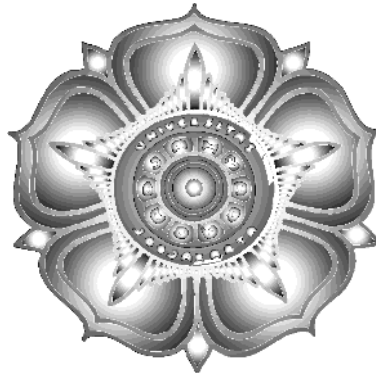


TUGAS MATAKULIAH KRIPTOGRAFI

**PROGRAM VALIDASI MATRIKS KUNCI
SISTEM KRIPTO CIPHER HILL**



DOSEN:
Dra. Diah Junia Eksi Palupi, M.S

DISUSUN OLEH :
Hedri Wahyudi
(07/259575/PPA/2248)

**PROGRAM S2 MAGISTER ILMU KOMPUTER
FAKULTAS MATEMATIKA DAN ILMU PENGETAHUAN ALAM
UNIVERSITAS GADJAH MADA
YOGYAKARTA
2008**

TUGAS KRIPTOGRAFI

PROGRAM VALIDASI MATRIKS KUNCI

SISTEM KRIPTO CIPHER HILL

A. Permasalahan

Pada sistem kriptografi cipher hill, yang dijadikan kunci untuk mengenkripsi suatu plaintext adalah matriks bujur sangkar. Matriks bujur sangkar yang bisa dijadikan kunci adalah matriks invertibel, yaitu matriks yang memiliki invers. Buatlah program untuk menentukan apakah suatu matriks dapat dijadikan kunci pada sistem kriptografi cipher hill atau tidak. Matriks yang digunakan adalah matriks yang berordo 2×2 . Program meminta masukan (input) berupa : elemen-elemen matriks ordo 2×2 . Hasil (output) program adalah suatu keterangan/ pernyataan bahwa matriks bisa atau tidak bisa dijadikan kunci pada sistem kriptografi cipher hill.

B. Analisis

Berdasarkan permasalahan yang dikemukakan tersebut diatas, dilakukan analisis permasalahan. Hasil analisis tersebut adalah sebagai berikut :

1. Program menggunakan bahasa pascal.
2. Matriks yang digunakan adalah matriks ordo 2×2 .
3. Data yang dimasukkan (input) adalah berupa angka. Angka yang dimasukkan adalah empat buah bilangan bulat.
4. Jika determinan matriks (dalam bilangan modulo 26) relatif prima dengan 26, maka matriks tersebut memiliki invers. Sebaliknya jika determinan matriks tidak relatif prima dengan 26 maka matriks tersebut tidak memiliki invers.
5. Untuk menguji kerelatifprimaan determinan matriks dan 26, dilakukan dengan mencari nilai pembagi bersama terbesar kedua bilangan tersebut menggunakan Algoritma Euclid. Jika pembagi bersama terbesar kedua bilangan adalah 1 maka kedua bilangan tersebut relatif prima. Jika pembagi bersama terbesar dari kedua bilangan tidak sama dengan 1 maka kedua bilangan tidak relatif prima.
6. Jika matriks tersebut invertibel (memiliki invers) maka matriks tersebut bisa

dijadikan kunci pada sistem kriptografi cipher hill. Sebaliknya jika matriks tersebut tidak invertibel maka matriks tersebut tidak bisa dijadikan kunci pada sistem kriptografi cipher hill.

