BAB II

LANDASAN TEORI

Algoritma LUC adalah algoritma yang dibangun berdasarkan penggunaan prinsip-prinsip dasar matematika, diantaranya fungsi modulo, teori bilangan untuk membangkitkan kunci umum maupun kunci rahasia serta penggunaan barisan Lucas untuk melakukan enkripsi maupun dekripsi. Teori-teori penunjang tersebut yang akan digunakan dalam pembahasan pada bab III.

2.1. Fungsi

Definisi 2.1.1 Himpunan

Himpunan adalah kumpulan benda atau obyek yang berbeda dengan syarat keanggotaan yang jelas.

Obyek dari suatu himpunan disebut dengan elemen atau anggota himpunan.

Contoh 2.1.1

Sebuah himpunan X yang terdiri dari atas elemen p,q,r dan s dinotasikan dengan $X = \{p,q,r,s\}$.

Definisi 2.1.2 Fungsi

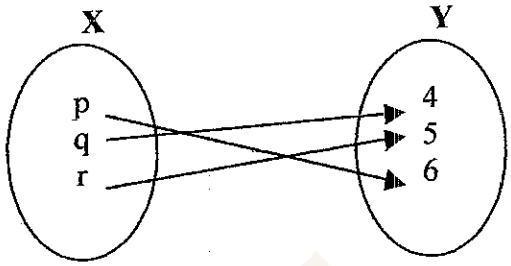
Misalkan X dan Y adalah dua buah himpunan. Fungsi f dari X dan Y adalah perkawanan dengan suatu aturan f antara setiap elemen $x \in X$ dengan tepat satu elemen $y \in Y$.

Notasi: $f : X \rightarrow Y, (\forall x \in X)(\exists ! y \in Y) \Rightarrow f(x) = y$.

X disebut dengan domain dan Y disebut kodomain.

Contoh 2.1.2

Misalkan X = {p,q,r} dan Y = {4,5,6}, diberikan suatu fungsi f (p) = 6, f (q) = 4 dan f (r) = 5. fungsi f diatas dapat digambarkan sebagai berikut :



Gambar 2.1 Fungsi dari himpunan X terhadap Y

Fungsi f merupakan fungsi karena $\forall x \in X$ mempunyai kawan tepat satu elemen $y \in Y$.

Definisi 2.1.3 Fungsi Injektif

Suatu fungsi $f : X \rightarrow Y$ disebut fungsi satu-satu atau injektif jika dan hanya jika untuk setiap $y \in Y$ yang mempunyai kawan, kawannya tepat satu $x \in X$ sedemikian sehingga $f(x) = y$.

Notasi: $f : X \rightarrow Y, (\exists y \in Y)(\exists ! x \in X) \Rightarrow f(x) = y$.

Contoh 2.1.2 merupakan contoh fungsi injektif.

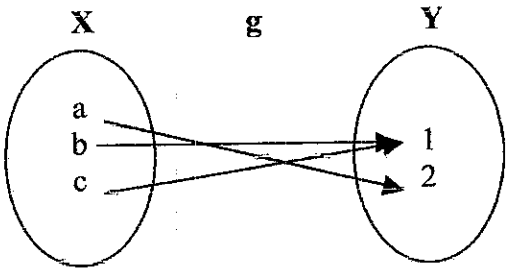
Definisi 2.1.4 Fungsi Surjektif

$f : X \rightarrow Y$ disebut surjektif atau onto jika dan hanya jika untuk setiap $y \in Y$ dikawankan dengan satu atau lebih dari satu elemen $x \in X$ dengan $f(x) = y$.

Notasi: $f : X \rightarrow Y, (\forall y \in Y)(\exists x \in X) \Rightarrow f(x) = y$.

