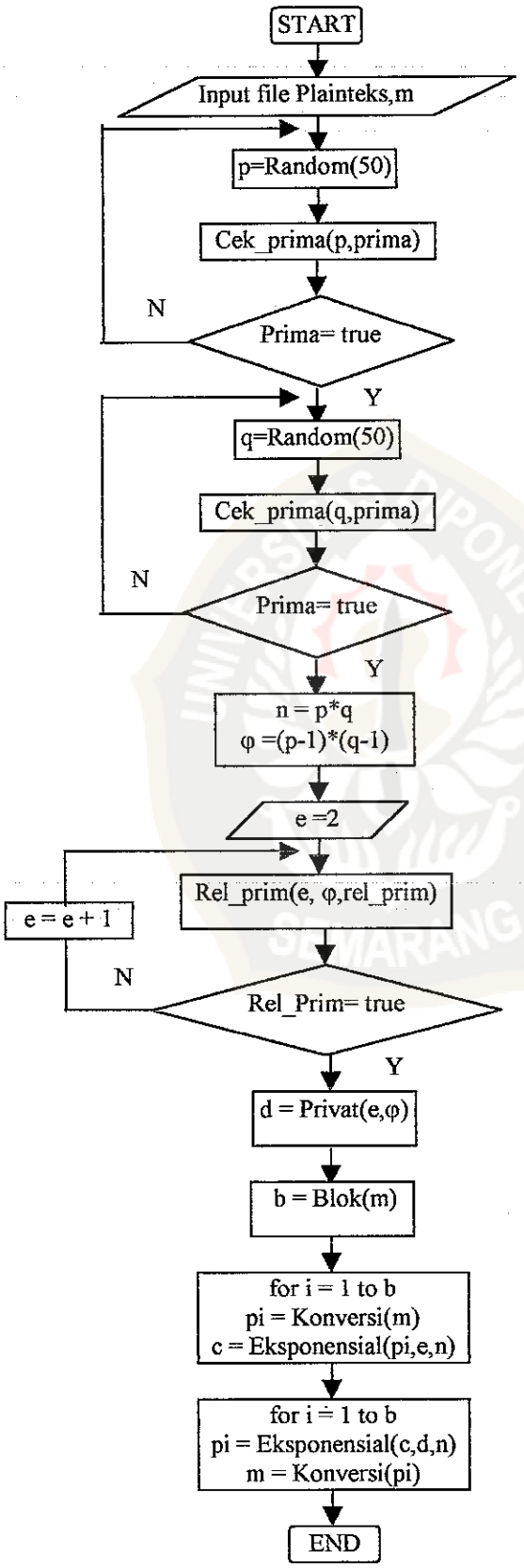
FLOWCHART ALGORITMA RIVEST-SHAMIR-ADLEMAN (RSA)



SUMBER KODE KONVERSI PLAINTEKS

Kode	Char	Kode	Char	Kode	Char	Kode	Char
01	Blank	25	8	49	P	73	h
02	!	26	9	50	Q	74	i
03	"	27	:	51	R	75	j
04	#	28	;	52	S	76	k
05	$	29	<	53	T	77	l
06	%	30	=	54	U	78	m
07	&	31	>	55	V	79	n
08	'	32	?	56	W	80	o
09	(	33	@	57	X	81	p
10	)	34	A	58	Y	82	q
11	*	35	B	59	Z	83	r
12	+	36	C	60	[	84	s
13	,	37	D	61	\	85	t
14	-	38	E	62	]	86	u
15	.	39	F	63	^	87	v
16	/	40	G	64	_	88	w
17	0	41	H	65	`	89	x
18	1	42	I	66	a	90	y
19	2	43	J	67	b	91	z
20	3	44	K	68	c	92	{
21	4	45	L	69	d	93	|
22	5	46	M	70	e	94	}
23	6	47	N	71	f	95	~
24	7	48	O	72	g		

