Sains dan Komputer (SAINTIKOM)
Vol.18, No.1, Februari 2019, pp. 30~34
P-ISSN: 1978-6603 E-ISSN : 2615-3475

Implementasi Algoritma RSA Terhadap Keamanan Data Simpan Pinjam

Badrul Anwar, Nurcahyo Budi Nugroho, Jaka Prayudha, Azanuddin
STMIK Triguna Dharma

Article Info

Article history:
Received Jul 18th, 2018
Revised Aug 15th, 2018
Accepted Jan 12th, 2019

Keyword:
Simpan Pinjam
Algoritma RSA

ABSTRACT

Koperasi kredit atau Credit Union (CU) adalah sebuah lembaga keuangan yang bergerak di bidang simpan pinjam yang bertujuan untuk mensejahterakan anggotanya sendiri. Perbedaan antara CU dengan koperasi biasa yaitu koperasi biasa masih mendapatkan bantuan dari Pemerintah, sementara CU bersifat mandiri dan tidak mendapatkan bantuan dari Pemerintah Dalam hal ini CU Suka Makmur sendiri memiliki sistem untuk simpan pinjam terhadap anggotanya sendiri, dan dalam sistem tersebut memiliki data yang hanya boleh diketahui pihak tertentu saja. Dibutuhkan suatu teknik pengaman tambahan untuk menjaga keamanan informasi penting tersebut. Tanpa adanya teknik tambahan untuk menjaga kerahasiaan data, maka banyak pihak yang tidak berhak dapat melakukan serangan, salah satunya adalah pencurian data.

Dalam hal ini CU Suka Makmur sendiri memiliki sistem untuk simpan pinjam terhadap anggotanya sendiri, dan dalam sistem tersebut memiliki data yang hanya boleh diketahui pihak tertentu saja. Keamanan data adalah salah satu hal yang paling perlu diperhatikan dalam menjaga kerahasiaan informasi kumpulan data yang penting. Dibutuhkan suatu teknik pengaman tambahan untuk menjaga keamanan informasi penting tersebut.

Algoritma kriptografi adalah satu solusi yang dapat digunakan untuk menjaga kerahasiaan informasi data. Kriptografi didalamnya adalah proses enkripsi dan dekripsi, dengan melakukan enkripsi pada suatu data, maka data tersebut tidak dapat terbaca karena teks asli atau plaintext telah diubah ke teks yang tak terbaca atau disebut chipertext

First Author
Nama: Mukhlis Ramadhan
Kantor : STMIK Triguna Dharma

1. PENDAHULUAN

Koperasi kredit atau Credit Union (CU) adalah sebuah lembaga keuangan yang bergerak di bidang simpan pinjam yang bertujuan untuk mensejahterakan anggotanya sendiri. Perbedaan antara CU dengan koperasi biasa yaitu koperasi biasa masih mendapatkan bantuan dari Pemerintah, sementara CU bersifat mandiri dan tidak mendapatkan bantuan dari Pemerintah. Di CU, penabung adalah anggota yang merupakan pemilik sekaligus sebagai pengguna jasa, dan anggota sebagai pemegang otoritas dan tunduk kepada Undang-Undang Koperasi. Dalam hal ini CU Suka Makmur sendiri memiliki sistem untuk simpan pinjam terhadap anggotanya sendiri, dan dalam sistem tersebut memiliki data yang hanya boleh diketahui pihak tertentu saja. Keamanan data adalah salah satu hal yang paling perlu diperhatikan dalam menjaga kerahasiaan informasi kumpulan data yang penting. Dibutuhkan suatu teknik pengaman tambahan untuk menjaga keamanan informasi penting tersebut. Tanpa adanya teknik tambahan untuk menjaga kerahasiaan data, maka banyak pihak yang tidak berhak dapat melakukan serangan, salah satunya adalah pencurian data.

Algoritma kriptografi adalah satu solusi yang dapat digunakan untuk menjaga kerahasiaan informasi data. Kriptografi didalamnya adalah proses enkripsi dan dekripsi, dengan melakukan enkripsi pada suatu data, maka data tersebut tidak dapat terbaca karena teks asli atau plaintext telah diubah ke teks yang tak terbaca atau disebut chipertext. Ada banyak algoritma kriptografi yang dapat digunakan, berdasarkan sifat kuncinya

dibagi menjadi dua yaitu simetris yang hanya memakai satu kunci rahasia dan asimetris (public key algorithm) yang memakai sepasang kunci publik dan kunci rahasia. Agar dapat dilakukan enkripsi dan dekripsi dengan baik dibutuhkan suatu algoritma untuk enkripsi dan dekripsi salah satunya algoritma kriptografi asimetris RSA yang ditemukan oleh Ron Rivest, Adi Shamir, dan Leonard Adleman pada tahun 1978 dan RSA merupakan singkatan inisial dari nama mereka bertiga.