Contoh 2.1.3

Misal X = {a,b,c}, Y = {1,2) diberikan fungsi g sebagai berikut:



Gambar 2.2 Fungsi Surjektif

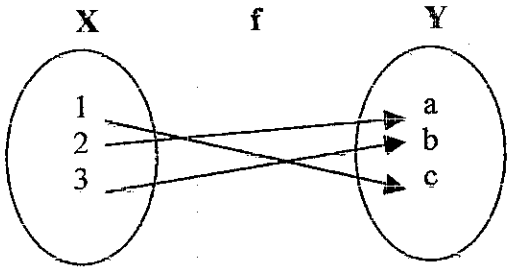
Fungsi g merupakan fungsi surjektif sebab setiap elemen y ∈ Y dikawankan dengan satu atau lebih dari satu elemen x ∈ X.

Definisi 2.1.5 Fungsi Bijektif

Jika f adalah fungsi yang injektif dan surjektif maka f disebut bijektif (berkorespondensi satu-satu).

Contoh 2.1.4

Misal X = {1,2,3}, Y = {a,b,c} diberikan fungsi f (1) = c, f (2) = a, f (3) = b.



Gambar 2.3 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.

Dari contoh diatas dapat disimpulkan bahwa jika himpunan X dan Y mempunyai banyak elemen himpunan yang sama dan f : X $\rightarrow$ Y fungsi injektif maka f merupakan fungsi bijektif.

Definisi 2.1.6 Fungsi Invers

Misalkan f fungsi bijektif dari X dan Y. fungsi invers dari f adalah suatu fungsi bijektif yang mengawankan setiap elemen y $\in$ Y ke elemen x $\in$ X dengan $f^{-1}(y) = x$.

Notasi: $f : X \rightarrow Y, \Rightarrow f^{-1} : Y \rightarrow X, f^{-1}(y) = x, y \in Y, x \in X$.

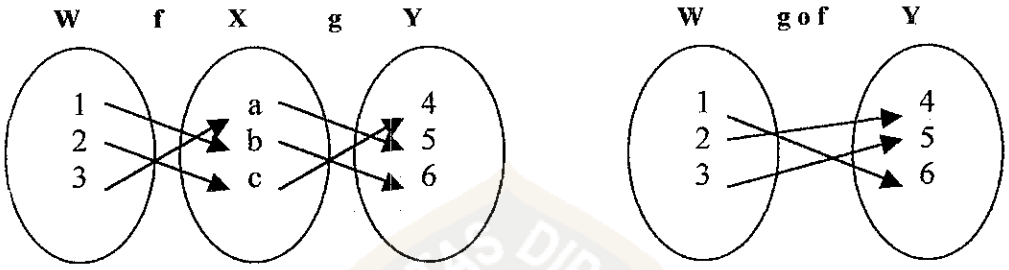
Definisi 2.1.7 Fungsi Komposit

Misalkan f : W $\rightarrow$ X dan g : X $\rightarrow$ Y maka fungsi komposit g dengan f, dinotasikan dengan g $\bullet$ f, adalah suatu fungsi dari himpunan W ke himpunan Y.

Notasi : $g \bullet f(w) = g(f(w)) = y, w \in W, y \in Y$.

Contoh 2.1.5

Misal W = {1,2,3}, X={a,b,c} dan Y={4,5,6}, f : W → X dan g : X → Y dengan f (1) = b, f (2) = c, f (3) = a, g (a) = 5,g (b) = 6 dan g (c) = 4 maka fungsi komposit g • f (w) dinyatakan sebagai berikut :



Gambar 2.4 Fungsi Komposit

Definisi 2.1.8 Fungsi berinvers 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.

Contoh 2.1.6

Misalkan f(x) = 2x + 3 dan g(x) = $\left(\frac{x-3}{2}\right)$ maka :

(i). $f(g(x)) = 2.\left(\frac{x-3}{2}\right) + 3 = x$

(ii). $g(f(x)) = \frac{(2x+3)-3}{2} = x$

Dari hasil (i) dan (ii), maka dapat disimpulkan bahwa f (x) dan g (x) merupakan fungsi-fungsi yang berinvers satu sama lain.