LISTING PROGRAM ALGORITMA RSA

```
Program algoritma_rsa;
{$m 40000,0,655360}
uses  dos,crt;
const nmax   = 100;
      jrmax  = 50;

type  pl     = record
                 kalimat :string;
               end;
      pl1    = record
                 kal :string;
               end;
      jumrec = 1..jrmax;
      psn    = array[jumrec] of pl1;
      fp     = file of pl;
      larik  = string;
      larik1 = array[jumrec] of integer;
      grup   = array[1..64] of string[128];
      grup1  = array[1..15] of string[20];
      bitt   = 0..1;
      bit    = array [0..nmax] of bitt;

var   fpl    : fp;
      recpl  : pl;
      pesan  : psn;
      nf     : larik;
      jr     : integer;
      pil    : grup1;
      ciper,plaint : grup;

{*procedure untuk mengkonversi bilangan desimal ke biner*}
Procedure Biner(xi: longint; var xb:bit; var k:longint);
var i : longint;
begin
k := 0;
for i:= 0 to nmax do
    begin
    if xi = 1 then
       begin
       xb[i]:= 1;
       exit
       end
    else
        begin
        xb[i]:= xi mod 2;
        xi := xi div 2;
        k := k + 1;
        end;
    end;
end;

{*function untuk menghitung fungsi enkripsi dan dekripsi rsa*}
Function Eksponensial(a,b,n: longint):longint;
var c,d,i,k : longint;
    xb      : bit;
begin
biner(b,xb,k);
c := 0;
```

```
d := 1;
for i := k downto 0 do
    begin
    c := 2 * c;
    d := ( d * d ) mod n;
    if xb[i] = 1 then
       begin
       c := c + 1;
       d := ( d * a ) mod n
       end
    end;
    eksponensial := d;
end;

{*function untuk mencari pembagi persekutuan terbesar dari dua bilangan*}
Function Euclid(a,b :longint) :longint;
var r : longint;
begin
while b <> 0 do
begin
r := a mod b;
a := b;
b := r;
end;
euclid := a;
end;

{*procedure untuk memeriksa kerelatif-primaan dua bilangan*}
Procedure Relprim(a,b :longint; var relatif_prima: boolean);
var r : longint;
begin
r := euclid(a,b);
if r = 1 then
    relatif_prima := true
 else
    relatif_prima := false;
end;

{*function untuk menghitung nilai eksponen dekripsi rsa*}
function Privat(a,b: longint):longint;
var i : longint;
begin
for i := 2 to ( b - 1 ) do
    begin
    if (( a * i ) mod b = 1) then
       privat := i;
    end;
end;

{*procedure untuk memeriksa keprimaan sebuah bilangan*}
Procedure Cek_Prima(a:longint;var prima:boolean);
var i : longint;
begin
prima:= true;
if(a >= 4) then
  begin
  for i:= 2 to ( a - 1 ) do
      begin
      if ( a mod i = 0 ) then
         prima :=false
      end;
  end;end;
```

```
{*procedure pembangkitan kunci rsa*}
Procedure Kunci(var p,q,e,d,n: longint);
var i,qmin,euler          : longint;
    prima,relatif_prima   : boolean;
begin
randomize;
prima := false;
while prima=false do
begin
    repeat
       p := random(50);
    until ( p > 1 );
    cek_prima(p,prima);
end;
prima := false;
while prima=false do
   begin
     repeat
       qmin := random(50);
       q    := (9596 div p) + qmin;
     until ( q > 1 );
     cek_prima(q,prima);
   end;
n := p * q;
euler := (p-1)*(q-1);
e := 2;
relatif_prima := false;
while relatif_prima = false do
begin
     relprim(euler,e,relatif_prima);
     if relatif_prima=false then
         e := e + 1;
end;
d := privat(e,euler);
end;

{*procedure mencetak kunci rsa*}
Procedure Cetak_Kunci(var p,q,e,d,n :longint);
var i : integer;
    t : char;
begin
clrscr;window(6,3,75,23);textbackground(0);clrscr;textcolor(1);
gotoxy(17,3);;writeln('kunci algoritma rivest-shamir-adleman ');writeln;
kunci(p,q,e,d,n);
gotoxy(31,6);writeln('p  : ',p);
gotoxy(31,7);writeln('q  : ',q);
gotoxy(31,8);writeln('n  : ',n);
gotoxy(31,9);writeln('e  : ',e);
gotoxy(31,10);writeln('d  : ',d);
gotoxy(17,13);write('kunci publik rsa (e,n): ( ',e:5,',');
gotoxy(50,13);writeln(n,' )');
gotoxy(17,14);write('kunci privat rsa (d,n): ( ',d:5,',');
gotoxy(50,14);writeln(n,' )'); textbackground(6);textcolor(1);
gotoxy(20,20);writeln('tekan<enter> untuk enkripsi ...');
repeat
t:=readkey;
until t=#13;
end;
```

```
{*procedure untuk menghitung blok dari inputan plainteks*}
Procedure Blok(var pesan:psn;var b: larik1);
var i           : jumrec;
    cacah,angka : larik1;
begin
jr := filesize(fpl);
for i:= 1 to jr do
     begin
     with pesan[i] do
         begin
         cacah[i] := length(kal);
         angka[i] := cacah[i] mod 2;
         if ( angka[i] <> 0 ) then
         kal[(cacah[i])+1] := chr(32);
         b[i] := round(cacah[i]/2);
         end;
     end;
end;

{*procedure enkripsi dan dekripsi rsa*}
Procedure RSA(var fpl:fp;var pesan:psn;var ciper,plaint : grup);
var t       : char;
    l       : jumrec;
    b       : larik1;
    p,q,e,d,n            : longint;
    relatif_prima        : boolean;
    p1,p2,mess1,mess2    : char;
    ms,str_c,cc,pes_gab  : grup;
    pesan_gab,pes1,pes2,cpr,des,message,m1,m2          : larik;
    i,j,c,pi,m,pl,kl,num1,num2,mes1,mes2,cod1,cod2,cod3 : integer;
begin
assign(fpl,nf);
reset(fpl);
jr := filesize(fpl);
for l:= 1 to jr do
    begin
    read(fpl,recpl);
    with recpl do
         begin
         pesan[l].kal := kalimat;
         end;
    end;
blok(pesan,b);
repeat
cetak_kunci(p,q,e,d,n);
for l:= 1 to jr do
     begin
     cpr:='';des:='';
     j :=1  ; kl:=1;
     with pesan[l] do
        begin
        for i:= 1 to b[l] do
             begin
             p1 :=kal[j];
             p2 :=kal[j+1];
             pesan_gab:= p1 + p2;
             num1 :=(ord(p1))-31;
             num2 :=(ord(p2))-31;
             str(num1, pes1);
             if length(pes1)=1 then insert('0',pes1,1);
             str(num2, pes2);
             if length(pes2)=1 then insert('0',pes2,1);
```

```
            pes_gab[i] :=pes1+pes2;
            val(pes_gab[i],p,cod1);
            if cod1 <> 0 then
               writeln('ada data tidak sah pada posisi:',cod1);
            c := eksponensial(p,e,n);
            m := eksponensial(c,d,n);
            str(c,cc[i]);
            str(m,message);
            if length(message)=3 then insert('0',message,1);
