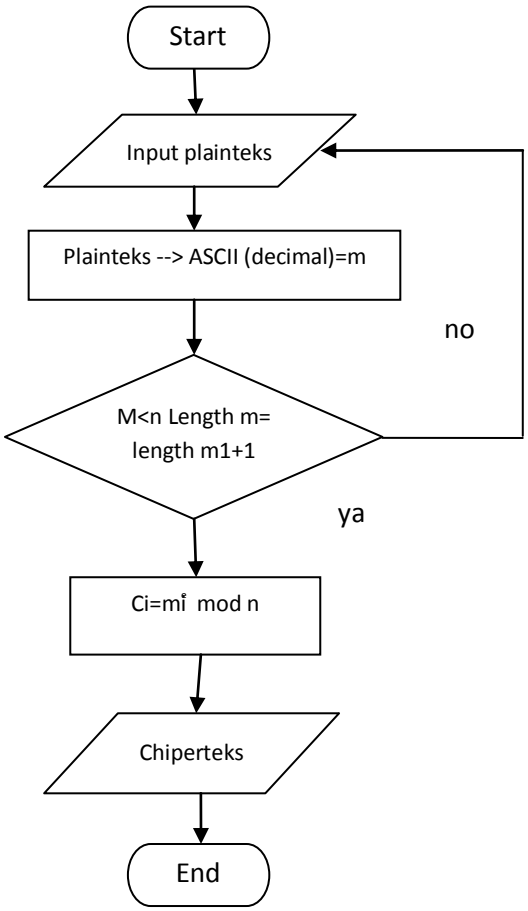


Gambar 2. *Flowchart* pembangkit kunci dalam algoritma RS

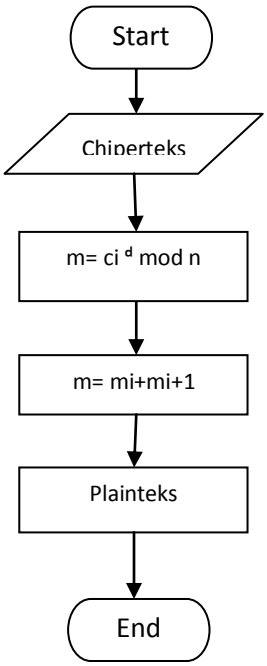
Proses selanjutnya adalah proses enkripsi. Langkah-langkah dari proses enkripsi adalah sebagai berikut:

a) Langkah pertama adalah mengambil nilai e dan n dari proses pembangkit kunci.
b) Masukkan teks yang akan dienkripsi (palinteks)
c) Berkas yang akan dienkripsi diubah ke dalam bentuk desimal sesuai dengan tabel ASCII.
d) Membagi berkas tersebut menjadi beberapa blok (mi), dengan syarat mi<n dan length(mi) length(mi+1).
e) Setelah itu setiap blok dari berkas tersebut dienkripsikan menggunakan pasangan kunci publik.

Setelah didapatkan chiperteksnya, dengan begitu informasi tersebut tidak akan dapat dibaca lagi oleh orang tanpa melalui proses deskripsi. Proses deskripsi pada algoritma RSA ini memerlukan yang dinamakan dengan kunci privat. Kunci privat hanya diketahui oleh orang yang berhak atas informasi tersebut.