Definisi 2.1.9 Fungsi Satu Arah

F : X $\rightarrow$ Y disebut fungsi satu arah, jika f (x) mudah dihitung untuk setiap x $\in$ X tetapi untuk hampir seluruh y $\in$ Y sangat sulit untuk menentukan nilai inversnya yaitu nilai x $\in$ X sedemikian sehingga f (x) = y.

y = f (x) mudah

$x = f^{-1}(y)$ sulit.

Contoh 2.1.7

Misalkan X = {1,2,3,4,5,6,7,8,9,10} diberikan f (x) = 6x mod 13. Hasil yang akan diperoleh adalah sebagai berikut:

TABEL 2.1 Hasil Fungsi f(x) = 6x mod 13

x	1	2	3	4	5	6	7	8	9	10
f(x)	6	12	5	11	4	10	3	9	2	8

Dari contoh tersebut di atas perhitungan nilai f (x) mudah untuk dikerjakan, tetapi apabila diberikan nilai f (x) = 3 tanpa melihat tabel di atas maka tidak mudah untuk menentukan nilai x sedemikian sehingga f (x) = 3.

Tetapi jika diberikan nilai f (x) = 6 maka dapat dengan mudah didapat nilai x = 1, akan tetapi untuk semua nilai f (x) yang diberikan tidak mudah menghitung nilai x yang bersesuaian tanpa menggunakan alat bantu seperti tabel di atas. Oleh sebab itulah f (x) pada contoh merupakan fungsi satu arah.

Definisi 2.1.10. Fungsi Satu Arah Trapdoor

Fungsi satu arah Trapdoor adalah fungsi satu arah dengan diberikan suatu tambahan informasi yang disebut Informasi Trapdoor untuk mempermudah pencarian invers dari fungsi.

$y = f_k(x)$ mudah

$x = f^{-1}_k(y)$ mudah jika y dan k diketahui

$x = f^{-1}_k(y)$ sulit jika y diketahui dan k tidak diketahui

dengan k adalah informasi trapdoor

Contoh 2.1.7

Diambil bilangan prima p = 43 dan q = 59 maka n = pq = 2537. didefinisikan sebuah fugsi $f(x) = x^4 \bmod n$ dengan $x \in X = \{1,2,3,..,n-1\}$. Misalkan diberikan f(x) = 2388 maka untuk mendapatkan nilai x sedemikian sehingga f(x) = 2388 tidak mudah didapat. Tetapi jika diberikan nilai k = 27029 maka akan didapatkan nilai x dari f(x) = 2388 yaitu x = 91 karena fungsi f(x) dapat dinyatakan dalam bentuk $x^4 = k.n + f(x)$ sehingga $(91)^4 = 27029 . 2537 + 2388$.

Oleh sebab itulah fungsi $f(x) = x^4 \bmod n$ disebut fungsi satu arah trapdoor dengan nilai k sebagai informasi trapdoor.

2.2 Teori Bilangan

2.2.1 Pembagi

Definisi 2.2.1.1 Himpunan Bilangan Bulat

Himpunan {...,-3,-2,-1,0,1,2,3,...} disebut himpunan bilangan bulat dengan notasi Z.

Himpunan {1,2,3,...} disebut himpunan bilangan bulat positif, dengan notasi Z^+.

Definisi 2.2.1.2 Pembagi

Misalkan a,b $\in$ Z, a dikatakan membagi b jika terdapat sebuah bilangan bulat c sedemikian sehingga b = a.c.

Jika a membagi b, ditulis a | b.

Definisi 2.2.1.3 Pembagi Persekutuan

Misalkan a,b $\in$ Z, a $\geq$ 0, b $\geq$ 0. pembagi persekutuan dari a dan b adalah bilangan bulat yang membagi baik a dan b.

Teorema 2.2.1.4

Misalkan a,b,c $\in$ Z. Jika c adalah pembagi persekutuan dari a dan b, maka

(i). c | (a + b)

(ii). c | (a – b)

(iii). Jika c | a, maka c | a.b.