            m1:=message[kl]+message[kl+1];
            m2 :=message[kl+2]+message[kl+3];
            val(m1,mes1,cod2);
            if cod2 <> 0 then
               writeln('ada data tidak sah pada posisi:',cod1);
            val(m2,mes2,cod3);
            if cod3 <> 0 then
               writeln('ada data tidak sah pada posisi:',cod3);
            mess1:= chr(mes1+31);
            mess2:= chr(mes2+31);
            ms[i]:= mess1 + mess2;
            cpr :=concat(cpr,cc[i]);
            des :=concat(des,ms[i]);
            j:=j +2;
            end;
         end;
      ciper[l] := cpr;
      plaint[l]:= des;
      end;
clrscr;window(6,3,75,23);textbackground(0);clrscr;textcolor(14);
gotoxy(15,2);writeln('enkripsi algoritma rivest-shamir-adleman ');
writeln;writeln;
for l:= 1 to jr do
    begin
    with pesan[l] do
       begin
       write(ciper[l]);
       end;
    end;
textbackground(6);textcolor(14);
gotoxy(20,20);writeln('tekan<enter> untuk dekripsi ...');
repeat
t:=readkey;
until t=#13;
clrscr;window(6,3,75,23);textbackground(0);clrscr;textcolor(3);
gotoxy(15,2);writeln('dekripsi algoritma rivest-shamir-adleman ');
writeln;writeln;
for l:= 1 to jr do
    begin
    with pesan[l] do
       begin
       writeln(plaint[l]);
       end;
    end;
textbackground(6);textcolor(3);
gotoxy(18,20);writeln('tekan<enter> untuk konfirmasi ...');
repeat
t:=readkey;
until t=#13;
clrscr;window(11,10,65,14);textbackground(2);clrscr;textcolor(0);
gotoxy(3,2);writeln('anda ingin mencoba lagi dengan plainteks yang sama
?');
gotoxy(15,4);writeln('ya');
```

```
gotoxy(35,4);writeln('tidak');
j:=1;textcolor(13);gotoxy(15,4);writeln('ya');
repeat
t:=readkey;
textcolor(0);
case j of
1:begin gotoxy(15,4);writeln('ya');end;
2:begin gotoxy(35,4);writeln('tidak');end;
end;
case t of
#75:j:=1;
#77:j:=2;
end;
textcolor(13);
case j of
1:begin gotoxy(15,4);writeln('ya');end;
2:begin gotoxy(35,4);writeln('tidak'); end;
end;
until (t=#13);
case j of
2: t:=#15; end;
until (t=#15);
end;

{*procedure musik pembuka program*}
Procedure Musik;
const
frk:array[1..13] of integer =
(0,0,213,227,256,288,320,341,384,427,453,512,576);
noot:array[0..29] of integer =
     (19,6,0,8,6,0,6,9,6,5,6,0,10,6,0,6,11,10,8,6,10,13,6,5,0,5,3,7,6,0);
jd:array[0..29] of integer =
   (60,4,4,6,2,2,2,4,4,4,4,4,6,2,2,2,4,4,4,4,4,4,2,2,2,2,4,4,12,24);
var
   jmlnot,point,base,i:integer;
   note,jeda:array[0..230] of byte;
   frek:array[1..25] of integer;
begin
move(frk,frek,30);
move(noot,note,26);
move(jd,jeda,30);
jmlnot:=note[0];
base:=jeda[0];
for i:=1 to jmlnot do
if note[i]=0 then delay(jeda[i]*base)
else
 begin
 point:= note[i];
 sound(frek[point]);delay(jeda[i]*base);
 nosound;
 end;
end;

{*procedure musik peringatan*}
Procedure Beep;
begin
sound(400);delay(100);
sound(300);delay(40);
sound(100);delay(120);
sound(300);delay(120);
sound(400);delay(120);
nosound;end;
```

```
{*procedure untuk membuat bingkai pada tampilan menu*}
Procedure Bingkai(x1,y1,x2,y2,wrn:integer);
var i: integer;
begin
textbackground(wrn);gotoxy(x1,y1);write(#201);
for i:= x1+1 to x2-1 do
    begin
    gotoxy(i,y1);write(#205);
    end;
write(#187);
for i:= 1 to y2-y1 do
    begin
    gotoxy(x1,y1+i);write(#186,#186:x2-x1);
    end;
gotoxy(x1,y2);writeln(#200);
for i:= x1+1 to x2-1 do
    begin
    gotoxy(i,y2);write(#205);
    end;
writeln(#188);delay(150);
end;

{*procedure petunjuk pada menu utama*}
Procedure Petunjuk1(var p: larik);
var x,y,n:integer;
begin
textcolor(1);textbackground(6);gotoxy(1,23);
write('gerakkan kursor ' ,+chr(24),' atau ',+chr(25),' dan tekan <enter>
untuk proses');
x:=wherex;
y:=wherey;
n:=81-x;
gotoxy(x,y);write('':n);
end;

{*procedure petunjuk pada menu pilihan plainteks*}
Procedure Petunjuk2(var p: larik);
var x,y,n:integer;
begin
textcolor(1);textbackground(6); gotoxy(1,23);
write('gerakkan kursor',+chr(24),'atau',+chr(25),' atau '+chr(26),' atau
',+chr(27));gotoxy(45,23);write(' dan tekan <enter> untuk proses');
x:=wherex;
y:=wherey;
n:=81-x;
gotoxy(x,y);write('':n);
end;

{*procedure cover program*}
Procedure Cover;
var t:char;
begin
window(1,1,79,24);textbackground(7);clrscr;textcolor(1);
gotoxy(32,4);writeln('* p r o g r a m *');
gotoxy(21,6);write('algoritma rivest-shamir-adleman ( rsa )');
gotoxy(39,9);writeln(#186);
gotoxy(34,11);writeln('dibuat oleh:');
gotoxy(32,12);writeln('nama: nur izzati');
gotoxy(32,13);writeln('nim : j2a 097 039');
gotoxy(39,15);writeln(#186);
gotoxy(31,17);writeln('jurusan matematika');
gotoxy(19,18);writeln('fakultas matematika dan ilmu pengetahuan alam');
```

```
gotoxy(29,19);writeln('universitas diponegoro');
gotoxy(37,20);writeln('semarang');
gotoxy(38,21);writeln('2002');
textbackground(6);gotoxy(25,23);writeln('tekan enter untuk memulai...!');
musik;
repeat
t:=readkey;
until t=#13;
end;

{*procedure informasi menu pada menu utama*}
Procedure Informasi_Menu;
var i : integer;
    t : char;
begin
window(5,5,75,22);textbackground(3);clrscr;textcolor(1);
gotoxy(22,2);writeln('menu utama algoritma rsa');
gotoxy(3,4);write(#3);writeln(' dalam menu algoritma rsa disediakan empat
pilihan');
gotoxy(55,4);writeln('yaitu informasi ');
gotoxy(5,5);writeln('menu,algoritma rsa,start dan exit.');
gotoxy(3,7);write(#3);writeln(' menu algoritma rsa memberikan gambaran
umum tentang algoritma rsa.');
gotoxy(3,9);write(#3);writeln(' menu start digunakan untuk memulai proses
enkripsi dan dekripsi');
gotoxy(5,10);writeln('algoritma rsa,user diminta memilih plainteks yang
kemudian akan ');
gotoxy(5,11);writeln('dikriptokan  atau membuat sendiri plainteks dengan
memilih menu ');
gotoxy(5,12);textcolor(6);writeln('buat plainteks.');textcolor(1);
gotoxy(3,14);write(#3);writeln(' menu exit digunakan untuk mengakhiri
program algoritma rsa.'); textbackground(6);
gotoxy(13,17);writeln(' tekan enter untuk kembali ke menu utama ...');
repeat
t:=readkey;
until t=#13;
end;

{*procedure algoritma rsa pada menu utama*}
Procedure Algor_rsa;
var i : integer;
    t : char;
begin