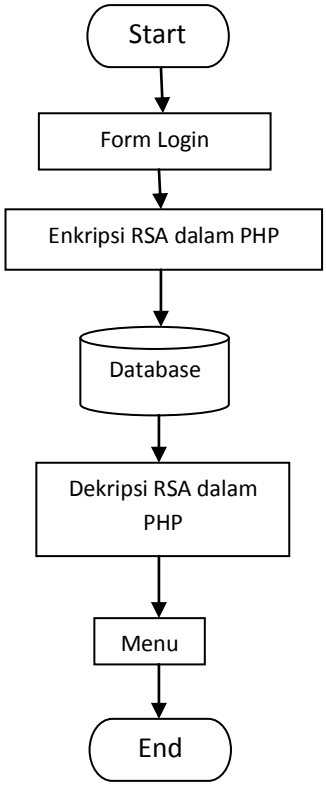
Gambar 3. *flowchart* untuk enkripsi



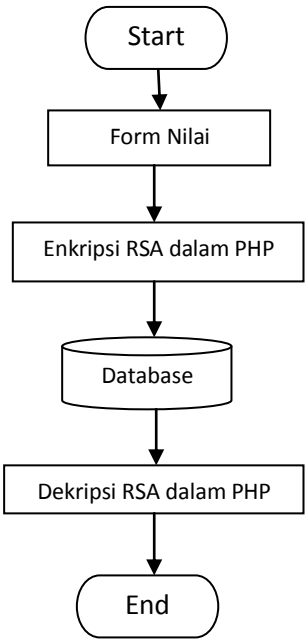
Gambar 4 *flowchart* proses deskripsi pada algoritma RSA

Implementasi Enkripsi atau Deksripsi algoritma RSA pada Sistem Akademik

Pada bagian ini metode enkripsi RSA diimplementasikan pada *Sistem Akademik* yang diimplementasikan pada form login