Bukti :

$c \mid a \Rightarrow a = c.q_1$ untuk $q_1 \in Z$ ... (1)

$c \mid b \Rightarrow b = c.q_2$ untuk $q_2 \in Z$ ... (2)

(i). Hasil penjumlahan persamaan (1) dan (2) adalah :

$a + b = c.q_1 + c.q_2 = c.(q_1 + q_2)$

$(q_1 \in Z)\,(q_2 \in Z) \Rightarrow (q_1 + q_2) \in Z$

maka terbukti bahwa c membagi habis (a + b), dengan kata lain $c \mid (a + b)$.

(ii). Hasil pengurangan persamaan (1) dan (2) adalah :

$a - b = c.q_1 - c.q_2 = c.(q_1 - q_2)$

$(q_1 \in Z)\,(q_2 \in Z) \Rightarrow (q_1 - q_2) \in Z$

maka terbukti bahwa c membagi habis (a - b), dengan kata lain $c \mid (a - b)$.

(iii). Persamaan (1) : $(\exists b \in Z) \Rightarrow a.b = c.(q_1.b)$

$(q_1 \in Z)\,(b \in Z) \Rightarrow (q_1.b) \in Z$

sehingga terbukti $c \mid a.b$

Definisi 2.2.1.5 Pembagi Persekutuan Terbesar

Misalkan a,b,c dan $d \in Z$, d disebut Pembagi Persekutuan Terbesar (FPB) atau (*Greatest Common Divisor = gcd*) dari a dan b jika :

(i). $d > 0$

(ii). $d \mid a$ dan $d \mid b$

(iii). Jika $c \mid a$ dan $c \mid b$ maka $c \mid d$

notasi : $d = FPB(a,b)$

FPB(a,b) merupakan bilangan bulat positif terbesar yang membagi a dan b.

Contoh 2.2.1.1

Pembagi persekutuan dari 12 dan 16 adalah {1,2,4} maka FPB(12,16) = 4.

Definisi 2.2.1.6 Kelipatan Persekutuan Terkecil

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

(i). $d > 0$

(ii). $a \mid d$ dan $b \mid d$

(iii). Jika $a \mid c$ dan $b \mid c$ maka $d \mid c$

Notasi : d = KPK(a,b).

KPK (a,b) adalah bilangan bulat positif terkecil yang dapat dibagi a dan b.

Contoh 2.2.1.2

Misalkan a = 12 dan b = 18 maka KPK(12,18) = 36 sebab 12 | 36 dan 18 | 36.

Definisi 2.2.17 Algoritma Pembagian

Jika a,b $\in$ Z dengan $a \geq 0$ dan $b > 0$. pembagian bilangan a oleh b menghasilkan sebuah hasil bagi q dan sisa r sedemikian sehingga

$$a = b\,q + r,\ 0 \leq r < b,\ q \geq 0$$

contoh 2.2.1.3

Misalkan a = 40, b = 12 maka q = 3 dan r = 4, sebab 40 = 3.(12) + (4)

Teorema 2.2.1.8

Jika $a \geq 0$, $b > 0$ dan $a = b.q + r$, $0 \leq r < b$ maka FPB(a,b) = FPB(b,r).

Bukti :

Misalkan c adalah pembagi persekutuan dari a dan b.

Teorema 2.2.1.4 (iii) : $c \mid b \quad \Rightarrow c \mid b.q, (q \in Z)$ ..... (1)

Teorema 2.2.1.4 (ii) : $c \mid a, c \mid b.q \quad \Rightarrow c \mid a - b.q\ (= r)$ ..... (2)

Dari persamaan (1) dan (2) : $c \mid b, c \mid r \quad \Rightarrow c = FPB(br)$

Sehingga terbukti FPB(a,b) = FPB(b,r).

Contoh 2.2.1.4

Contoh 2.2.1.3 didapat bahwa FPB (40,12) = 4 dan FPB (12,4) = 4 sehingga FPB (40,12) = FPB (12, 4) = 4.