window(6,4,75,22);textbackground(0);clrscr;textcolor(1);
gotoxy(22,2);writeln('gambaran umum  algoritma rsa');
gotoxy(3,4);write(#6);writeln('algoritma rivest-shamir-adleman(rsa)
pertama kali dikenalkan');
gotoxy(6,5);writeln('oleh r.rivest,shamir dan adi adleman pada tahun
1978.');
gotoxy(3,7);write(#6);writeln('  algoritma rivest-shamir-adleman ( rsa )
merupakan  algoritma');
gotoxy(6,8);writeln('dalam kriptosistem kunci umum.algoritma rsa
menggunakan  dua ');
gotoxy(6,9);writeln('kunci dalam proses enkripsi dan dekripsinya.satu
kunci publik');
gotoxy(6,10);writeln('(e,n) digunakan dalam enkripsi dan satu kunci
privat (d,n) di');
gotoxy(6,11);writeln('gunakan dalam dekripsi.');
gotoxy(3,13);write(#6);writeln('  algoritma rivest-shamir-adleman ( rsa )
didasarkan pada teori');
gotoxy(6,14);writeln('bilangan.keamanan algoritma rsa terletak pada
kesulitan dalam');
```

```
gotoxy(6,15);writeln('menentukan faktor bilangan prima dari suatu
bilangan.'); textbackground(6);
gotoxy(13,18);writeln(' tekan enter untuk kembali ke menu utama ...');
repeat
t:=readkey;
until t=#13;
end;

{*procedure konfirmasi untuk memilih plainteks dari menu pilihan
plainteks*}
Procedure Pilih_plainteks;
var j:integer;
    t:char;
begin
window(25,20,55,24);textbackground(6);clrscr; textcolor(1);
gotoxy(4,2);writeln('anda pilih plainteks ini ?');
gotoxy(8,4);writeln('ya');
gotoxy(20,4);writeln('tidak');
j:=1;textcolor(13);gotoxy(8,4);writeln('ya');
repeat
t:=readkey;
textcolor(1);
case j of
1:begin gotoxy(8,4);writeln('ya');end;
2:begin gotoxy(20,4);writeln('tidak');end;
end;
if t = #0 then
begin
t:= readkey;
case t of
#75:j:=1;
#77:j:=2;
end;end;textcolor(13);
case j of
1:begin gotoxy(8,4);writeln('ya');end;
2:begin gotoxy(20,4);writeln('tidak'); end;
end;
until (t=#13);
if j=1 then
   begin
   window(1,1,80,25);textbackground(6);clrscr;
   rsa(fpl,pesan,ciper,plaint);
   end
else t:=#15;
end;

{*procedure tampilan plainteks dari menu pilihan plainteks*}
Procedure Tampilan_plainteks(var fpl:fp;var nf:larik);
var l : integer;
    i : jumrec;
begin
assign(fpl,nf);
reset(fpl);
jr := filesize(fpl);
gotoxy(19,1);writeln('plainteks pilihan dengan nama ',nf);
for l:= 1 to 69 do write(#205);
for i:= 1 to jr do
    begin
    read(fpl,recpl);
    with recpl do
        begin
        writeln(kalimat);
```

```
        end;
    end;
close(fpl);
pilih_plainteks;
end;

{*procedure untuk menambah isi plainteks dari sub menu buat plainteks di
menu pilihan plainteks*}
Procedure Tambah_isi_pl(var fpl :fp;var nf :larik);
var j,l,i : integer;
    t : char;
begin
assign(fpl,nf);
reset(fpl);
jr := filesize(fpl);
seek(fpl,jr);
i := 0;
repeat;
i := i+1;
begin
    with recpl do
      begin
      readln(kalimat);
      end;
end;
write(fpl,recpl);
window(22,19,58,23);textbackground(6);clrscr;textcolor(1);
gotoxy(4,2);writeln('anda ingin tambah isi plainteks ?');
gotoxy(10,4);writeln('ya');
gotoxy(23,4);writeln('tidak');
j:=1;textcolor(13);gotoxy(10,4);writeln('ya');
repeat
t:=readkey;textcolor(1);
case j of
1:begin gotoxy(10,4);writeln('ya');end;
2:begin gotoxy(23,4);writeln('tidak');end;
end;
if t = #0 then
begin
t:= readkey;
case t of
#75:j:=1;
#77:j:=2;
end;end;textcolor(13);
case j of
1:begin gotoxy(10,4);writeln('ya');end;
2:begin gotoxy(23,4);writeln('tidak'); end;
end;
until (t=#13);
case j of
1: begin
   window(6,3,75,24);textbackground(7);clrscr;textcolor(1);
   gotoxy(21,1);writeln('plainteks dengan nama ',nf);textcolor(6);
   gotoxy(20,2);writeln('tekan <enter> untuk konfirmasi ');
   gotoxy(10,3);writeln('tiap anda selesai memasukkan 1 kalimat plainteks
   dan');
   gotoxy(10,4);writeln('ketika kursor berhenti setelah 126 karakter
   ditulis ');
   gotoxy(9,5);writeln('tekan <esc> untuk meghapus kalimat plainteks
   sebelumnya');textcolor(1);
   for l:= 1 to 70 do write(#205);
   end;
```

```
2: begin
   window(1,1,80,25);textbackground(6);clrscr;
   rsa(fpl,pesan,ciper,plaint);
   t:=#15;
   end;
end;
until (t=#15);
close(fpl);
end;

{*procedure untuk menambah plainteks dari sub menu buat plainteks di menu
pilihan plainteks*}
Procedure Tambah_pl;
var j,l:integer;
    t:char;
begin
window(22,19,58,23);textbackground(6);clrscr;textcolor(1);
gotoxy(4,2);writeln('anda ingin tambah isi plainteks ?');
gotoxy(10,4);writeln('ya');
gotoxy(23,4);writeln('tidak');
j:=1;textcolor(13);gotoxy(10,4);writeln('ya');
repeat
t:=readkey;
textcolor(1);
case j of
1:begin gotoxy(10,4);writeln('ya');end;
2:begin gotoxy(23,4);writeln('tidak');end;
end;
if t = #0 then
begin
t:= readkey;
case t of
#75:j:=1;
#77:j:=2;
end;end;textcolor(13);
case j of
1:begin gotoxy(10,4);writeln('ya');end;
2:begin gotoxy(23,4);writeln('tidak'); end;
end;
until (t=#13);
if j=1 then
   begin
   window(6,3,75,24);textbackground(7);clrscr;textcolor(1);
   gotoxy(21,1);writeln('plainteks dengan nama ',nf);textcolor(6);
   gotoxy(20,2);writeln('tekan <enter> untuk konfirmasi ');
   gotoxy(10,3);writeln('tiap anda selesai memasukkan 1 kalimat plainteks
   dan ');
   gotoxy(10,4);writeln('ketika kursor berhenti setelah 126 karakter
   ditulis ');
   gotoxy(9,5);writeln('tekan <esc> untuk meghapus kalimat plainteks
   sebelumnya');textcolor(1);for l:= 1 to 70 do write(#205);
   tambah_isi_pl(fpl,nf);
   end
else
begin
window(1,1,80,25);textbackground(6);clrscr;
rsa(fpl,pesan,ciper,plaint);
end;end;

{*procedure untuk menampilkan plainteks dari sub menu buat plainteks di
menu pilihan plainteks*}
Procedure Tampilan_pl(var fpl:fp;var nf:larik);
```

```
var l : integer;
    i : jumrec;
begin
window(6,3,75,24);textbackground(7);clrscr;textcolor(1);
assign(fpl,nf);
reset(fpl);
jr := filesize(fpl);gotoxy(19,1);
writeln('tampilan plainteks dengan nama ',nf);writeln;
for l:= 1 to 70 do write(#205);
for i:= 1 to jr do
    begin
    read(fpl,recpl);
    with recpl do
        begin
        writeln(kalimat);
        end;
    end;
close(fpl);
tambah_pl;
end;

{*procedure untuk mengisi nama plainteks dari sub menu buat plainteks di
menu pilihan plainteks*}
