KRIPTOGRAFI TEKS DENGAN MENGGUNAKAN ALGORITMA LUC

Ragil Saputra, Bambang Yismianto, Suhartono
Program Studi Ilmu Komputer Jurusan Matematika
FMIPA Universitas Diponegoro
Jl. Prof. Soedarto, Kampus UNDIP Tembalang, Semarang

Abstrak: Salah satu metode untuk mengamankan data atau informasi adalah dengan metode kriptografi. Algoritma LUC merupakan metode kriptografi dengan menggunakan dua kunci yang berbeda dalam kriptosistemnya. Untuk mengenkripsi file teks digunakan fungsi enkripsi yang menggunakan sebuah sebuah kunci publik, hasil enkripsi berupa file terenkripsi yang aman dari pengganggu. Selanjutnya dengan mendekripsi file terenkripsi di gunakan fungsi dekripsi dengan menggunakan kunci privat akan menghasilkan kembali file teks yang sama dengan aslinya. Operasi pada Algoritma LUC dilakukan dalam domain bilangan, oleh karena itu sebelum dilakukan enkripsi, teks terlebih dahulu di konversi kedalam bentuk angka.

Kata Kunci: Kriptografi, Algoritma LUC, Enkripsi, Dekripsi

PENDAHULUAN

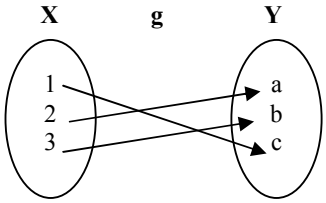
Dalam era konektifitas sekarang ini, dimana setiap informasi dapat diakses dengan mudah, maka keamanan data benar-benar menjadi permasalahan yang sangat penting. Perkembangan komputer dan interkoneksinya melalui jaringan telah meningkat sehingga membutuhkan keamanan data dan informasi yang handal agar terhindar dari serangan (attack). Salah satu cara untuk mengamankan data dan informasi adalah dengan menyandikan informasi tersebut.

Kriptografi adalah seni untuk mengamankan informasi atau plainteks dengan menggunakan teknik penyandian. Proses penyandian informasi asli (plainteks) disebut enkripsi yang menghasilkan informasi tersandikan (ciperteks), sedangkan proses menguraikan ciperteks menjadi informasi asli disebut dekripsi. Dalam proses enkripsi dan dekripsi diperlukan dapat menggunakan kunci yang berbeda. Salah satu metode dalam kriptografi yang menggunakan kunci berbeda adalah Algoritma LUC. Kunci untuk melakukan enkripsi disebut dengan kunci publik (public key) sedangkan dekripsi menggunakan kunci rahasia (private key).

TINJAUAN PUSTAKA

Fungsi Bijektif

Jika f adalah fungsi yang injektif dan surjektif maka f disebut bijektif (berkorespondensi satu-satu). Misal X = {1,2,3}, Y = {a,b,c} diberikan fungsi f(1) = c, f(2) = a, f(3) b



Gambar 1. Fungsi Bijektif

Fungsi f merupakan fungsi yang bijektif sebab :

1. f merupakan fungsi yang injektif
   setiap elemen $y \in Y$ yang mempunyai kawan, dan kawannya tepat satu elemen $x \in X$
2. f merupakan fungsi yang surjektif
   setiap elemen $y \in Y$ dikawankan dengan elemen $x \in X$.

Fungsi Berivers Satu Sama Lain

Misalkan f dan g fungsi bijektif. Fungsi f dan g dikatakan berinvers satu sama lain jika f(g(x)) = x, x adalah elemen dalam domain fungsi g, dan g(f(x)) = x, x adalah elemen dalam domain fungsi f.

Faktor Persekutuan Terbesar

Misalkan a,b,c dan d $\in$ Z, d disebut Faktor Persekutuan Terbesar (FPB) atau *Great Common Divisor*) dari a dan b jka :

(i) d > 0
(ii) d | a dan d | b
(iii) Jika c|a dan c | b maka c | d

Notasi : d = FPB(a,b)

Dua buah bilangan dikatakan relatif prima jika Faktor Persekuan Terbersarnya adalah 1, FPB(a,b) = 1.