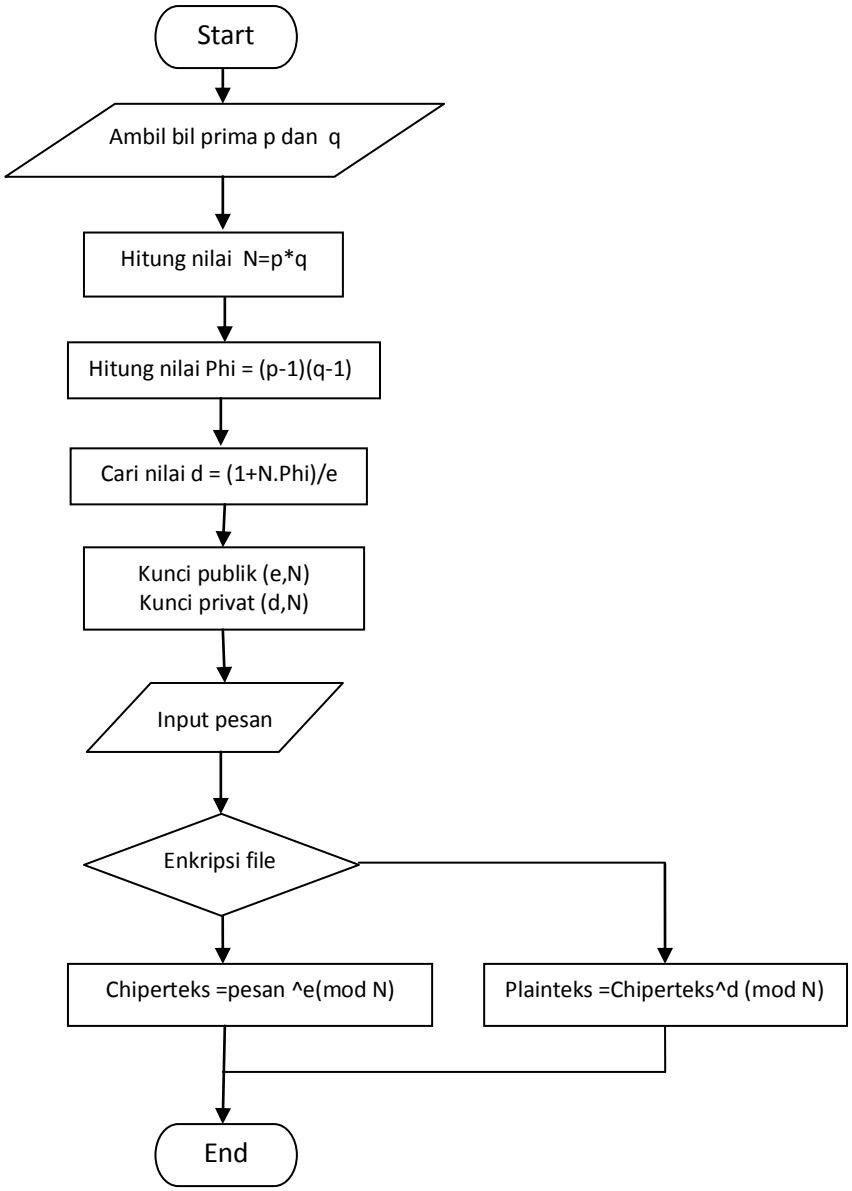


Gambar 5. *Flowchart* implementasi enkripsi / dekripsi RSA pada login



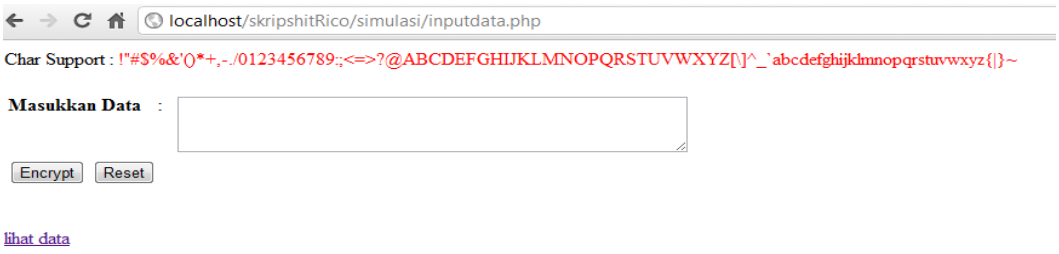
Gambar 6. *Flowchart* implementasi enkripsi / dekripsi RSA pada form Nilai