Procedure Nama_pl(var nf:larik;var t:char);
var j:integer;
begin
repeat
window(22,10,58,16);textbackground(5);clrscr;textcolor(1);
gotoxy(8,2);writeln('tulis nama plainteks anda');
gotoxy(5,3);writeln('dan tekan<enter> untuk proses');
gotoxy(4,5);write('nama plainteks : ');readln(nf);
clrscr;window(22,10,58,16);textbackground(6);clrscr;textcolor(1);
gotoxy(2,3);writeln('anda ingin mengubah nama plainteks ?');
gotoxy(10,5);writeln('ya');
gotoxy(23,5);writeln('tidak');
j:=1;textcolor(13);gotoxy(10,5);writeln('ya');
repeat
t:=readkey;
textcolor(1);
case j of
1:begin gotoxy(10,5);writeln('ya');end;
2:begin gotoxy(23,5);writeln('tidak');end;
end;
if t = #0 then
begin
t:= readkey;
case t of
#75:j:=1;
#77:j:=2;
end;end;textcolor(13);
case j of
1:begin gotoxy(10,5);writeln('ya');end;
2:begin gotoxy(23,5);writeln('tidak'); end;
end;
until (t=#13);
case j of
2: t:=#14;
end;
until t=#14;
end;
```

```
{*procedure untuk membuat plainteks dari sub menu buat plainteks di menu
pilihan plainteks*}
Procedure Buat_pl(var fpl:fp;var nf: larik);
var j,i,l  : integer;
    t      : char;
begin
window(6,3,75,24);textbackground(7);clrscr;textcolor(1);
assign(fpl,nf);
rewrite(fpl);
gotoxy(21,1);writeln('plainteks dengan nama ',nf);textcolor(6);
gotoxy(20,2);writeln('tekan <enter> untuk konfirmasi ');
gotoxy(10,3);writeln('tiap anda selesai memasukkan 1 kalimat plainteks
dan '); gotoxy(10,4);
writeln('ketika kursor berhenti setelah 126 karakter ditulis ');
gotoxy(9,5);writeln('tekan <esc> untuk meghapus kalimat plainteks
sebelumnya');textcolor(1);
for l:= 1 to 70 do write(#205);
i := 0;
repeat
i:=i+1;
with recpl do
   begin
   readln(kalimat);
   end;
write(fpl,recpl);textcolor(13);textbackground(0);
window(22,19,58,23);textbackground(6);clrscr;textcolor(1);
gotoxy(4,2);writeln('anda ingin tambah kalimat lagi ?');
gotoxy(10,4);writeln('ya');
gotoxy(23,4);writeln('tidak');
j:=1;textcolor(13);gotoxy(10,4);writeln('ya');
repeat
t:=readkey;
textcolor(1);
case j of
1:begin gotoxy(10,4);writeln('ya');end;
2:begin gotoxy(23,4);writeln('tidak');end;
end;
if t = #0 then
begin
t:= readkey;
case t of
#75:j:=1;
#77:j:=2;
end;end;textcolor(13);
case j of
1:begin gotoxy(10,4);writeln('ya');end;
2:begin gotoxy(23,4);writeln('tidak'); end;
end;
until (t=#13);
case j of
1: begin
   window(6,3,75,24);textbackground(7);clrscr;textcolor(1);
   gotoxy(21,1);writeln('plainteks dengan nama ',nf);textcolor(6);
   gotoxy(20,2);writeln('tekan <enter> untuk konfirmasi ');
   gotoxy(10,3);writeln('tiap anda selesai memasukkan 1 kalimat plainteks
   dan ');
   gotoxy(10,4);writeln('ketika kursor berhenti setelah 126 karakter
   ditulis ');
   gotoxy(9,5);writeln('tekan <esc> untuk meghapus kalimat plainteks
   sebelumnya');textcolor(1);for l:= 1 to 70 do write(#205);
   end;
2: t:=#3; end;
```

```
until (t=#3);
close(fpl);
end;

{*procedure untuk membaca plainteks dari sub menu buat plainteks di menu
pilihan plainteks*}
Procedure Baca_pl(var t:char);
var baru,jawab: char;
    file_ada,cek,f_baru  : boolean;
begin
repeat
window(1,1,80,25);textbackground(7);clrscr;
nama_pl(nf,t);
if t=#14 then begin
assign(fpl,nf);
{$i-}
reset(fpl);
{$i+}
file_ada:=(ioresult=0);
if file_ada then
begin
beep;
window(22,10,58,16);textbackground(6);clrscr;textcolor(2+blink);
gotoxy(10,4);writeln('file sudah ada !!!');delay(2500);end;end;
until not file_ada;
buat_pl(fpl,nf);
tampilan_pl(fpl,nf);
end;

{*procedure konfirmasi untuk membuat plainteks dari sub menu buat
plainteks di menu pilihan plainteks*}
Procedure Plainteks;
var j:integer;
    t:char;
begin
clrscr;window(22,10,60,16);textbackground(6);clrscr;textcolor(1);
gotoxy(4,3);writeln('anda ingin buat plainteks sendiri ?');
gotoxy(10,5);writeln('ya');
gotoxy(26,5);writeln('tidak');
j:=1;textcolor(13);gotoxy(10,5);writeln('ya');
repeat
t:=readkey;textcolor(1);
case j of
1:begin gotoxy(10,5);writeln('ya');end;
2:begin gotoxy(26,5);writeln('tidak');end;
end;
if t =#0 then
begin
t:=readkey;
case t of
#75:j:=1;
#77:j:=2;
end;end;textcolor(13);
case j of
1:begin gotoxy(10,5);writeln('ya');end;
2:begin gotoxy(26,5);writeln('tidak'); end;
end;
until (t=#13);
if j=1 then baca_pl(t)
else t:=#6;
end;
```

```
{*procedure nama plainteks di menu pilihan plainteks*}
Procedure Tulisan_pl(var pil:grup1);
begin
pil[5] := '1. doa.dat';
pil[6] := '2. sahabat.dat';
pil[7] := '3. zodiak.dat';
pil[8] := '4. tertawan.dat';
pil[9] := '5. lowongan.dat';
pil[10]:= '6.  tips.dat';
pil[11]:= '7.  anekdot.dat';
pil[12]:= '8.  resep.dat';
pil[13]:= '9.  buat plainteks';
pil[14]:= '10. ke menu utama';
end;

{*procedure untuk menempatkan pilihan nama plainteks di menu pilihan
plainteks*}
Procedure Pilih_tulisan_pl(pilih:integer);
begin
tulisan_pl(pil);
case pilih of
5  : begin gotoxy(4,5) ;write(pil[5]) ;end;
6  : begin gotoxy(4,6) ;write(pil[6]) ;end;
7  : begin gotoxy(4,7) ;write(pil[7]) ;end;
8  : begin gotoxy(4,8) ;write(pil[8]) ;end;
9  : begin gotoxy(4,9) ;write(pil[9]) ;end;
10 : begin gotoxy(24,5);write(pil[10]);end;
11 : begin gotoxy(24,6);write(pil[11]);end;
12 : begin gotoxy(24,7);write(pil[12]);end;
13 : begin gotoxy(24,8);write(pil[13]);end;
14 : begin gotoxy(24,9);write(pil[14]);end;
end;end;
{*procedure untuk menampilkan isi menu pilihan plainteks*}
Procedure tampilan_menu_pl;
var i:integer;
begin textcolor(1);textbackground(6);
gotoxy(11,1);writeln('menu pilihan plainteks');
gotoxy(8,2);writeln('algoritma rivest-shamir-adleman');
for i:= 5 to 9 do
begin gotoxy(4,i);writeln(pil[i]);end;
for i:= 10 to 14 do
begin gotoxy(24,i-5);writeln(pil[i]);end;
textbackground(15);pilih_tulisan_pl(5);
end;

{*procedure tampilan menu pilihan plainteks*}
Procedure Menu_pilihan_pl;
var p : larik;
begin
clrscr;window(1,1,80,25); petunjuk2(p);
textcolor(1);bingkai(18,6,61,17,6);window(19,7,60,18);
tulisan_pl(pil);tampilan_menu_pl;
end;

{*procedure pemilihan menu pada menu pilihan plainteks*}
Procedure Kursor_pilih_pl(var pilih:integer);
var x,baris,i : integer;
    t,jawab: char;
begin
pilih:=5;
repeat
t:=#15;
```