Teorema 2.2.1.9 Algoritma Euclid

Misalkan $a \geq 0, b > 0$ dan

$$a = bq_0 + r_1 \quad ,0 \leq r_1 < b,$$

$$b = r_1q_1 + r_2 \quad ,0 \leq r_2 < r_1,$$

$$r_1 = r_2q_2 + r_3 \quad ,0 \leq r_3 < r_2,$$

$$\vdots$$

$$r_n = r_{n+1}q_{n+1} + r_{n+2} \quad ,0 \leq r_{n+2} < r_{n+1},$$

maka terdapat suatu bilangan bulat terkecil n sedemikian sehingga $r_{n+1} = 0$

$$r_{n-1} = r_nq_n + r_{n+1}, r_{n+1} = 0$$

Bukti :

Definisi 2.2.1.7 : $b \mid a \Rightarrow a = b.q_0 + r_1, \quad 0 \leq r_1 < b,$

Teorema 2.2.1.8 : FPB(a,b) = FPB(b,r_1)

$(r_1 \neq 0), (r_1 \mid b) \Rightarrow b = r_1.q_1 + r_2, \quad 0 \leq r_2 < r_1$

Teorema 2.2.1.8 : FPB(b,r_1) = FPB(r_1,r_2)

Demikian seterusnya terjadi pembagian r_i dengan r_{i+1} dengan $r_{i+1} \neq 0$.

Karena $r_1 > r_2 > r_3 >$ ... maka akhirnya terdapat $r_i = 0$.

Misalkan r_{n+1} merupakan sisa pertama yang nol maka berdasarkan teorema 2.2.1.8

FPB(a,b) = FPB(b,r_1) = ... = FPB(r_n,r_{n+1}) = FPB(r_n,0)

Karena FPB(r_n,0) = r_n maka FPB(a,b) = FPB(r_n,0) = r_n

Jadi pembagi persekutuan terbesar dari a dan b akan menjadi sisa hasil pembagian terakhir yang tidak nol.

Contoh 2.2.1.5

Pembagi persekutuan terbesar dari 803 dan 154 dengan menggunakan algoritma Euclid adalah sebagai berikut :

$$803 = 5 \cdot 154 + 33, \quad (q_0 = 5, r_1 = 33)$$

$$154 = 4 \cdot 33 + 22, \quad (q_1 = 4, r_2 = 22)$$

$$33 = 1 \cdot 22 + 11, \quad (q_2 = 1, r_3 = 11)$$

$$22 = 2 \cdot 11 \quad (q_3 = 2, r_4 = 0)$$

Karena sisa hasil pembagian terakhir yang tidak nol adalah $r_4 = 2$ maka FPB(803,154) = 11.

Definisi 2.2.1.10

Dua bilangan bulat a dan b dikatakan relatif prima jika pembagi persekutuan terbesarnya adalah 1, FPB(a,b) = 1.

Definisi 2.2.1.11

Bilangan bulat $p \geq 2$ disebut sebagai bilangan prima jika bilangan pembagi dari p adalah 1 dan p.

2.2.2 Aritmatika Modulo

Misalkan $n \in Z^+$

Definisi 2.2.2.1 Kongruensi Modulo

Jika $a,b \in Z$ maka a kongruen ke b modulo n jika hanya jika n membagi (a–b), ditulis $a \equiv b \pmod{n}$

Contoh 2.2.2.1

$24 \equiv 9 \pmod{5}$ sebab $5 \mid (24 - 9)$

Teorema 2.2.2.2

Jika $a,b \in Z$ maka a kongruen b modulo n maka terdapat $k \in Z$ sedemikian sehingga

$a = b + k.n$

Bukti :

Definisi 2.2.2.1 : $a \equiv b \pmod{n} \Leftrightarrow n \mid a - b$

Definisi 2.2.1.2 : $n \mid a - b \Leftrightarrow a - b = k.n, k \in Z$

$\Leftrightarrow a = b + k.n$

Definisi 2.2.2.3 Himpunan Bilangan Bulat Modulo n

Himpunan bilangan bulat modulo n ditulis Z_n adalah himpunan yang anggota-anggotanya bilangan bulat modulo n { 0,1,2,3,...,n-1 }. Dimana operasi penjumlahan, pengurangan dan perkalian dalam Z_n dibentuk oleh modulo n.