Flowchart Program

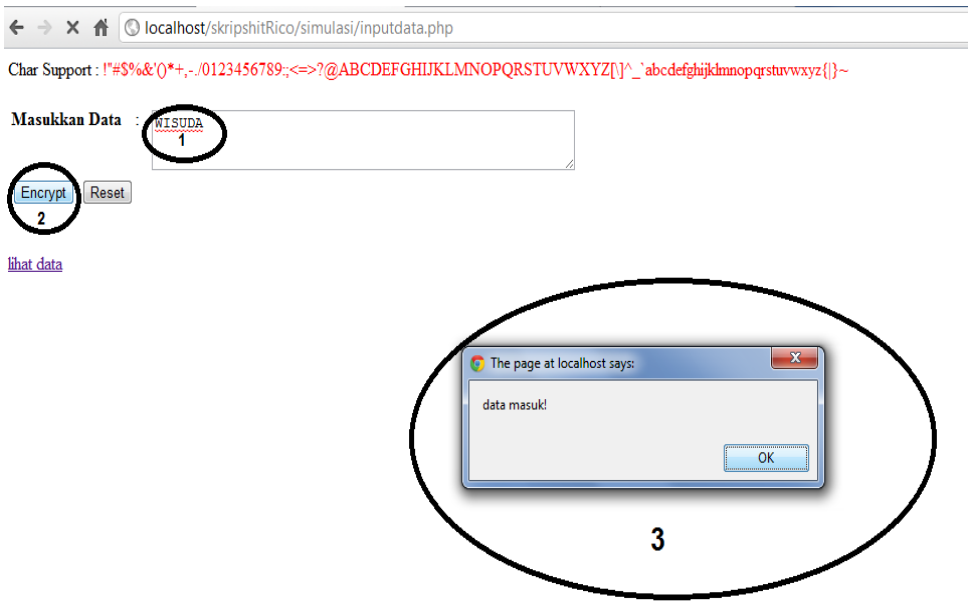


Gambar 6. *Flowchart* Program

Hasil Simulasi



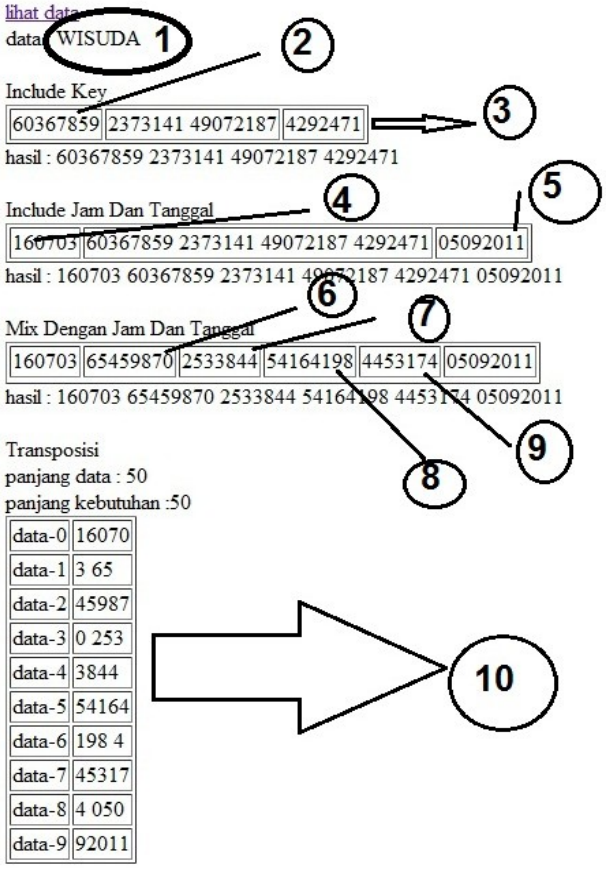
Gambar 7 form input data



Gambar 8. form hasil input data

Form hasil input data berfungsi untuk melakukan enkripsi, langkah-langkahnya dalam melakukan enkripsi sebagai berikut :

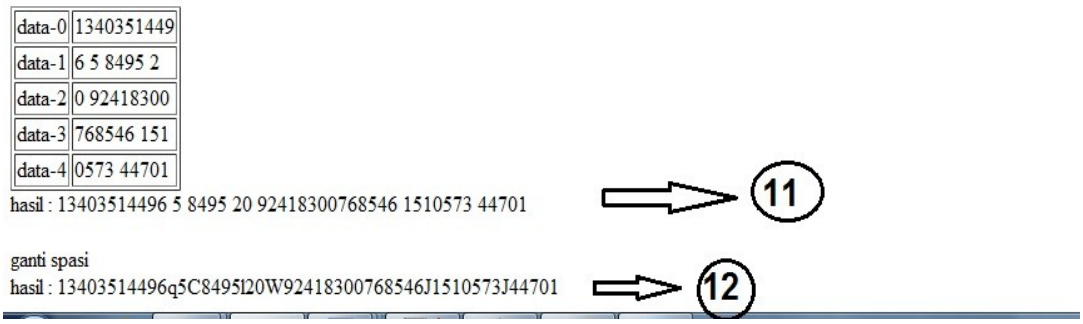
1. Pertama input data pada kolom yang tertulis *masukkan data*, seperti yang terlihat pada keterangan no 1. Kata "WISUDA" diinputkan.
2. Setelah berhasil diinputkan, lalu tekan *tombol encrypt* seperti pada keterangan no 2.
3. Setelah ditekan, maka akan ada peringatan berupa javascript (no.3) yang memberitahukan bahwa data sudah tersimpan dalam database.