2. LANDASAN TEORI

2.1 Koperasi Kredit

Koperasi adalah bentuk kerjasama dibidang ekonomi yang sesuai dengan pancasila dan Undang-Undang Dasar 1945. Didalam Undang-Undang Dasar 1945 pasal 33 ayat (1) ditegaskan bahwa perekonomian disusun sebagai usaha bersama berdasarkan atas asas kekeluargaan. Didalam Undang-Undang Dasar 1945 pasal 33 ditegaskan bahwa kemakmuran masyarakatlah yang diutamakan dan bukan kemakmuran perseorangan. Maka sebab itu perekonomian disusun sebagai usaha bersama berdasarkan asas kekeluargaan.

Credit Union adalah sebuah koperasi, menjelaskan corak maupun kekhususannya secara jelas. Coraknya adalah perkoprasian, karena perusahaan dibentuk oleh anggota secara sukarela dengan modal mereka sendiri, dengan pengurus yang dipilih oleh anggota sendiri, dengan hak dan kewajiban anggota yang sama. Bertujuan untuk melayani kepentingan dan kebutuhan anggota, dan pembagian keuntungan disesuaikan dengan jasa masing-masing anggota. Kekhususannya adalah bahwa credit union khusus bergerak dibidang keuangan, yaitu simpan dan pinjam yang dilakukan dengan cara yang praktis, menarik, dan menguntungkan.

2.2 Algoritma RSA

Tingkat keamanan algoritma penyandia RSA sangat tergantung pada ukuran kunci sandi (dalam bit). Semakin besar ukuran kunci, maka semakin sulit juga penyadap terjadi. Kombinasi kunci ini lebih dikenal dengan istilah *brute fore attack* yang bila panjang kuncinya 256 bit, maka menjadi tidak ekonomis dan sia-sia jika hacker pun meyadap sandi.

2.2.1 Proses Pembuatan Kunci

Algoritma pembangkit kunci ada 2 bilangan prima besar yaitu n = p x q sangat sulit untuk difaktorisasikan. Direkomendasikan besar p dan q adalah 512 bit sehingga n berukuran 1024 bit. Karena p dan q adalah bilangan prima, maka n =(p – 1) (q – 1). Kemudian pilih sebuah integer e dipilih secara acak dari Ƶϕ(n) yang memenuhi gcd(e,ϕ(n)) sehingga e merupakan generator pada Ƶϕ(n). Selanjutnya algoritma pembangkit kunci RSA menghitung d invers perkalian e pada Ƶϕ(n). Pada akhirnya algoritma pembangkit kunci RSA menetapkan (e,n) sebagai kunci publik dan d sebagai kunci privat atau tetap dirahasiakan. Langkah-langkah dalam pembangkit kunci RSA adalah

1. Pilih dua buah bilangan prima sembarang p dan q. nilai p dan q harus dirahasiakan.
2. Hitung nilai n dari rumus, *n – p x q*. Besaran n tidak perlu dirahasiakan
3. Hitung *m = (p – 1) (q – 1).* Bersaran m perlu dirahasiakan
4. Dipilih sebuah bilangan bulat sebgai kunci publik, disebut namanya e, yaitu relativ prima terhadap m. e relative prima terhadap m artinya factor pembagi terbesar keduanya adalah 1, secara matematis disebut gcd (e,m)=1. Untuk mencarinya dapat digunakan algoritma Euclid. Nilai e bersifat tidak rahasia.
5. Hitung kunci privat, disebut namanya d sedemikian agar (d x e) mod m=1. Untuk mencari d yang sesuai dapat juga digunakan algoritma Extended Euclid.

Maka hasil dari algoritma tersebut diperoleh :

a. Kunci public adalah pasangan (e,n) bersifat tidak rahasia.
b. Kunci privat adalah pasangan (d,n) bersifat rahasia.

2.2.2 Enkripsi dan Dekripsi

Enkripsi merupakan data yang disandikan dengan kunci publiknya (n,e) agar tidak dapat diketahui data (informasi) yang akan dikirimkan (P).kemudian menghitung ciphertext (c) sesuai dengan :

$C = p^e mod\ n$……[2.1]

Deskripsi adalah mendapatkan data maupun informasi yang telah dienkripsi atau disandikan (n,e) dari pengirim (p) untuk membaca daa asli menggunakan kunci privatnya, dapat dienkripsi dengan :

$P = c^d mod\ n$……[2.2]

Enkripsi dan dekripsi harus mengetahui nilai e dan nilai n, satu diantaranya harus memiliki d untuk melakukan dekripsi terhadap hasil enkripsi dengan menggunakan *public key* e. Syarat nilai e dan d adalah gcd(d,e)=1. Berikut contoh proses pembangkit kunci, yaitu :

a. Pilih bilangan prima, misalnya p = 3 dan q = 641
b. Hitung n = p*q = 3 x 641 = 1923
c. Hitung n = (p - 1) (q – 1) = 2 x 640 = 1280
d. pilih e yang relative prime terhadap m, ged (e,n) = 1 e = 427 => gcd (427,1280) = 1 nilai e yang diambil adalah 427.