Kelipatan Persekutuan Terkecil

Misalkan a,b,c dan d $\in$ Z, d disebut Kelipan Persekutuan Terkecil (KPK) atau *Least Common Multiple*) dari a dan b jika :

(i). d >0
(ii). A | d dan b | d
(iii). Jika a | c dan b | c maka d | c

Notasi : d = KPK(a,b)

Kongruensi Modulo

Jika a,b $\in$ Z maka a kongruen ke b modulo n jika hanya jika n membagi (a-b), ditulis a $\equiv$ b (mod n)

Invers Perkalian Modulo

Misalkan a $\in$ Z_n dan FPB(a,n) = 1. Perkalian invers a modulo n adalah sebuah bilangan bulat tunggal x $\in$ Z_n sedemikian sehingga ax $\equiv$ a (mod n)

Barisan Lucas

Barisan Lucas merupakan dua buah deret U_n dan V_n yang dibangun oleh dua bilangan bulat positif P dan Q. Kemudian dibangun sebuah persamaan kuadrat :

$X^2 - PX + Q = 0$.

Akar dari persamaan adalah $\left(P \pm \sqrt{P^2 - 4Q}\right)/2$. Bagian $\left(P^2 - 4Q\right)$ disebut Diskriminan atau D. Dimisalkan kedua akar sebagai :

$\alpha = \frac{P + \sqrt{D}}{2}$ dan $\beta = \frac{P - \sqrt{D}}{2}$, sesuai persamaan tersebut α dan β dapat diperlihatkan $\alpha + \beta = P, \alpha\beta = Q, \alpha - \beta = \sqrt{D}$ diasumsikan pemilihan D $\neq$ 0.

Kemudian barisan Lucas didefinisikan sebagai berikut :

$U_n(P,Q) = \frac{\alpha^n - \beta^n}{\alpha - \beta}$ dan $V_n(P,Q) = \alpha^n + \beta^n$, untuk n $\geq$ 2 :

$V_n(P,Q) = PV_{n-1}(P,Q) - QV_{n-2}(P,Q)$ dan $U_n(P,Q) = PU_{n-1}(P,Q) - QU_{n-2}(P,Q)$

Sebagai contoh dimisalkan P = 3, Q = 1, 10 barisan Lucas pertama :

Tabel 1. Perhitungan Barisan Lucas sampai n = 10

n	0	1	2	3	4	5	6	7	8	9	10
$V_n(3,1)$	2	3	7	18	47	123	322	843	2.207	5.778	15.127
$U_n(3,1)$	0	1	3	8	21	55	144	377	987	2.584	6.765

PEMBAHASAN

Kriptografi

Secara umum kriptografi dapat diartikan sebagai kajian terhadap teknik-teknik yang bersifat matematis yang berkaitan dengan aspek keamanan informasi atau data seperti kerahasiaan, integritas data, otentifikasi data dan otentifikasi entitas.

Tranformasi Kunci Enkripsi Dan Dekripsi

Sebuah skema enkripsi terdiri atas transformasi enkripsi $\{E_e : e \in K\}$ dan transformasi dekripsi $\{D_d : d \in K\}$ dengan setiap $e \in K$ maka terdapat dengan tunggal $d \in K$ sedemikian sehingga $D_d : E_e^{-1}$. D_d dan E_e merupakan fungsi yang berinvers satu dengan yang lain sehingga didapat $D_d(D_d(m)) = m$, $\forall m \in M$.

Proses penyandian menggunakan E_e terhadap $m \in M$ disebut enkripsi. Proses penguraian sandi dengan D_d terhadap $c \in C$ disebut dekripsi. Skema enkripsi terdiri dari ruang plainteks M, ruang ciperteks C, dan ruang kunci K.