C. Desain Program

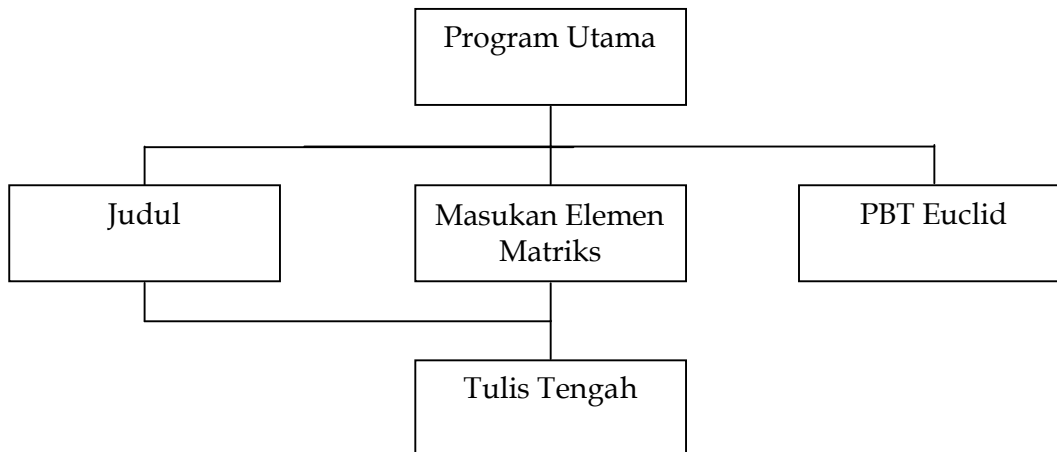
C. 1. Struktur Program

Pada program yang dibuat terdapat beberapa modul. Pada *Tabel Modul Program* dibawah diterangkan nama modul, fungsi dan bentuk implementasinya :

Tabel Modul Program

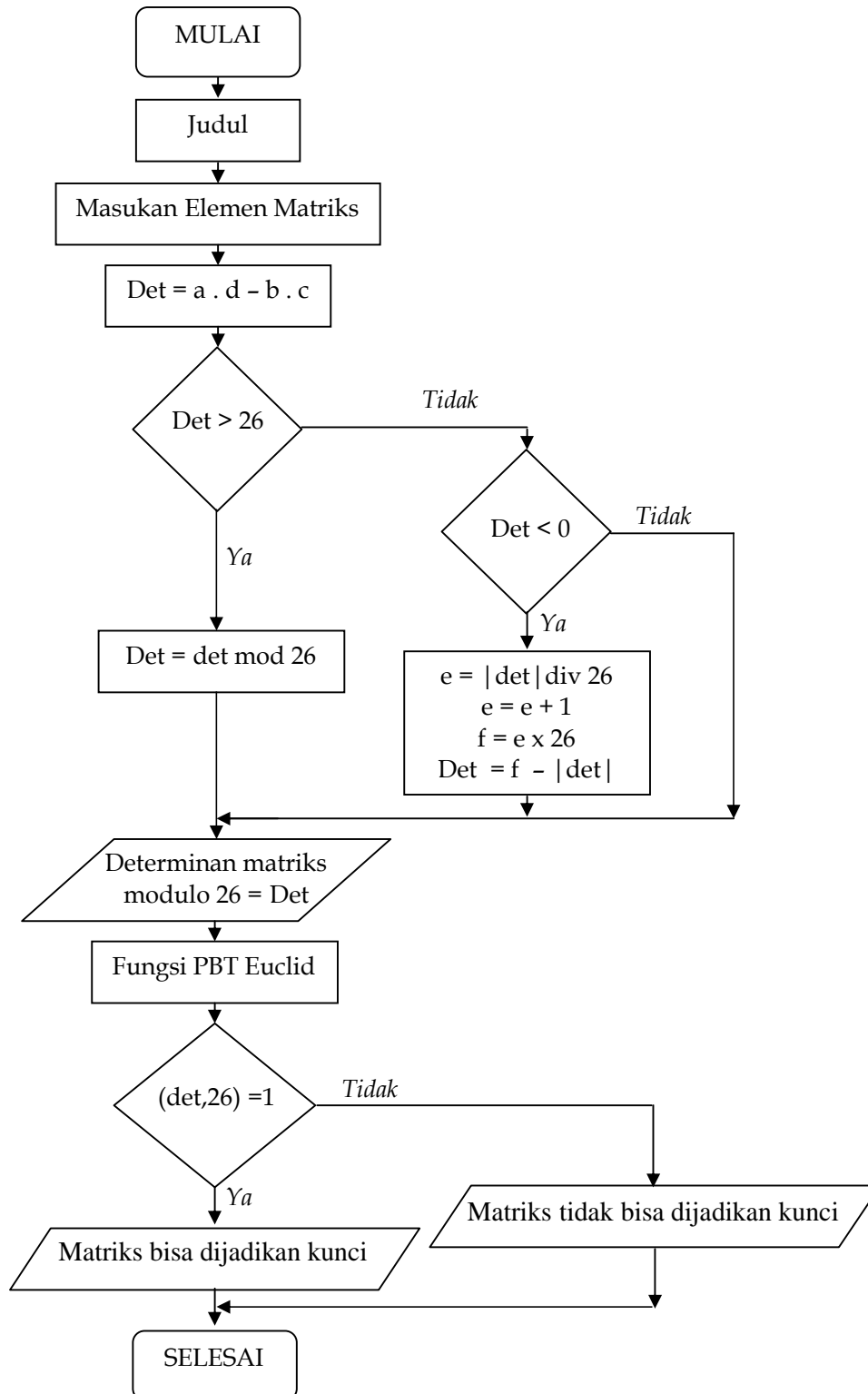
No	Nama Modul	Fungsi	Bentuk Implementasi
1	Judul	Menuliskan judul program	Prosedur
2	Tulis Tengah	Menuliskan sebuah string pada posisi tengah secara horisontal	Prosedur
3	Masukan Elemen Matriks	Memasukkan elemen matriks ordo 2 x 2	Prosedur
4	PBT Euclid	Mencari nilai pembagi bersama terbesar	Fungsi