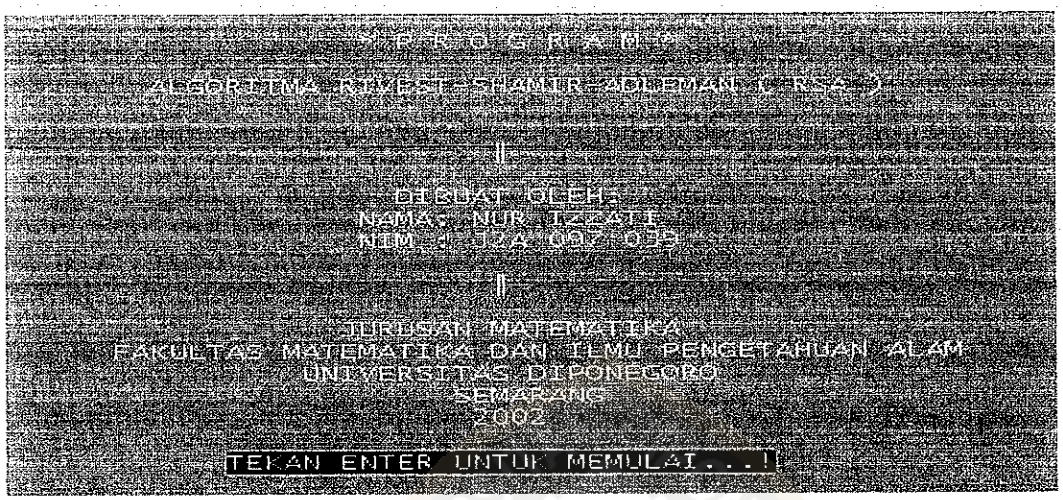
```
repeat
t:= readkey;
if t = #0 then
begin
t:= readkey;
case t of
#77:begin
    if (pilih<=9) then pilih:=pilih+5 else pilih:=pilih;
    textbackground(6);pilih_tulisan_pl(pilih-5);
    textbackground(15);pilih_tulisan_pl(pilih);gotoxy(24,pilih-5);
    end;
#75:begin
    if (pilih>=9) then pilih:=pilih-5 else pilih:=pilih;
    textbackground(6);pilih_tulisan_pl(pilih+5);
    textbackground(15);pilih_tulisan_pl(pilih);gotoxy(4,pilih);
    end;
#80:begin
    if (pilih = 9) or (pilih = 14) then pilih:=pilih else pilih:=pilih+1;
    textbackground(6);pilih_tulisan_pl(pilih-1) ;
    textbackground(15);pilih_tulisan_pl(pilih);
    if (pilih<=9) then gotoxy(4,pilih) else gotoxy(24,pilih-5);
    end;
#72:begin
    if (pilih = 5) or (pilih = 10) then pilih:=pilih else pilih:=pilih-1;
    textbackground(6);pilih_tulisan_pl(pilih+1);
    textbackground(15);pilih_tulisan_pl(pilih);
    if (pilih<=9) then gotoxy(4,pilih) else gotoxy(24,pilih-5);
    end;
end;end;
if (t=#013) then
  begin
  window(1,1,80,25);clrscr;
  case pilih of
  5:begin
    window(6,3,74,23);textbackground(7);clrscr;textcolor(1);
    nf:='doa.dat';tampilan_plainteks(fpl,nf);
    end;
  6:begin
    window(6,3,74,23);textbackground(7);clrscr;textcolor(1);
    nf:='sahabat.dat';tampilan_plainteks(fpl,nf);
    end;
  7:begin
    window(6,3,74,23);textbackground(7);clrscr;textcolor(1);
    nf:='zodiak.dat';tampilan_plainteks(fpl,nf);
    end;
  8:begin
    window(6,3,74,23);textbackground(7);clrscr;textcolor(1);
    nf:='tertawan cinta.dat';tampilan_plainteks(fpl,nf);
    end;
  9:begin
    window(6,3,74,23);textbackground(7);clrscr;textcolor(1);
    nf:='lowongan.dat';tampilan_plainteks(fpl,nf);
    end;
 10:begin
    window(6,3,74,23);textbackground(7);clrscr;textcolor(1);
    nf:='tips.dat';tampilan_plainteks(fpl,nf);
    end;
 11:begin
    window(6,3,74,23);textbackground(7);clrscr;textcolor(1);
    nf:='anekdot.dat';tampilan_plainteks(fpl,nf);
    end;
 12:begin
```

```
    window(6,3,74,23);textbackground(7);clrscr;textcolor(1);
    nf:='resep.dat';tampilan_plainteks(fpl,nf);
    end;
 13:begin
    window(6,3,74,23);textbackground(7);clrscr;textcolor(1);
    plainteks;
    end;
  end;end;
until(t=#013);t:=#5;until (t=#5);
end;

{*procedure pemrosesan pilihan pada menu pilihan plainteks*}
Procedure Menu_plainteks;
var pilih :integer;
    p: larik;
begin
repeat
window(1,1,80,25);textbackground(0);
menu_pilihan_pl;
gotoxy(4,5);kursor_pilih_pl(pilih);
until pilih=14;
end;

{*procedure untuk menulis nama menu di menu utama*}
Procedure Tulisan_menut(var pil:grup1);
begin
pil[7]:= '1. informasi menu';
pil[8]:= '2. algoritma rsa';
pil[9]:= '3. start';
pil[10]:= '4. exit';
end;

{*procedure untuk menempatkan pilihan menu di menu utama*}
Procedure Pilih_tulisan_menut(pilih:integer);
begin
tulisan_menut(pil);
case pilih of
7  : begin gotoxy(4,7); write(pil[7]); end;
8  : begin gotoxy(4,8); write(pil[8]); end;
9  : begin gotoxy(4,9); write(pil[9]); end;
10 : begin gotoxy(4,10);write(pil[10]);end;
end;end;

{*procedure untuk menampilkan isi menu utama*}
Procedure Tampilan_menut;
var i:integer;
begin
textcolor(5);textbackground(1);
gotoxy(15,2);writeln('menu utama');
gotoxy(5,3);writeln('algoritma rivest-shamir-adleman');
gotoxy(16,4);writeln('( r s a )');
for i:= 7 to 10 do
begin gotoxy(4,i);writeln(pil[i]);
end;textbackground(15);pilih_tulisan_menut(7);
end;

{*procedure tampilan menu utama*}
Procedure Menut_pilihan;
var p:string;
begin
clrscr;window(1,1,80,25);textbackground(1);clrscr;petunjuk1(p);
textcolor(white);bingkai(19,6,59,19,1);window(20,7,58,18);
```

