PERHITUNGAN MODULO-26

Contoh:

15 mod 26 = 15 (15 : 26 = 0 sisa 15)

26 mod 26 = 0 (26 : 26 = 1 sisa 0)

35 mod 26 = 9 (35 : 26 = 1 sisa 9)

435 mod 26 =19 (435 : 26 = 16 sisa 19)

− 8 mod 26 = 18 ( 26 – 8) = 18

−58 mod 26 = −6, kemudian –6 mod 26 = 20 (26 – 6 = 20)

Jadi : −58 mod 26 = 20

%SeperDeterminant Modulo 26

clc

Z=[];

seperZ=[];

for Z1=1:25

for i=1:25

if mod((Z1\*i),26)==1

Z=[Z Z1];

seperZ=[seperZ i];

end

end

end

Z

seperZ

Hasilnya :

Z =

1 3 5 7 9 11 15 17 19 21 23 25

seperZ =

1 9 21 15 3 19 7 23 11 5 17 25

%SeperDeterminant Modulo 27

clc

Z=[];

seperZ=[];

for Z1=1:26

for i=1:26

if mod((Z1\*i),27)==1

Z=[Z Z1];

seperZ=[seperZ i];

end

end

end

Z

seperZ

Hasilnya :

Z =

1 2 4 5 7 8 10 11 13 14 16 17 19 20 22 23 25 26

seperZ =

1 14 7 11 4 17 19 5 25 2 22 8 10 23 16 20 13 26

%SeperDeterminant Modulo 28

clc

Z=[];

seperZ=[];

for Z1=1:27

for i=1:27

if mod((Z1\*i),28)==1

Z=[Z Z1];

seperZ=[seperZ i];

end

end

end

Z

seperZ

Hasilnya:

Z =

1 3 5 9 11 13 15 17 19 23 25 27

seperZ =

1 19 17 25 23 13 15 5 3 11 9 27

MENGHITUNG INVERS MATRIK MOD 26

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *Table Determinants’ Reciprocals Modulo 26* | | | | | | | | | | | | |
| Z | 1 | 3 | 5 | 7 | 9 | 11 | 15 | 17 | 19 | 21 | 23 | 25 |
| *Z-1* | 1 | 9 | 21 | 15 | 3 | 19 | 7 | 23 | 11 | 5 | 17 | 25 |

Diketahui matrik K, Tentukan invers matrik K mod 26



Det(K) = 3.5 – 2.3 = 9

Berdasarkan tabel, *Z* = 9 mempunyai *Z – 1* = 3

Cacatan :

Jika nilai det(K) mod 26 tidak terdapat pada tabel Z, maka dapat dipastikan bahwa permasalahan tidak akan terpecahkan(terdapat kesalahan pada matriks key). Jadi harus cari kunci lain. Pada Kasus Hill Cipher, nilai determinan Matriks Key di Mod 26, harus terdapat pada tabel Z.



Mencari invers matrik K ordo 2x2



Jadi  

Untuk matrik yang lain

 

 

 

 

Matrik ordo 3x3



Setelah dihitung, Det(K) = 1889 Z = 1889 mod 26 = 17 maka Z – 1 = 23

Kemudian menghitung matrik adjoint K, diperoleh:









Untuk matrik yang lain

 

**KRIPTOGRAFI: ALGORITMA HILL CHIPPER**

|  |
| --- |
| *Table A– Letters and Their Corresponding Positions* |
| A B C D E F G H I J K L M N O P Q R S T U V W X Y Z |
| 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 0 |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *Table Determinants’ Reciprocals Modulo 26* | | | | | | | | | | | | |
| Z | 1 | 3 | 5 | 7 | 9 | 11 | 15 | 17 | 19 | 21 | 23 | 25 |
| *Z-1* | 1 | 9 | 21 | 15 | 3 | 19 | 7 | 23 | 11 | 5 | 17 | 25 |

Kata-2 yang bisa digunakan sebagai Kunci: JAMU, MALU, dll.

Misalkan Toyes mengirim pesan “UDINUS” pada Bu Erna, dengan menggunakan kunci : MALU, maka proses kriptografinya adalah sebagai berikut.

Kunci K = MALU = 13 1 12 21, dijadikan matrik ordo 2x2 menjadi



Pesan = UDINUS = 21 4 9 14 21 19, dijadikan matrik ordo 2x2 menjadi



Pesan yang dikirim di Enskripsi menjadi Chipper Teks = C



Chipper teks dijadikan huruf = 9 1 25 17 7 4 = I A Y Q G D

Bu Erna menerima pesan C = I A Y Q G D. dan Kunci K = MALU.

Untuk mendeskrip pesan tersebut bu Erna harus menghitung invers dari K = K – 1

Kunci K = MALU = 13 1 12 21, dijadikan matrik ordo 2x2 menjadi





Jadi Z = 1, maka berdasarkan tabel Z – 1 = 1,



Pesan C = I A Y Q G D = 9 1 25 17 7 4 , dijadikan matrik ordo 2x2



Pesan P diperoleh dengan cara P = K – 1 \*C



Pesan = 21 4 9 14 21 19 = UDINUS.