Bukti : (427,1280)
1280 mod 427 = 426
426 mod 427 = 1
1 mod 1 = 0

e. Sehingga cari nilai de = 1 (mod 1280) dan d < 1280
Mencari nilai = d x 427 = 1 mod 1280
d x 427 mod 1280 = 1
d = 427
Bukti : 427 x 3 mod 1280 = 1

Sehingga di dapatkan :

a. public key : e(427), n(1923)
b. private key : d(3), n(1923)

Proses Enkripsi :

Public Key dan *Private Key* sudah diketahui, maka selanjutnya dilakukan enkripsi pada *plaintext* (p) = 10000000 dengan cara mengubah *plaintext* terlebih dahulu ke bentuk ASCII yaitu :

Plaintext:	1	0	0	0	0	0	0	0
ASCII	: 49	48	48	48	48	48	48	48

Setelah dilakukan perubahan dari *plaintext* ke ASCII, pecah menjadi sebuah block yang berukuran 3 digit yaitu :

X1 = 494
X2 = 848
X3 = 484
X4 = 848
X5 = 484
X6 = 800 (diberi penambahan 00)

Maka akan dilakukan perhitungan dengan rumus $C = P^e \bmod n$ untuk proses enkripsi yaitu :

$C1 = 494^{427} \bmod 1923 = 533$ $C4 = 848^{427} \bmod 1923 = 209$
$C2 = 848^{427} \bmod 1923 = 209$ $C5 = 484^{427} \bmod 1923 = 874$
$C3 = 484^{427} \bmod 1923 = 874$ $C6 = 800^{427} \bmod 1923 = 1202$

Gabungkan seluruh hasil dari C1 sampai C6. Hingga hasil yang didapatkan *chipertext* (c) = 533.209.874.209.874.1202 dalam karakter ASCII (*American Standart Code for information Interchage)*. Maka, hasil dari 10.000.000 sudah tersandikan (enkripsi).

Proses dekripsi :

Proses deskripsi dilakukan agar dapat membaca data yang telah dienkripsi. Sebelum dekripsi, tentunya data sudah terenkripsi terlebih dahulu. Kemudian, jika mendekripsikannya kembali digunakan rumus $P = C^d \bmod n$dengan perhitungan :

$P1 = 533^3 \bmod 1923 = 494$ $P4 = 209^3 \bmod 1923 = 848$
$P2 = 209^3 \bmod 1923 = 848$ $P5 = 874^3 \bmod 1923 = 484$
$P3 = 874^3 \bmod 1923 = 484$ $P6 = 1202^3 \bmod 1923 = 800$

Maka, hasil gabungan P1 sampai P6 = 533.209.874.209.874.1202, adalah 10.000.000.

3. PEMBAHASAN DAN HASIL

3.2 Algoritma Sistem

Kunci untuk melakukan enkripsi disebut kunci public, sedangkan kunci untuk melakukan dekripsi disebut sebagai kunci private. Orang yang mempunyai kunci public dapat melakukan enkripsi tetapi dalam melakukan dekripsi hanyalah orang yang mempunyai kunci privat saja. Kunci private banyak dimiliki oleh sembarang orang, tetapi kunci private hanya dimiliki orang tertentu saja.

Proses Pembangkit Kunci

Pembangkit kunci merupakan bilangan yang menentukan kunci enkripsi (public key) dan kunci dekripsi (private key) dengan syarat itu yaitu :

a. Pilihlah bilangan prima sembarang. Bilangan prima adalah bilangan asli yang lebih besar dari 1, yang tidak dapat dibagi oleh bilangan lain kecuali bilangan itu sendiri dan 1 yang tidak dapat dibagi oleh bilangan lain kecuali bilangan itu sendiri dan 1. Karena bilangan prima lebih besar dari 1, maka bilangan prima dimulai dari 2, yaitu 2,3,5,7,11,13 dan seterusnya. Seluruh bilangan prima adalah ganjil, kecuali 2 yang merupakan bilangan genap. Secara *sistematis* tidak ada "bilangan prima yang terbesar" karena jumlah bilangan prima tak terhingga dan kedua bilangan prima tidak boleh sama antara p dan q dalam pemilihan ini, dipilihlah nilai prima (p)=47 dan quotient (q)= 71.

b. Untuk mencari nilai dari kedua bilangan prima. Maka, perlu dilakukan perkalian yaitu n = p * q = 47 * 71 = 3337.
c. Hitung m = (p – 1)(q – 1) = 46 * 71 = 3220.
d. Pilih nilai e dengan syarat e > 1 dan *greatest common divisior* (e,3220) = 1 nilai e yang diambil adalah 101.