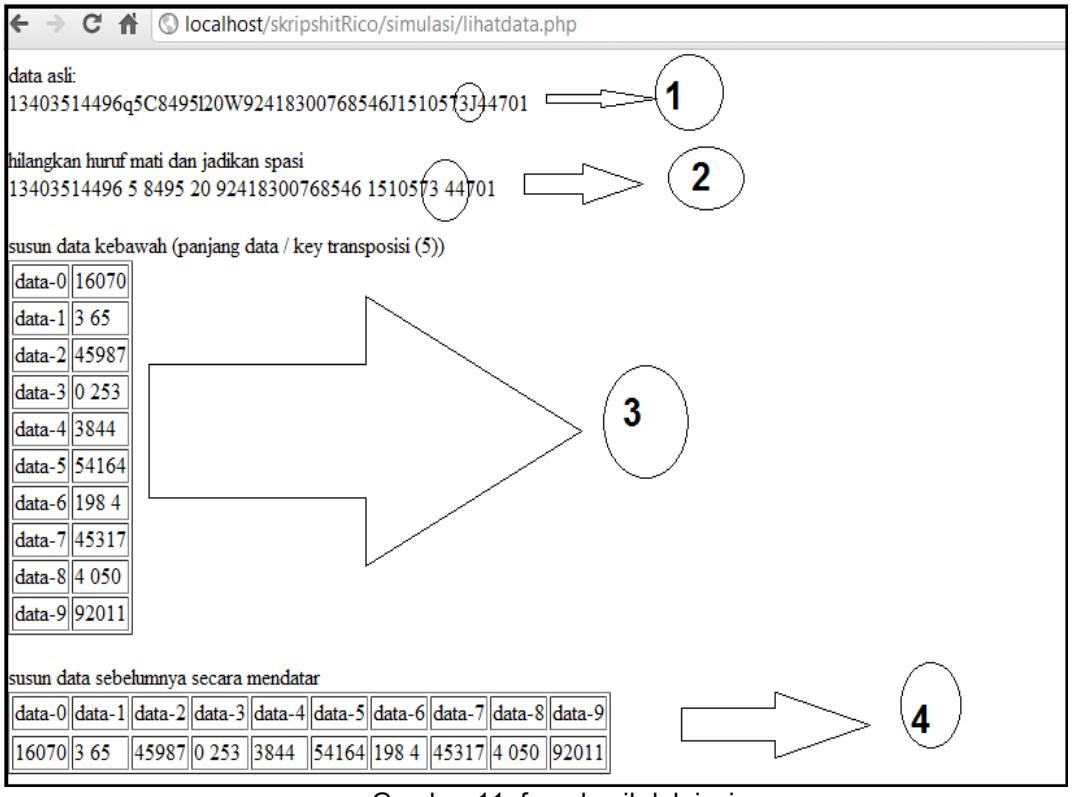
Gambar 9. form detail enkripsi

Setelah *tombol encrypt* ditekan lalu keluar peringatan kalau data sudah tersimpan dalam database maka akan muncul form seperti diatas. Form itu menerangkan bagaimana alur enkripsi berjalan, yaitu :

1. Pertama, data aslinya atau plainteks akan ditampilkan seperti pada keterangan no 1.
2. Kedua, plainteks yang sudah dienkripsi menjadi cipherteks ditampilkan lalu dimasukkan kuncinya *(key)* seperti pada keterangan no 2 dan 3.
3. Setelah selesai memasukkan kuncinya kedalam cipherteks, langkah selanjutnya adalah memasukkan jam dan tanggal pada bagian depan dan belakang cipherteks seperti pada keterangan no 4 dan 5.
4. Langkah selanjutnya menjumlahkan cipherteks dengan jam dan tanggal, dengan aturan kolom genap akan dijumlahkan dengan tanggal sedangkan kolom yang ganjil akan dijumlahkan dengan jam seperti keterangan pada no 6, 7, 8, dan 9. Contohnya: 60367859 + 05092011(tanggal) = 65459870
5. Kemudian setelah selesai pada langkah ke 4 , lalu akan dilakukan enkripsi dengan algoritma transposisi seperti pada keterangan no 10.
6. Setelah itu akan ditampilkan hasilnya seperti pada keterangan no 11, tetapi pada hasil cipherteks tersebut masih ada spasinya.
7. Langkah terakhir yaitu mengganti spasi dengan huruf yang sudah diajak, seperti pada keterangan no 12 .