Struktur program dapat digambarkan sebagai berikut:



Gambar 1 Struktur Modul

C. 2. Algoritma



Gambar 1. Algoritma Program

D. Kode Program

```
1  {
2  Nama Program      : PROGRAM VALIDITAS KUNCI CIPHER HILL
3  Nama File        : validhil.pas
4  Tanggal Dibuat   : 22 April 2008
5  Pembuat          : Hedri Wahyudi
6  Deskripsi        : Program ini meminta input berupa elemen matriks ordo 2 x 2.
7                   Selanjutnya Program akan memberikan output berupa pernyataan
8                   bahwa matriks bisa/ tidak bisa dijadikan kunci dalam sistem
9                   kripto cipher Hill
10 }
11
12
13 Program ValiditasKunciCipherHill;
14 uses wincrt;
15 var a, b, c, d, e, f, det : longint;
16     lagi : char;
17
18
19 {PROSEDUR UNTUK MENULIS STRING DI TENGAH WINDOW}
20 Procedure Tulistengah(x,y:byte;kata:string);
21 begin
22     x := (80-length(kata)) div 2;
23     gotoxy(x,y);
24     write(kata);
25 end;
26
27 {PROSEDUR MENULIS JUDUL}
28 Procedure Judul;
29 begin
30     tulistengah(0, 2, '+=====');
31     tulistengah(0, 3, '|');
32     tulistengah(0, 4, '|');
33     tulistengah(0, 5, '|');
34     tulistengah(0, 6, '|-----');
35     tulistengah(0, 7, '|');
36     tulistengah(0, 8, '|');
37     tulistengah(0, 9, '|');
38     tulistengah(0,10, '|');
39     tulistengah(0,11, '|');
40     tulistengah(0,12, '|');
41     tulistengah(0,13, '|');
42     tulistengah(0,14, '+=====');
43     tulistengah(0, 4, 'PROGRAM VALIDASI VALIDASI MATRIKS KUNCI');
44     tulistengah(0,5, 'SISTEM KRIPTO CIPHER HILL');
45     tulistengah(0, 8, 'TUGAS MATA KULIAH KRIPTOGRAFI');
46     tulistengah(0,10, 'DISUSUN OLEH');
47     tulistengah(0,10, 'HEDRI WAHYUDI');
48     tulistengah(0,12, '(07/259575/PPA/2248)');
49     tulistengah(0,16, '<< Tekan Enter >>');
50     readln;
51     clrscr;
52 end;
53
54 {PROSEDUR UNTUK MEMASUKKAN ELEMEN MATRIKS}
55 Procedure MasukanElemenMatriks(var a, b, c, d:longint);
56 begin
57     tulistengah (0,5, '-----');
58     tulistengah (0,6, 'Masukkan Elemen Matriks Kunci');
59     tulistengah (0,7, '-----');
60     gotoxy (10,9);write ('Elemen Matriks E[1,1] :'); readln (a);
61     gotoxy (46,9);write ('Elemen Matriks E[1,2] :'); readln (b);
62     gotoxy (10,16);write ('Elemen Matriks E[2,1] :'); readln (c);
```

```

63         gotoxy (46,16);write ('Elemen Matriks E[2,2] :'); readln (d);
64         clrscr;
65     end;
66
67
68     {FUNGSI UNTUK Mencari Nilai Pembagi Bersama Terbesar Menggunakan Algoritma
69     EUCLID}
70     Function PBTEuclid (a,b : longint):longint;
71     var R, Q : array [0..10] of integer;
72         m      : integer;
73     begin
74         R[0]:=a;
75         R[1]:=b;
76         m:=1;
77         while R[m]<>0 do
78             begin
79                 Q[m]:=R[m-1] div R[m];
80                 R[m+1]:=R[m-1] - Q[m] * R[m];
81                 m:= m + 1;
82             end;
83         m:= m - 1;
84         PBTEuclid:=R[m];
85     end;
86
87     {-----PROGRAM UTAMA-----}
88
89     begin
90         judul;
91         lagi:='Y';
92         repeat
93             clrscr;
94             MasukanElemenMatriks(a,b,c,d);
95             det:= a * d - b * c;
96             gotoxy (15,5);
97             write ('Determinan matriks yang akan dijadikan kunci = ',det);
98             if det > 26 then det:=det mod 26
99             else
100                 if det<0 then
101                     begin
102                         e:=abs(det) div 26;
103                         e:=e+1;
104                         f:=26 * e;
105                         det:= f - abs(det);
106                     end;
107                 gotoxy (16,7);
108                 write ('Determinan Matriks dalam Bilangan Modulo 26 = ',det);
109                 if PBTEuclid(det, 26)=1 then
110                     begin
111                         gotoxy (6,11);
112                         write('Matriks tersebut bisa dijadikan Kunci dalam Sistem
113                         Kripto Cipher Hill')
114                     end
115                 else
116                     begin
117                         gotoxy (15,10);
118                         write ('Determinan Matriks tidak Relatif Prima dengan
119                         26');
120                         gotoxy (33,12);write ('Dengan demikian');
121                         gotoxy (3,14);
122                         write ('Matriks tersebut tidak bisa dijadikan Kunci
123                         dalam sistem Kripto Cipher Hill');
124                     end;
125                 gotoxy (31,17);write ('Coba Lagi [Y/T] ? ');
126                 readln (lagi);
127                 lagi:=upcase(lagi);

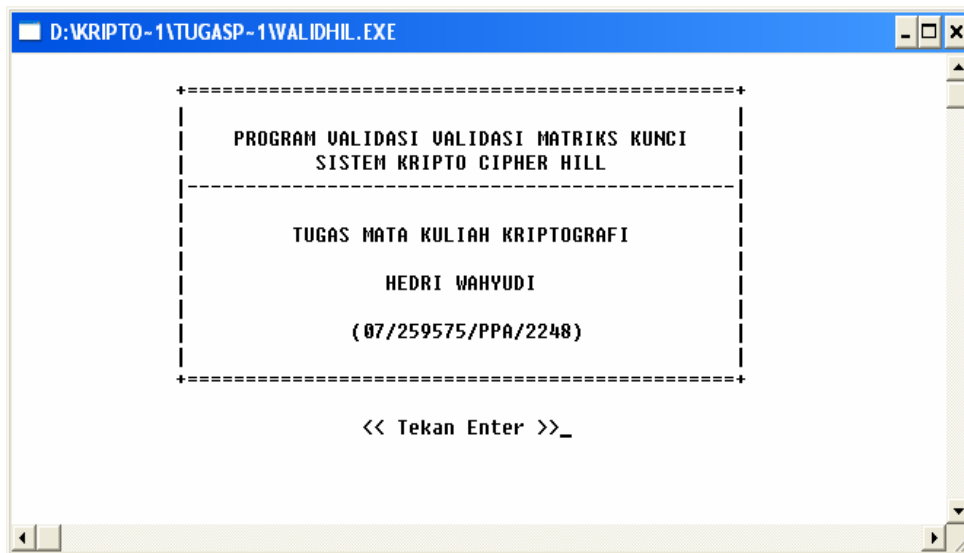
```

```
128     until (lagi='T');
129     clrscr;
130     end.
131
132     {-----AKHIR PROGRAM UTAMA-----}
133
```