Bukti : (101,3220)
3220 mod 101=89
101 mod 89 = 12
89 mod 12 = 5
12 mod 5 = 2
5 mod 2 = 1
2 mod 1=0

e. Sehingga d e = 1 (mod 3220) dan d < 3220
Mencari nilai = d x 101 = 1 mod 3220
d x 101 mod 3220 = 1
d = 1881
Bukti : 1881 x 101 mod 3220 = 1
Sehingga pasangan kunci yang didapat adalah kunci enkripsi (public key) =(101,3337) dan kunci dekripsi (private key) = (1881,3337).

Proses Enkripsi

Setelah didapat perhitungan diatas, maka akan dilakukan enkripsi plaintext P = 200000 pertama-tama plaintext tersebut diubah menjadi format ASCII sebagai berikut :

Karakter	2	0	0	.	0	0	0
ASCII	50	48	48	46	48	48	48

Setelah dibagi perblock, maka akan dihitung menggunakan rumus sebagai berikut yaitu Ci=Pi ^e mod n.

C1 = 50 ^ 101 mod 3337 = 1071
C2 = 48 ^ 101 mod 3337 = 471
C3 = 48 ^ 101mod 3337 = 471
C4 = 46 ^ 101 mod 3337 = 46
C5 = 48 ^ 101 mod 3337 = 471
C6 = 48 ^ 101 mod 3337 = 471
C7 = 48 ^ 101 mod 3337 = 471

Maka chipertext yang didapatkan C = 1071 471 471 46 471 471 471

Setelah chipertext dari 200.000 didapat, untuk mengubah kembali jadi plaintext menggunakan dekripsi dengan rumus Pi = Ci ^ d mod n.

P1 = 1071 ^ 1881 mod 3337 = 50
P2 = 471 ^ 1881 mod 3337 = 48
P3 = 471 ^ 1881 mod 3337 = 48
P4 = 46 ^ 1881 mod 3337 = 46
P5 = 471 ^ 1881 mod 3337 = 48
P6 = 471 ^ 1881 mod 3337 = 48
P7 = 471 ^ 1881 mod 3337 = 48

Maka, setelah dideskripsi hasil akan sama yaitu 50 48 48 46 48 48 48. Dalam karakter ASCII yaitu :

ASCII	50	48	48	46	48	48	48
Karakter	2	0	0	.	0	0	0

4. KESIMPULAN

Dari hasil pembahasan pada bab sebelumnya dan pengamatan yang telah dilakukan maka dapat diambil kesimpulan diantaranya sebagai berikut:

1. Memecahkan permasalahan yang terjadi berkenaan dengan pengamanan data Simpan Pinjam yaitu menggunakan teknik Kriptografi dengan Algoritma RSA.
2. Untuk merancang Aplikasi Algoritma RSA melalui 3 tahap yang pertama kita harus membangkitkan kunci dengan menggunakan bilangan prima, proses Enkripsi, lalu proses Dekripsi
3. Dengan cara menginstal aplikasi Visual Basic 2010 dan menerapkan pengkodean untuk sistem pengamanan yang sudah ditentukan untuk teknik kriptografi dan algoritma RSA
4. Untuk menguji sistem yang dirancang dilihat dari kualitas perangkat lunak dan mempresentasikan kajian pokok dan spesifikasi, desain dan pengkodean dalam menjalankan sebuah program seperti pengujian sistem yang telah dirancang berjalan sesuai dengan yang diharapkan.

5. Implementasi sistem keamanan data menggunakan 2 buah kunci dan prosesnya sedikit lama, karena harus memfaktorkan bilangan prima untuk mendapatkan dua buah kunci agar tidak mudah dipecah oleh pihak lain yang tidak berkepentingan bagi para anggota di CU Suka Makmur

REFERENSI

[1] Shadikin, F. 2012.Kriptografi Untuk Keamanan Jaringan.
[2] A.S Rosa, & M. Shalahuddin. 2013. Rekayasa Perangkat Lunak. Yogyakarta : Informatika
[3] Tri Rahajoeningroum, Muhammad Aria. Studi dan Implementasi Algoritma RSA UntukPengamanan Data Transkip Akademik Mahasiswa. UNIKOM, 8 (1),79
[4] Albert, G., R. Rizal, I., & Ike, P. W. 2015. Implementasi Algoritma Kriptografi RSA untuk Enkripsi dan Dekripsi Email. Jurnal Teknologi dan Sistem Komputer, 3(2), 254
[5] Sulindawati & Fathoni, M. 2010. Ilmu Pengantar Analisa Perancangan Sistem. Jurnal Santikom, 2 (9), 14