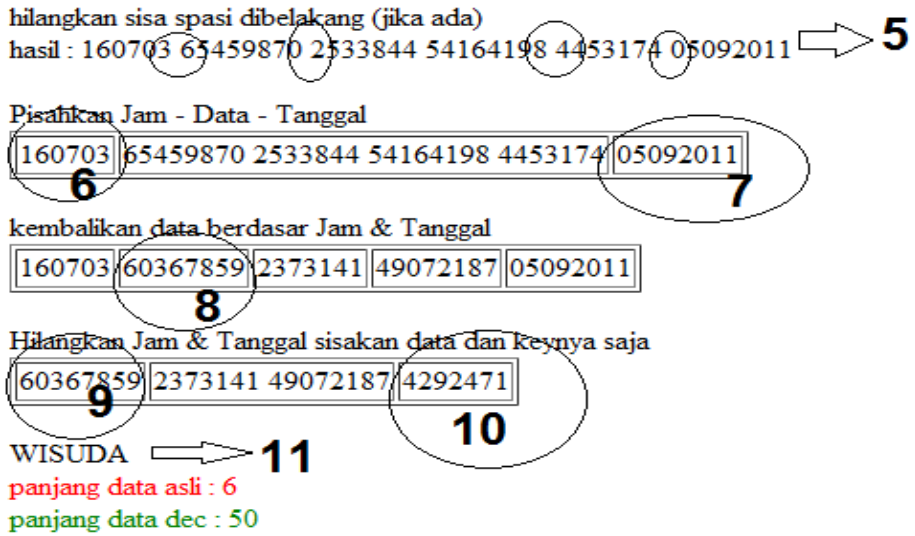
Gambar 10. form detail enkripsi



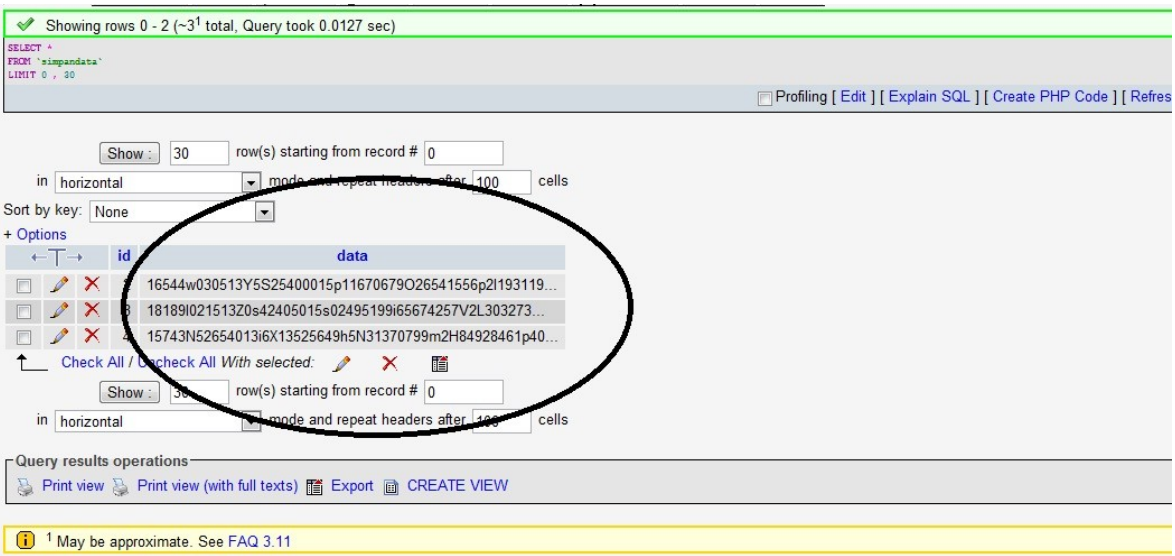
Gambar 11. form hasil dekripsi

Pada gambar di atas menerangkan bagaimana form dekripsi berjalan. Form ini akan tampil setelah link lihat data yang terdapat pada form input data saat melakukan enkripsi ditekan maka akan menampilkan form dekripsi tersebut. Alur kerja dari form dekripsi tersebut sebagai berikut :

1. Data asli atau cipherteks ditampilkan sesuai yang tersimpan dalam database, seperti keterangan no 1
2. Cipherteks asli tersebut mengandung huruf mati, oleh karena itu hilangkan huruf tersebut dengan spasi karena pada awalnya huruf tersebut adalah spasi.
3. Kemudian susun cipherteks tersebut kebawah (*no.3*), setelah itu disusun secara mendatar (*no.4*). Karena untuk membalikkan algoritma transposisi yang sebelumnya digunakan untuk proses enkripsi.
4. Setelah itu hilangkan spasi dibelakang (jika ada), seperti pada keterangan no.5
5. Langkah selanjutnya pisahkan antara jam - data – tanggal, seperti pada keterangan no.6 dan 7
6. Lalu kembalikan data berdasarkan jam & tanggal, seperti saat proses enkripsi. Perbedaannya pada saat proses enkripsi data ditambah dengan jam dan tanggal, sedangkan pada dekripsi data dikurangi dengan jam dan tanggal (no.8).
7. Kemudian hilangkan jam dan tanggalnya, lalu sisakan data dan kuncinya (*key*) seperti pada keterangan no.9 dan 10.
8. Setelah semua selesai maka proses dekripsi berhasil dilakukan, seperti yang terlihat pada no.11.