E. Hasil Program

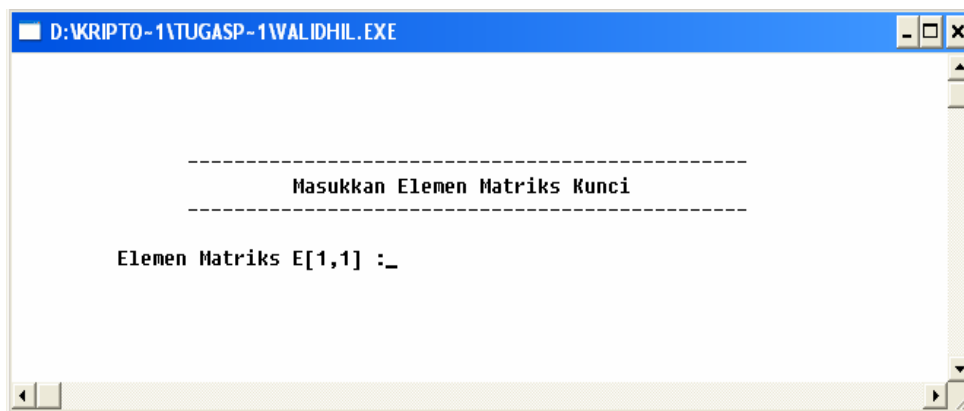
Contoh output program :