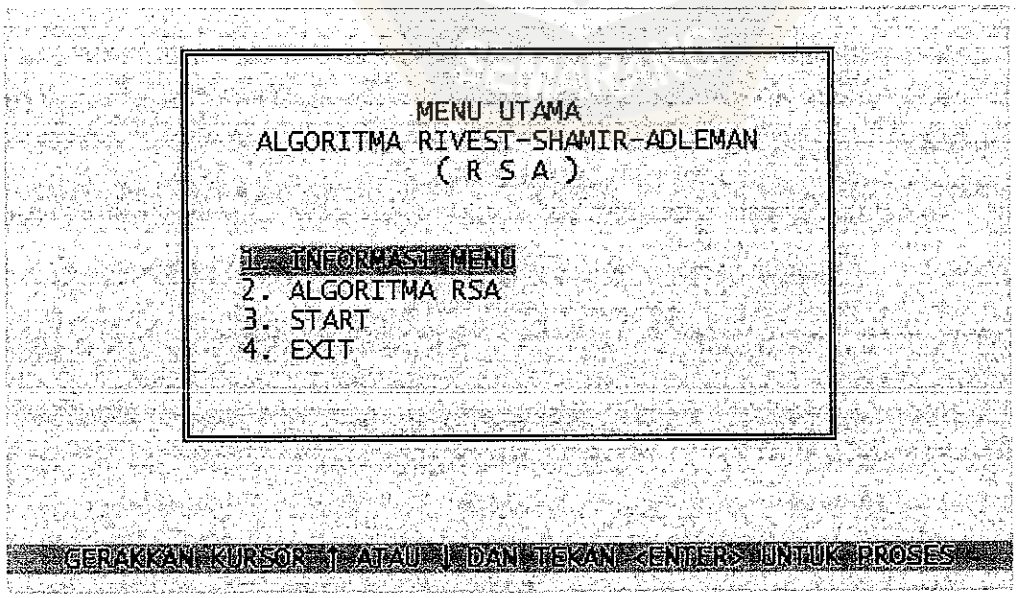
```
tulisan_menut(pil);tampilan_menut;
end;

{*procedure pemilihan menu pada menu utama*}
Procedure Kursor_pilih_menut(var pilih:integer);
var x,baris,i : integer;
    t,jawab: char;
begin
pilih:=7;
repeat
t:=#0;
repeat
t:= readkey;
baris:=wherey;
if t = #0 then
begin
t:= readkey;
if(t=#072)and( baris in[7..10]) then
  begin
  if baris=7 then pilih:=10 else pilih:= baris-1;
  textbackground(1);pilih_tulisan_menut(baris);
  textbackground(15);pilih_tulisan_menut(pilih);gotoxy(4,pilih);
  end;
if(t=(#080)) and (baris in[7..10]) then
  begin
  if baris=10 then pilih:=7 else pilih:=baris+1;
  textbackground(1);pilih_tulisan_menut(baris);textbackground(15);
 pilih_tulisan_menut(pilih);gotoxy(4,pilih);
  end;
end;
if (t=#013) then
  begin
  case pilih of
  7:begin
    window(1,1,80,25);textbackground(7);clrscr;informasi_menu;
    end;
  8:begin
    window(1,1,80,25);textbackground(1);clrscr;algor_rsa;
    end;
  9:begin
    textbackground(0);menu_plainteks;
    end;
  end;end;
until(t=#013);t:=#27;
until (t=#27);
end;

{*procedure pemrosesan pilihan pada menu utama*}
Procedure Menu_utama;
var pilih :integer;
begin
repeat
textbackground(0);window(1,1,80,25);textcolor(5);
menut_pilihan;gotoxy(4,7);kursor_pilih_menut(pilih);
until pilih=10;
end;

{*procedure exit pada menu utama*}
Procedure Bye;
begin
clrscr;window(1,1,80,25);textbackground(0);clrscr;
gotoxy(17,6);textcolor(1);
```

```
writeln('terima kasih anda telah menggunakan program ini');
gotoxy(24,10);textcolor(6+blink);writeln('silahkan tekan sebarang
tombol');
repeat until keypressed;
end;

{*program utama*}
begin
clrscr;
cover;
menu_utama;bye;
end.
```