Barisan Lucas dalam Kriptografi

Dalam pengembangan barisan Lucas sebagai sebagai algoritma dalam kriptografi, yang akan digunakan hanya pada fungsi Lucas $V_n(P,Q)$. Pertambahan nilai barisan Lucas sampai dengan n suku sangat cepat, sehingga dikembangkan fungsi modulo $N > 2$. Dengan mengaplikasikan operasi modulo dalam tiap langkahnya didapatkan hasil yang sama. Sehingga memenuhi persamaan :

$V_n(P \bmod N, Q \bmod N) = V_n(P,Q) \bmod N$

Jika $Q = 1$ maka didapatkan fungsi : $V_n(P,1) \bmod N$

Sehingga fungsi Lucas yang akan dipakai dalam algoritma LUC adalah :

$V_{de}(P,1) \equiv P \bmod N$

Aplikasi selanjutnya dalam kriptografi yaitu nilai e dan d disebut kunci, dengan e adalah kunci enkripsi dan d adalah kunci dekripsi. P merupakan plainteks asli dengan $P < n$, sebuah plainteks akan dienkripsi dengan fungsi Lucas sehingga :

$V_e(P \bmod N,1) \equiv C$, dengan C adalah ciperteks

Kemudian ciperteks didekripsi dengan barisan Lucas yang lain yaitu :

$V_d(C \bmod N,1) \equiv P$

Algoritma LUC

Algoritma LUC merupakan salah satu algoritma dalam kriptografi kunci umum, algoritma dibangun berdasarkan fungsi matematika yaitu barisan Lucas yang telah didefinisikan sebelumnya :

$f_{luc}(P) = V_n(P,1) \bmod N$

Dalam algoritma LUC terdapat tiga bagian utama yaitu pembangkit kunci, proses enkripsi, dan proses dekripsi.

1. Pembangkitan Kunci

   Dalam algoritma LUC pada saat membangkitkan sepasang kunci membutuhkan dua buah bilangan prima p dan q. Kemudian dikalikan menghasilkan nilai modulus $N \in Z$.

   (1) $N = p \times q$

   Dihitung nilai fungsi perluasan euler $\Phi(N)$:

   (2) $\Phi(N) = (p-1)(p+1)(q-1)(q+1)$

   Sebuah bilangan bulat, $e \in Z$, $1 < e < \Phi(N)$, yang disebut kunci enkripsi, kemuadian dicari semikian sehingga e dan $\Phi(N)$ berelatif prima. Faktor Persekutuan Terbesar (FPB) dari e dan $\Phi(N)$ adalah 1.

   (3) $FPB(e, \Phi(N)) = 1$

   Nilai (e,N) kemudian dipublikasikan sebagai kunci publik algoritma LUC.

   Setelah kunci publik diperoleh, langkah selanjutnya menghitung kunci dekripsi (kunci privat) d diperoleh dengan terlebih dahulu menghitung nilai D (diskriminan) barisan Lucas :

   (4) $D = m2 - 4$, dimana m adalah plainteks yang akan dienkripsi.

   Kemudian dicari Kelipatan Persekutuan Terkecil (KPK) dari fungsi Lehmer Totient sehingga diperoleh :

   (5) $$S(N) = KPK\left[\left(p - \left(\frac{D}{p}\right)\right), \left(q - \left(\frac{D}{q}\right)\right)\right]$$

   Karena simbol Legendre mempunyai nilai 1 dan -1 maka nilai S(N) mempunyai empat kemungkinan yaitu :

   $S(N) = KPK[(p-1),(q-1)]$

   $S(N) = KPK[(p-1),(q+1)]$

   $S(N) = KPK[(p+1),(q-1)]$

   $S(N) = KPK[(p+1),(q+1)]$

   Sehingga nilai kunci dekripsi d mempunyai empat kemungkinan tergantung dari nilai S(N), dan diperoleh dengan mencari invers perkalian modulo S(N) :

   (6) $ed \equiv 1 \bmod S(N)$

   Nilai (d,N) merupakan kunci dekripsi (kunci privat) pasangan dari (e,N).