1. Setelah program mulai dijalankan akan muncul tampilan awal program seperti gambar 2.



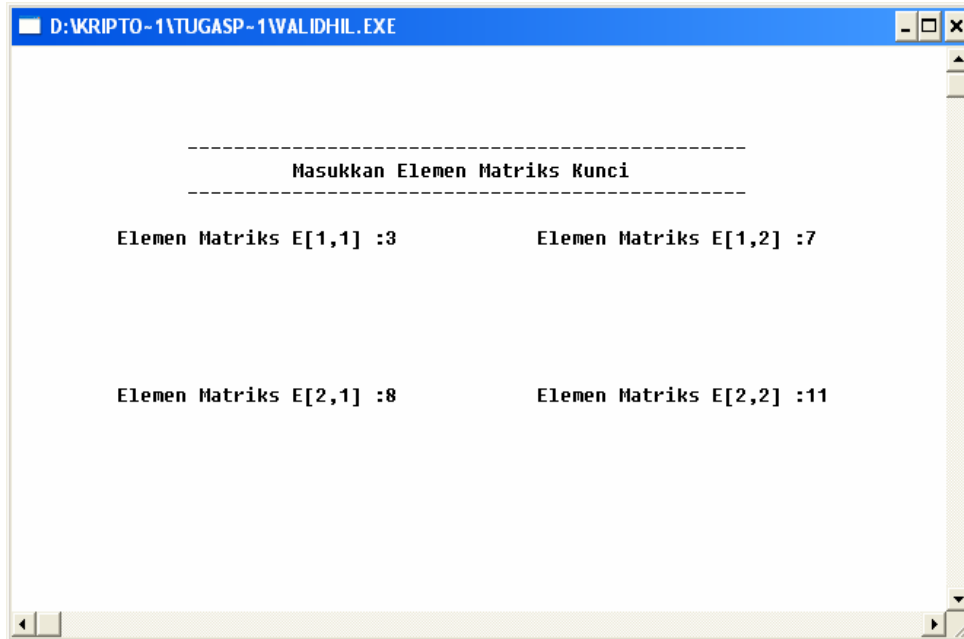
Gambar 2. Tampilan Awal Program

2. Setelah menekan tombol keyboard akan muncul tampilan seperti gambar 3.

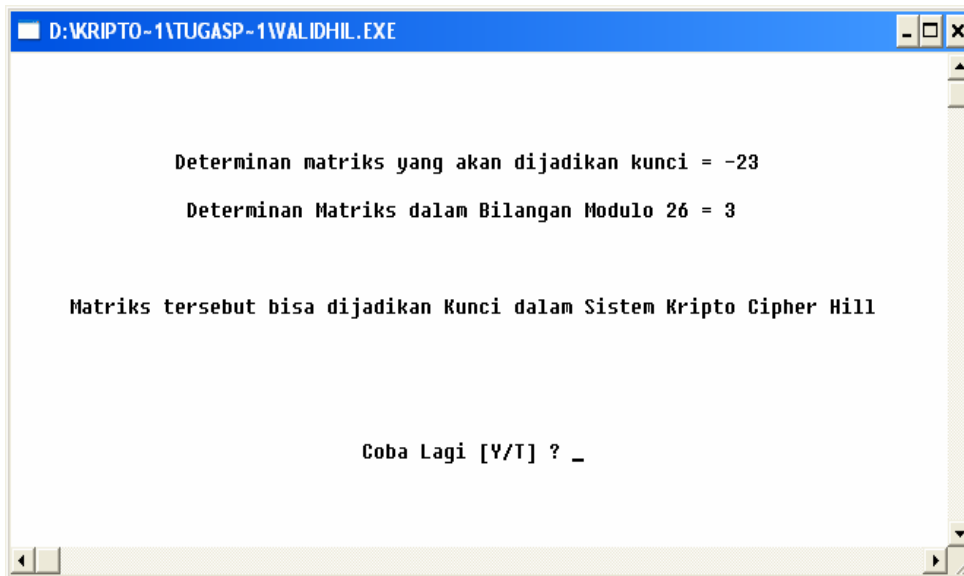


Gambar 3. Menu Input Bilangan

3. Misalkan kita ingin menguji apakah matriks $\begin{pmatrix} 3 & 7 \\ 8 & 11 \end{pmatrix}$ bisa dijadikan kunci pada sistem kriptografi cipher hill. Pada saat program tampil seperti gambar 3, masukkan elemen-elemen matriks tersebut. Perhatikan gambar 4. Setelah menekan enter, akan muncul tampilan hasil program seperti gambar 5.

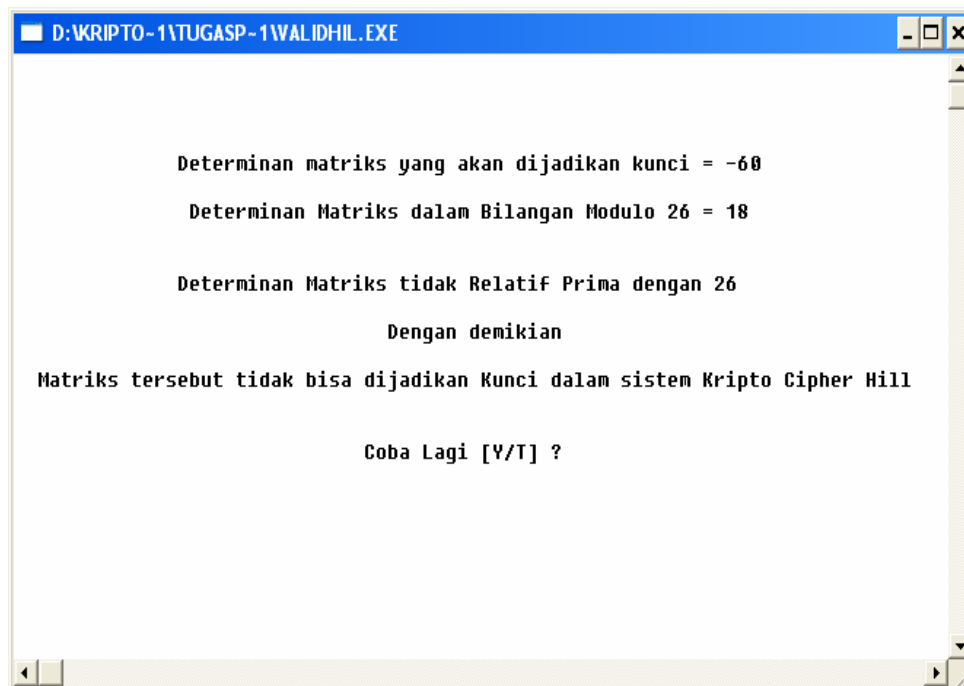


Gambar 4. Menu Input Bilangan



Gambar 5. Tampilan hasil program

4. Jika kita ingin menguji matriks lainnya, saat program tampil seperti pada gambar 5, tekan tombol huruf 'Y' atau 'y' pada keyboard, lalu tekan tombol enter. Misalkan kita ingin menguji apakah matriks $\begin{pmatrix} 4 & 8 \\ 11 & 7 \end{pmatrix}$. Lakukan kembali langkah 3. Hasil program akan tampil seperti gambar 6. Pada gambar tersebut akan terlihat tampilan program jika bilangan yang ingin kita cari inversnya ternyata tidak memiliki invers perkalian.



Gambar 6. Tampilan hasil program

5. Jika anda ingin mengakhiri program, pada saat program tampil seperti pada gambar 5 atau gambar 6, tekan tombol huruf 'T' atau 't' pada keyboard.

----- ηεδρι ωαηψυδι -----