

LISTING PROGRAM ENKRIPSI ElGamal ECC

Enkripsi.m

```
p=input("\nBilangan Prima p: ");
A=input("\nKoefisien A untuk  $Y^2 = X^3 + AX + B$ : ");
B=input("\nKoefisien B untuk  $Y^2 = X^3 + AX + B$ : ");
G=input("\nBasic point (G): ");
Ng=input("\nOrder Basic Point (Ng): ");
e=input("\nBanyaknya Percobaan Representasi Titik: ");
PB=input("\nPublic Key (PB): ");
fprintf("\nPenulisan Pesan yang akan dienkripsi harus diawali dan diakhiri
dengan tanda: ' ');
fprintf("\nMisalkan Pesannya: Penting ==> Ketik: \"Penting\" ");
fprintf("\n*****==== Tulis Pesan yang akan di-enkripsi =====*\n");
pesan=input("");
if(isnumeric(pesan)==1)
    pesan=num2str(pesan);
end
lpesan=length(pesan);
nkunci=length(des2bin(p));
bpesan=ceil(nkunci/8)-1;
ipesan=ceil(lpesan/bpesan);
akhir=0;
if (lpesan>bpesan)
    for ips=1:1:lpesan
        if (ips<ipesan)
            awal=akhir+1;
            akhir=bpesan*ips;
            plain{ips}=pesan(awal:akhir);
        else
            plain{ips}=pesan(akhir+1:lpesan);
        end
        p2n(ips)=eccplain2num(plain{ips});
        PM=eccnum2titik(p,A,B,p2n(ips),e);
        n2t{ips}=PM;
    end
    for nti=1:1:length(n2t)
        PC{nti}=eccenk(p,A,G,Ng,PB,n2t{nti});
    end
elseif (lpesan<=bpesan)
    p2n=eccplain2num(pesan);
    n2t=eccnum2titik(p,A,B,p2n,e);
    PC=eccenk(p,A,G,Ng,PB,n2t);
end
fprintf("\nBanyaknya Percobaan Setiap Representasi Titik : %.0f ',e);
```

LANJUTAN LISTING PROGRAM ENKRIPSI ElGamal ECC

```
fprintf('\n##### CHIPERTEXT #####');
fprintf('\n[');
if (lpesan>bpesan)
    for prn=1:1:length(PC)
        fprintf('%0f ',PC{prn}(1,:));
        fprintf('\b;');
    end
elseif(lpesan<=bpesan)
    fprintf('%0f ',PC);
end
fprintf('\b]');
fprintf('\n\n##### PROGRAM ENKRIPSI ElGamal ECC #####');
fprintf('\n\n***** INPUT PROGRAM *****');
fprintf('\n  1. Bilangan Prima p : %0f,p);
fprintf('\n  2. Koefisien Persamaan Kurva Eliptik  $Y^2 = X^3 + AX + B$ );
fprintf('\n      A = %0f,A);
fprintf('\n      B = %0f,B);
fprintf('\n  3. Basic Point G :(%0f , %0f)',G(1),G(2));
fprintf('\n  4. Order Basic Point Ng : %0f,Ng);
fprintf('\n  5. Banyaknya Percobaan Representasi Titik (e): %0f,e);
fprintf('\n  6. Public Key (PB) : (%0f , %0f)',PB(1),PB(2));
fprintf('\n  7. ----- Plaintext-----');
fprintf('\n    %s',pesan);
fprintf('\n\n***** OUTPUT PROGRAM (Chipertext) *****\n');
if (lpesan>bpesan)
    for prn=1:1:length(PC)
        fprintf('%12.0f ',PC{prn}(1,:));
        fprintf('\n');
    end
elseif (lpesan<=bpesan)
    fprintf('%12.0f ',PC);
end
fprintf('\n#####');
```