Contoh 2.2.2.2

Z_8 = { 0,1,2,3,...,7 }. Dalam Z_8, $5 + 4 = 9 \bmod 8 \equiv 1$.

Definisi 2.2.2.4 Invers perkalian modulo n

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 $ax \equiv 1 \pmod n$

Teorema 2.2.2.5

Jika $a \equiv b \pmod n$ dan $c \equiv d \pmod n$ maka :

(i). $a + c \equiv b + d \pmod n$

(ii). $a.c \equiv b.d \pmod n$

Bukti :

Teorema 2.2.2.2 : $a \equiv b \pmod n$ $\quad a = b + n.k_1, k_1 \in Z$ .....(1)

$c \equiv d \pmod n$ $\quad c = d + n.k_2, k_2 \in Z$ .....(2)

(i). Operasi penjumlahan dari persamaan (1) dan (2) didapat

$a + c = (b + n.k_1) + (d + n.k_2)$

$= b + d + n.(k_1 + k_2)$

$a + c \equiv b + d \pmod n$

(ii). Operasi perkalian dari persamaan (1) dan (2) didapat

$a.c = (b + n.k_1) . (d + n.k_2)$

$= b.d + b.n.k_2 + d.n.k_1 + n.k_1.k_2$

$= b.d + n.(b.k_2 + d.k_1 + n.k_1.k_2)$

$a.c \equiv b.d \pmod n$

Definisi 2.2.2.6 Pasangan Relatif Prima

Bilangan – bilangan bulat $a_1,a_2,a_3,...,a_n$ disebut pasangan relatif prima jika $FPB(a_i,a_j) = 1$, $1 \leq i < j \leq n$.

Contoh 2.2.2.3

Bilangan {10,17,21} merupakan pasangan relatif prima karena FPB(10,17) = 1, FPB(17,21) = 1 dan FPB(10,21) = 1.

Definisi 2.2.2.7 Himpunan Grup Multiplikatif

Himpunan grup multiplikatif dari Z_n adalah $Z_n^* = \{ a \in Z_n \mid FPB(a,n) = 1 \}$, jika n bilangan prima maka $Z_n^* = \{ a \mid 1 \leq a \leq n - 1 \}$

Contoh 2.2.2.4

$Z_8^* = \{ 1,3,5,7 \}$. Dalam Z_8^*, $3 * 5 = 15 \bmod 8 \equiv 7$

$Z_7^* = \{ 1,2,3,4,5,6 \}$. Dalam Z_7^*, $4 * 5 = 20 \bmod 7 \equiv 6$.

Definisi 2.2.2.8 Kuadrat Residu dan Kuadrat Non-residu

Misalkan a $\in Z_n^*$, a dikatakan sebagai kuadrat residu modulo n jika ada x $\in$ Z_n^* sedemikian sehingga $x^2 \equiv a \pmod{n}$. Jika tidak terdapat x yang memenuhi maka a disebut kuadrat non-residu modulo n. Himpunan semua kudrat residu modulo n dinotasikan dengan Q_n dan himpunan semua kuadrat non-residu dinotasikan $\overline{Q}_n$.

Contoh 2.2.2.5

Misalkan bilangan bulat modulo n = 7 maka :

$1^2 = 1 \equiv 1 \pmod{7}$, $4^2 = 16 \equiv 2 \pmod{7}$

$2^2 = 4 \equiv 4 \pmod{7}$, $5^2 = 25 \equiv 1 \pmod{7}$

$3^2 = 9 \equiv 2 \pmod{7}$, $6^2 = 36 \equiv 1 \pmod{7}$

Sehingga kuadrat residu modulo 7 adalah 1,2 dan 4 atau Q_n = { 1,2,4 }dan 3,5,6 merupakan kuadrat non-residu modulo 7 atau $\overline{Q}_n$ = {3,5,6 }.