2. Algoritma Enkripsi LUC
   Plainteks m akan dienkripsi dengan kunci publik e yang diperoleh dari hasil pembangkit kunci. Fungsi enkripsi didefinisikan sebagai berikut :
   $f_{enk}(M) = V_n(M,1) \bmod N$
   Fungsi enkripsi akan menghitung suku ke-n dari barisan Lucas dengan indeks n adalah kunci publik e dan M adalah plainteks. Sehingga untuk mengenkripsi plainteks $m \in M$ dan kunci publik LUC (e,N) dinyatakan sebagai :
   $c = V_e(m,1) \bmod N$
   Proses enkripsi menghasilkan ciperteks $c \in C$.
3. Algoritma Dekripsi LUC
   Ciperteks $c \in C$ diperoleh dari algoritma enkripsi LUC, langkah selanjutnya yaitu proses dekripsi ciperteks $c \in C$ menjadi plainteks asli $m \in M$ dengan kunci privat. Fungsi dekripsi didefinisikan sebagai :
   $f_{dek}(C) = V_n(C,1) \bmod N$
   Untuk mendekripsi $c \in C$ dan kunci privat LUC (d,N) untuk mendapatkan plainteks $m \in M$ dinyatakan sebagai :
   $m = V_d(c,1) \bmod N$

Imlementasi Algoritma LUC

Implementasi Algoritma LUC dalam melakukan enkripsi, setiap karakter dari string berupa teks / plainteks yang dimasukkan dikonversi ke dalam bentuk bilangan dengan kode ASCII (*American Standard Code for Information Interchange*) dan inputan plainteks berupa file berecord, setiap kalimat merupakan satu record. Dan plainteks dipecah kedalam blok berisi 2 karakter kemudian dienkripsi tiap-tiap blok, ciperteks yang diperoleh merupakan hasil dari gabungan dari blok-blok plainteks yang telah terenkripsi. Kemudian ciperteks didekripsi tiap-tiap blok dan dikonversi kembali dengan kode ASCII untuk menghasilkan plainteks yang diinginkan.

Sebagai contoh teks “Algorithm” akan dienkripsi dengan algoritma LUC, plainteks dibagi dalam blok yang berisi dua karakter, jika blok terakhir hanya berisi 1 karakter maka di tambah dengan spasi/blank. Sehingga setelah dikonversi dengan kode ASCII menjadi 5 blok plainteks, M = 3477 7280 8374 8573 7801
Dari hasil Pembangkitan kunci diperoleh bilangan prima p = 47, bilangan prima q = 241 dan kunci publik (e,N) = (7,11327) dan kunci privat (d,N) = (103,11327), kemudian setiap blok plainteks M dienkripsi dengan fungsi enkripsi menghasilkan ciperteks :
C = 4749 6482 3387 9470 942
Kemudian setiap blok ciperteks didekripsi dengan fungsi dekripsi menghasilkan :
M = 3477 7280 8374 8573 7801
Plainteks M dikonversi kedalam bentuk teks dengan kode ASCII didapatkan teks asli kembali “Algorithm”

KESIMPULAN

Kunci dekripsi pada algoritma LUC tergantung pada kunci enkripsi dan dipengaruhi oleh simbol legendre plainteks dengan bilangan prima p dan q, setiap satu kunci enkripsi mempunyai empat kemungkinan kunci dekripsi

Operasi pada Algoritma LUC dilakukan dalam domain bilangan, oleh karena itu sebelum dilakukan enkripsi, teks terlebih dahulu di konversi kedalam bentuk bilangan. Hasil enkripsi berupa teks yang telah disandikan dalam bentuk bilangan.

DAFTAR PUSTAKA

[1]. Albertson, Michael O. and Joan P. Hutchinson, *Discrete Matematics With Algorithms,* John Wiley & Sons Inc., Canada, 1988.

[2]. Glbert, Jimmie, *Element of Modern Algebra*, Third Edotion, The Pridel, Weber & Schmidt Press, 1989.

[3]. Hillman, Abraham P. and Gerald L. Alexanderson, *Abstrak Algebra*, Fifth Edition, PWS Publhising Company, Boston, 1994

[4]. Menezes, A. P.van Oorschot, and Vanstone, S., *Handbook of Applied Cryptography*, CRC Press, 1996.

[5]. Scheier, Bruce., *Applied Cryptography*, Second Edition, John Wiley & Sons Inc., Canada, 1996.

[6]. Simmons, Gustavus J,. *Contemporary Cryptograpy,* IEEE Pres, New York, 1991.

[7]. Smith, Peter J. and Michael J.J. Lennon., *LUC : A New Publik Key System*, University of Auckland, New Zealand, 1993.