Gambar 12. form hasil dekripsi



Gambar 13. Hasil Enkripsi di Database

Implemenstasi Sistem
Proses Pembangkitan Kunci

Proses pembangkitan kunci dalam algoritma RSA terdiri dari 2 kunci yaitu kunci public dan kunci privat. Pada kunci public terdapat 2 nilai yaitu nilai e dan n (e,n) yang digunakan untuk melakukan enkripsi data sedangkan pada kunci privat terdapat 2 nilai yaitu nilai d (d,N) yang digunakan untuk melakukan dekripsi data.

Sebagai contoh :

1. Pilih bilangan prima p = 4973 dan q = 4651
2. N= p.q = 4973. 4651 = 23129423
3. Phi= (p-1).(q-1)= (4973 - 1)(4651 - 1) = 23119800
4. e = 8527
5. d = 16645063
6. Sehingga didapatkan = public key : (8527 , 23129423) dan privat key : (16645063, 23129423)
7. Enkripsi : pesan “AKU”
   Kemudian Diubah dalam decimal (kode ASCII)
   A = 65
   B = 75
   C = 85
   Masing-masing tiap karakter dalam ASCII dikurangi 30, karena nilai hasil konversi *string* huruf ke dalam ASCII decimal menghasilkan nilai yang cukup besar yang rentangnya antara 97 (a) hingga 112 (z) sedangkan untuk angka nilainya cukup kecil berkisar antara 48 (0) hingga 57 (9). Agar jumlah digit hasil konversi ke ASCII memiliki keserangaman 2 digit angka maka perlu dilakukan pengurangan 30 untuk setiap hasil konversi ASCII .
   menjadi :
   A = 65 – 30 = 35
   B = 75 – 30 = 45
   C = 85 – 30 = 55
   Setelah itu disetiap 3 huruf dibatasi dengan angka 1, menjadi :
   13545551
   Setelah itu menghitung Chiperteks dengan rumus C = pesan ^ e (mod N)
8. C = 13545551 ^ 8527 (mod 23129423) = 7377261
9. Kemudian kuncinya dimasukkan didepan dan dibelakang data cipherteks : 23129423 7377261 16645063
10. Masukkan jam dan tanggal menjadi : 180713 23129423 7377261 16645063 05092011
11. Jumlahkan jam dan tanggal sehingga menjadi : 180713 28221434 7557974 21737074 05092011
12. Kemudian diubah lagi menggunakan algoritma transposisi menjadi : 1324720518 2 917010 177749 724543 2 1835 700
13. Ganti spasi yang ada menjadi huruf : 1324720518b2o917010O177749h724543v2l1835s700J

Dalam enkripsi ini diambil juga tanggal dan waktu dari server, lalu ditambah kan pada chiperteks. Pada akhir Chiperteks maka aka ada angka yang menunjukkan tanggal, ini digunakan untuk menyembunyikan chiperteks yang sebenarnya. Tanggal dan jam tesebut juga berguna kalau seandainya kita akan melihat waktu penginputan data.

Setelah tanggal dan jam sudah ditambah kan lalu chiperteks tersebut dimodifikasi lagi dengan algoritma cipher transposisi.