2.2.3 Fungsi Euler

Untuk n ≥ 1, φ(n) dinotasikan sebuah bilangan integer dalam interval [1,n] yang relatif prima dengan n. Fungsi φ(n) disebut fungsi euler.

Definisi 2.2.3.1 Fungsi Euler

(i) Jika p $\in Z^+$, $\varphi(p) = |Z_p^*|$, $Z_p^* = \{ a \in Z_p \mid FPB(a,p) = 1 \}$, Z_p^* disebut himpunan grup multiplikatif

(ii) Jika p bilangan prima maka $\varphi(p) = p - 1$

(iii) Jika p,q adalah bilangan prima, n = pq maka $\varphi(n) = (p-1)(q-1)$.

Contoh 2.2.3.1

Berikut ini adalah nilai fungsi Euler dari p = 1 sampai p = 10

Tabel 2.3 Nilai Fungsi Euler

p	1	2	3	4	5	6	7	8	9	10
φ(p)	1	1	2	2	4	2	6	4	6	4

Keterangan :

(i) $\varphi(8) = 4$, yaitu diperoleh dari $Z_8^* = \{1,3,5,7\}$, $\varphi(8) = |Z_8^*| = 4$

(ii) $\varphi(5) = 5 - 1 = 4$

(iii) $\varphi(6) = \varphi(3.2) = (3-1)(2-1) = 2$.

2.2.4 Simbol Legendre (*Legendre Symbols*)

Definisi 2.2.4.1 Simbol Legendre

Jika a bilangan bulat positif dan p > 2 adalah bilangan prima maka Simbol Legendre $\left(\frac{a}{p}\right)$ atau L(a,p) akan diberi nilai :

(i). L(a,p) = 0, jika p | a

(ii). L(a,p) = 1, jika a adalah kuadrat residu modulo p

(iii). L(a,p) = -1, jika a adalah kuadrat nonresidu modulo p

Contoh 2.2.4.1

Misalkan a = 15 dan p = 17 terdapat x = 7 yang memenuhi $7^2 = 49 \equiv 15 \pmod{17}$, sehingga 15 dikatakan kuadrat residu modulo 17, dengan demikian simbol legendre $\left(\frac{15}{17}\right) = 1$, dimisalkan a = 10 dan p = 17 maka tidak terdapat x yang

memenuhi $x^2 \equiv 10 \pmod{17}$, sehingga 10 dikatakan dikatakan kuadrat non-residu modulo 17, dengan demikian simbol legendre $\left(\frac{10}{17}\right) = -1$.

2.2.5 Fungsi Lehmer Totient

Definisi 2.2.5.1 Fungsi Lehmer Totient

Untuk setaip bilangan bulat positif N = pq dengan p dan q keduanya bilangan prima yang berbeda serta $\left(\frac{D}{p}\right)$ dan $\left(\frac{D}{q}\right)$ adalah simbol legendre maka fungsi lehmer totient didefinisikan sebagai :

$$T(N) = \left(p - \left(\frac{D}{p}\right)\right)\left(q - \left(\frac{D}{q}\right)\right)$$

Contoh 2.2.5.1

Misalkan p = 17 , q = 29 dan D = 15, maka dari contoh 2.2.4.1 simbol legendre untuk $\left(\frac{15}{17}\right) = 1$ dan simbol legendre untuk $\left(\frac{15}{29}\right) = -1$, karena tidak ada $x < 29$ yang memenuhi $x^2 \equiv 15 \pmod{29}$, sehingga nilai fungsi Lehmer Totient adalah:

$T(N) = (p - 1)(q + 1) = 16 \cdot 30 = 480$.