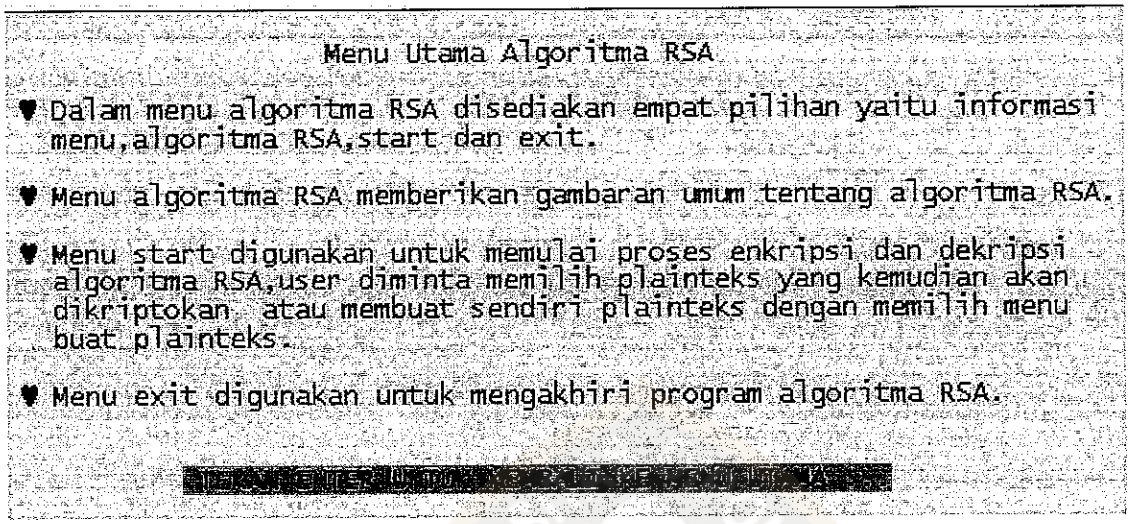
OUT-PUT PROGRAM ALGORITMA RSA



Gambar 1. Tampilan Cover Program

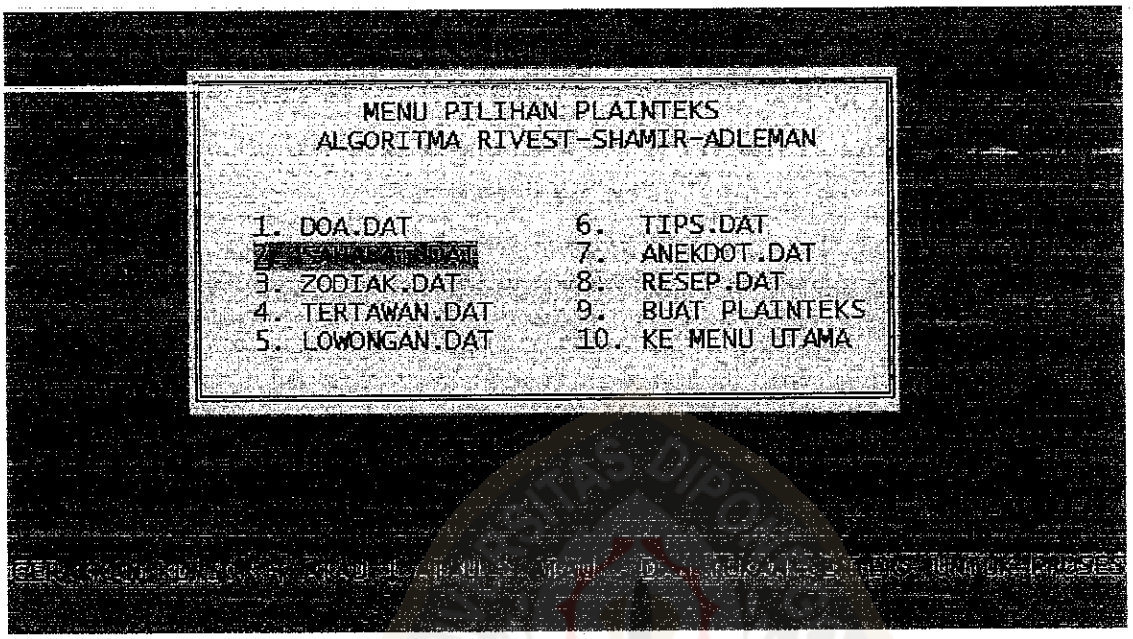


Gambar 2. Tampilan Menu Utama

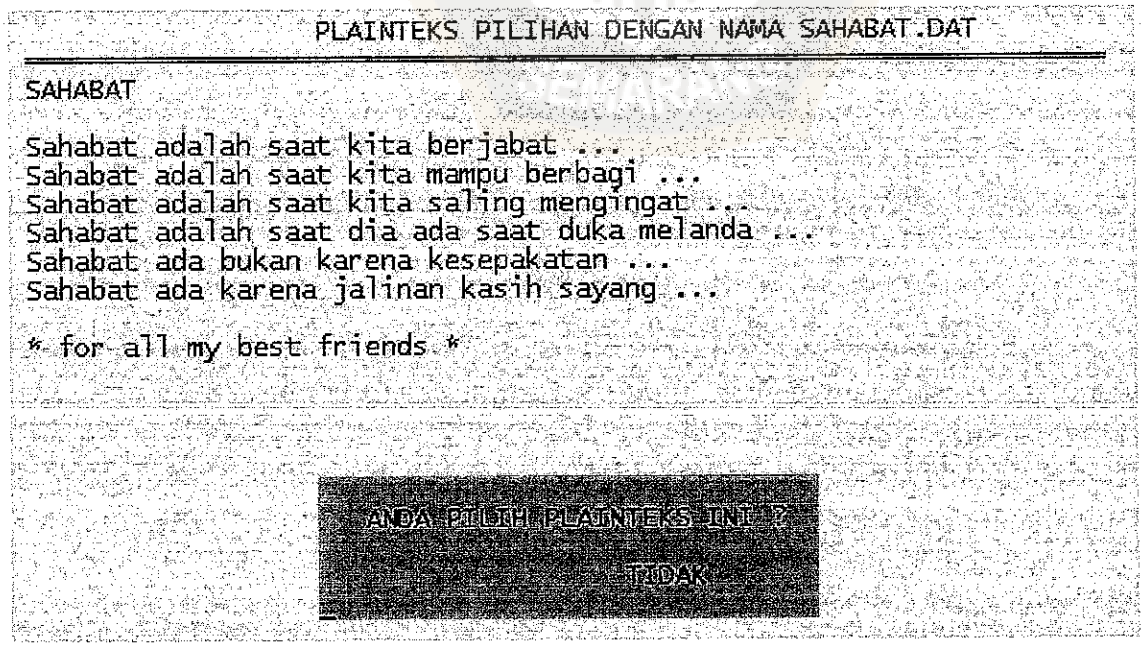


Gambar 3. Tampilan Informasi Menu

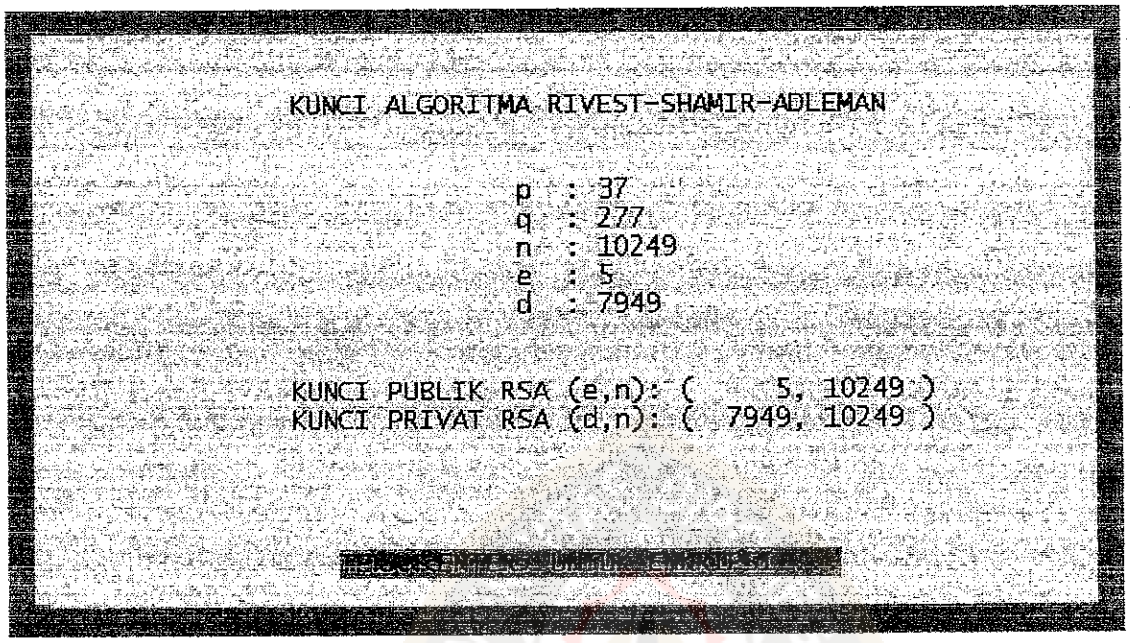
Gambar 4. Tampilan Menu Algoritma RSA



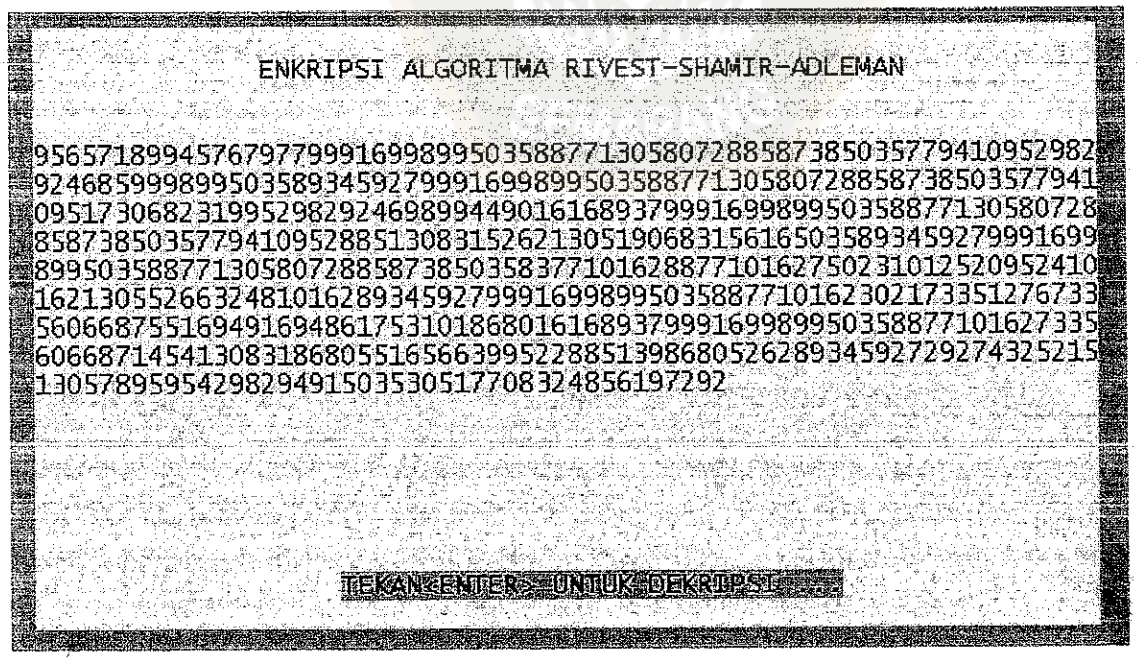
Gambar 5. Tampilan Menu Pilihan Plainteks



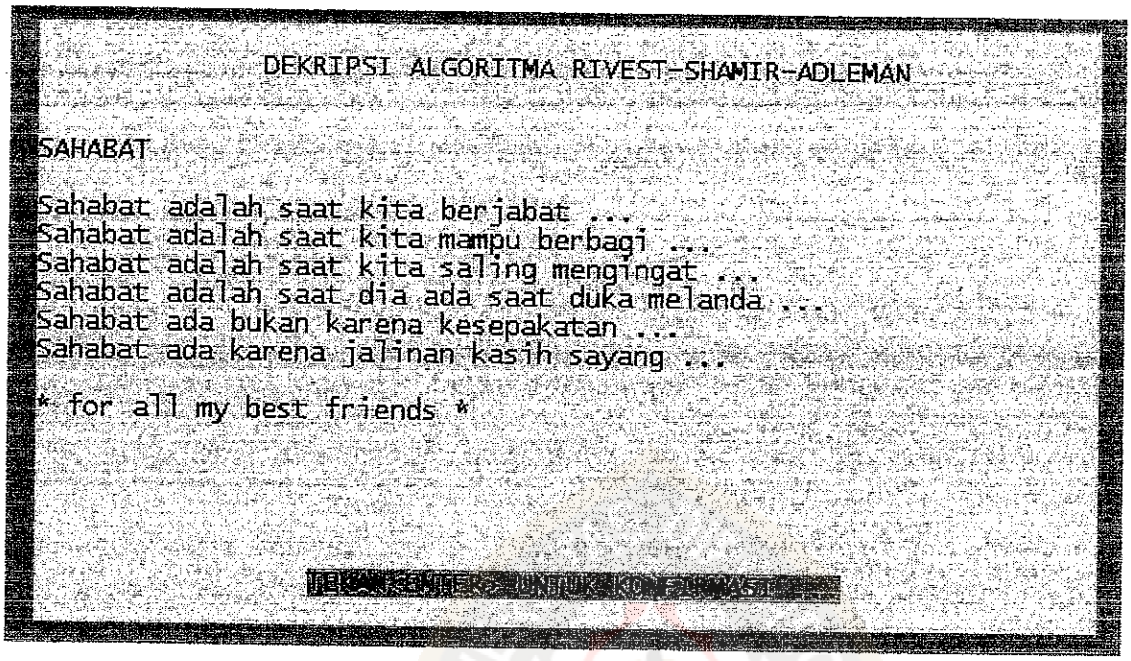
Gambar 6. Tampilan Plainteks



Gambar 7. Pembangkitan Kunci RSA



Gambar 8. Enkripsi RSA



Gambar 9. Dekripsi RSA

Gambar 10. Konfirmasi untuk Pembangitan Kunci kembali

Gambar 11. Menu Exit