Untuk melakukan dekripsi langkah-langkahnya sebagai berikut :

1. Data Asli : 1324720518b2o917010O177749h724543v2l1835s700J, hilangkan data yang ada hurufnya menjadi seperti ini : 1324720518 2 917010 177749 724543 2 1835 700

2. Kemudian data tersebut disusun kebawah, setelah itu data disusun secara mendatar untuk membalikkan algoritma transposisi : 180713 28221434 7557974 21737074 05092011 , hilangkan spasi dibelakang jika ada
3. Lalu pisahkan jam dan tanggal, menjadi : 180713 28221434 7557974 21737074 05092011
4. Kembalikan data berdasarkan jam dan tanggal : 180713 23129423 7377261 05092011
5. Hilangkan jam dan tanggalnya, tetapi sisakan kunci dan datanya : 23129423 7377261 16645063
6. Dekripsi dilakukan dengan cara yang pertama yaitu mengembalikan cipherteks yang telah diubah menggunakan algoritma cipher transposisi tadi. Setelah itu jam dan tanggal yang ditambahkan tadi dihilangkan setelah itu baru kemudian chiperteks awal kembali yaitu 6904554
   chiperteks "7377261"
   M = chiperteks ^ d (mod N)
7. M = 7377261 ^ 16645063 (mod 23129423)
   = 13545551

   Setelah itu angka 1 pada awal dan akhir dihilangkan, menjadi :

   35
   45
   55

   Lalu angka-angka tersebut ditambah 30, menjadi :

   65
   75
   85

   Angka tersebut kemudian diubah ke dalam kode ASCII menjadi :

   65 = A
   75 = K
   85 = U

Kesimpulan

Kesimpulan yang dapat diberikan hasil implementasi sebagai berikut:

a. Keamanan algoritma RSA terletak pada sulitnya memfaktorkan bilangan yang besar menjadi factor-faktor prima. Pemfaktoran dilakukan untuk memperoleh kunci privat sehingga keamanan algoritma RSA tetap terjamin.
b. Pembuatan tekhnik kriptografi enkripsi dekripsi dengan menggunakan metode RSA dan algoritma Cipher Transposisi diharapkan dapat mendukung proses perlindungan data yang tidak mudah dicuri dan tidak mudah dipecahkan yang dapat digunakan sebagai keamanan data-data yang sangat penting sehingga dapat dijaga kerahasiannya.

DAFTAR PUSTAKA

[1] Nursanto, J. (2003). Tugas Akhir Kuliah Keamanan Jaringan Informasi : Tinjauan Mengenai Aplikasi Metode Montgomery Multiflication-Chinese Remainder Theorem (Crt) dalam Mempercepat Deskripsi RSA. Program Magister Teknologi Elektro Institut Teknologi Bandung, Bandung.

[2] Yang, Y.; Zhou, J.; Weng, J.; Bao, F., 2009, A New Approach for Anonymous Password Authentication, 2009 Annual Computer Security Applications Conference, IEEE Computer Society, pp. 199 – 208.

[3] Yang, Y.; Zhou, J.; Weng, J.; Bao, F., 2009, A New Approach for Anonymous Password Authentication, 2009 Annual Computer Security Applications Conference, IEEE Computer Society, pp. 199 – 208.

[4] Chakrabarti, S.; Singhal, M., 2007, Password-Based Authentication: Preventing Dictionary Attacks, IEEE Computer Society, pp. 68 – 74.

[5] Halevi, S.; Krawczyk, H., 1998, *Public-key Cryptography and Password Protocols*. Proc. ACM. Computer and Communication Security, pp. 122-131.

[6] Ardiansyah D. 2003, *Tekhnologi Jaringan Komputer.* http ://ilmukomputer.com (januari 2005).
[7] Kurniawan Y. 2004. *kriptografi keamanan internet dan jaringan telekomunikasi*.Bandung: Informatika.Indonesia.
[8] Ariyus,Dony. 2008. *Pengantar Ilmu Kriptografi Teori, Analisis dan Implementasi*. ANDI, Yogyakarta.
[9] Diffie, W., and Hellman, M. (1976). *Multiuser cryptograhics Technique. IEEE Transactions on Information Theory.*
[10] Rivest, R.,L, Shamir, A., Adleman, L.: 1977, "On Digital Signatures and Public Key Cryptosystems", Laboratory of Computer Science, Massachusetts Institute of Technology, Technical Memo 82.
[11] Rivest, R., L.: 1978, A Method for Obtaining Digital Signatures and Public-Key Cryptosystems, Communications of theACM, vol. 21(2), pp. 120-126.
[12] Gustavus J., S.: 1992, Contemporary Cryptology : The science of Information Integrity, IEEE Press, USA.