2.3 Sistem Bilangan Biner

Sistem bilangan biner adalah sistem bilangan yang hanya menggunakan dua simbol yaitu 0 dan 1. Pembacaan bilangan biner dimulai dari kanan, simbol pertama mewakili bilangan satuan atau 2^0, bilangan kedua mewakili bilangan dua-an atau 2^1, bilangan ketiga mewakili bilangan empat-an atau 2^2 dan seterusnya. Secara umum, simbol dengan posisi n, dengan simbol paling kanan pada posisi 0 menyatakan 2^n – an. Bilangan biner dinyatakan dalam bentuk $(j_n\ j_{n-1}\ j_{n-2}\ ..\ j_2\ j_1\ j_0)_2$ dengan j_i adalah bilangan 0 atau 1.

$$\sum_{i=0}^{n} j_i \cdot 2^i = j_0.2^0 + j_1.2^1 + j_2.2^2 + j_3.2^3 + \ldots + j_n.2^n$$

contoh 2.3.1

Bilangan $(1010)_2$ dalam basis 10 (desimal) adalah :

$(1010)_2 = (1.2^3) + (0.2^2) + (1.2^1) + (0.2^0)$

$= 1.8 + 0 + 1.2 + 0$

$= 10$

Algoritma untuk mengkonversi desimal ke biner dapat disajikan sebagai berikut :

1. masukkan bilangan desimal n
2. jika n > 0 maka dilakukan proses :
   a. lakukan pembagian n dengan sisa, dimana sisa adalah sisa pembagian dari (n mod 2)
   b. nilai n akan berubah menjadi hasil pembagian (n div 2)
   c. ulangi langkah a dan b hingga n = 0, kemudian tulis hasil dimulai dari hasil terakhir atau paling bawah.

Contoh 3.2.2

Tabel 2.4 Konversi Bilangan Desimal ke Biner

Perhitungan	Hasil
n ← 10	
	10 mod 2 → 0
n ← 10 div 2 = 5	
	5 mod 2 → 1
n ← 5 div 2 = 2	
	2 mod 2 → 0
n ← 2 div 2 = 1	
	1 mod 2 → 1
n ← 1 div 2 = 0	

Dari tabel diperoleh konversi bilangan desimal $(10)_{10}$ ke biner = $(1010)_2$

2.4 Barisan Lucas

Barisan Lucas adalah dua deret U_n dan V_n yang dibangun oleh dua bilangan bulat positif P dan Q.

2.4.1 Definisi Barisan Lucas

Dipilih dua bilangan bulat positif P dan Q, dan mengingat persamaan kuadrat:

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

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

$$\alpha = \frac{P + \sqrt{D}}{2} \text{ dan } \beta = \frac{P - \sqrt{D}}{2}$$

Sesuai kedua persamaan tersebut α dan β dapat diperlihatkan :

$$\alpha + \beta = P, \qquad \alpha\beta = Q, \qquad \alpha - \beta = \sqrt{D}$$

Diasumsikan pemilihan P dan Q sedemikian hingga $D \neq 0$. Kemudian jumlah barisan Lucas didefinisikan sebagai berikut :

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

Dengan demikian 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 yang pertama :

Tabel 2.5 barisan Lucas sampai n = 10

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

2.5. Definisi Kriptografi

Kriptografi berasal dari bahasa Yunani yaitu kryptos dan graphein, kryptos berarti rahasia dan graphein yang berarti tulisan.

Definisi 2.5.1. Kriptografi

Kriptografi adalah seni tentang penulisan rahasia dengan menggunakan konsep-konsep dasar matematika untuk mengamankan suatu informasi sehingga seorang pengirim dapat mengirim suatu informasi kepada seorang penerima dengan aman

.

Definisi 2.5.2. Kriptosistem

Kriptosistem adalah sistem dalam kriptografi yang membentuk skema enkripsi untuk mengkonversi plainteks ke ciperteks dan ciperteks ke plainteks.

2.6. File

Definisi 2.6.1 File

File atau berkas adalah kumpulan sejumlah komponen bertipe data sama, yang jumlahnya tidak tertentu.

Komponen berkas disebut dengan rekaman atau *record.*