

LISTING FUNCTION ElGamal ECC

Nama File	Kode Program
bin2des.m	<pre>function des=bin2des(bin) lbin=length(bin); des=0; bi=0; for i=1:1:lbin bi=bi+1; dbin=str2num(bin(i)); des=des + (dbin*(2^(lbin-bi))); end</pre>
des2bin.m	<pre>function bin=des2bin(des) lbin=0; while (des>0) lbin=lbin+1; d=des; des=floor(des/2); r=d-(2*des); bins(lbin)=num2str(r); end bi=0; for i=lbin:-1:1 bi=bi+1; bin(bi)=bins(i); end</pre>
des2bindig.m	<pre>function bin=des2bindig(des,dig) bin1=des2bin(des); if (length(bin1)<dig) bin(1:dig-length(bin1))='0'; bi=0; for i=dig-length(bin1)+1:1:dig bi=bi+1; bin(i)=bin1(bi); end else bin=bin1; end</pre>
ecckunci.m	<pre>function [minkey,maxkey]=ecckunci(nkunci) ukunci=1; while (ukunci==1) if ((nkunci>8) & (nkunci<52))</pre>

	<pre> ukunci=0; else fprintf('\nPanjang kunci dalam interval (8,52)'); nkunci=input('\nMasukkan panjang kunci: ');</pre>
--	---

LANJUTAN LISTING FUNCTION ElGamal ECC

Nama File	Kode Program
ecckunci.m	<pre> ukunci=1; end end bina(1)='1'; binb(1)='1'; for ikunci=2:1:nkunci binb(ikunci)='0'; bina(ikunci)='1'; end minkey=bin2des(binb); maxkey=bin2des(bina);</pre>
eccprima.m	<pre>function prim=eccprima(bb,ba) fprintf('\nCara Menentukan Bilangan Prima'); fprintf('\n1. Bilangan prima ditentukan sendiri'); fprintf('\n2. Bilangan Prima ditentukan oleh komputer'); pilih=0; while ((pilih~=1) & (pilih~=2)) pilih=input('\nPilih 1 atau 2 : '); end ulang=1; while (ulang==1) if (pilih==1) fprintf('\nBilangan Prima [%0f,%0f]: ',bb,ba); r=input(""); while ((r<bb) (r>ba) (isnumeric(r)==0)) fprintf('\nBilangan Prima [%0f,%0f]: ',bb,ba); r=input(""); end elseif (pilih==2) r=randint(1,1,[bb ba]); end if (mod(r,2)~=0) if (ba<=(2^32)) tesp=isprime(r);</pre>

	<pre> A=rAB(1); B=rAB(2); end syrt11=eccfpangkat(A,3,p); syrt1=eccfkali(4,syrt11,p); syrt21=eccfpangkat(B,2,p); syrt2=eccfkali(27,syrt21,p); syarat=eccfadd(syrt1,syrt2,p); if (abs(A)<=p-1) & (abs(B)<=p-1) & (syarat~=0)) ulang=0; end end end </pre>
--	---

LANJUTAN LISTING *FUNCTION* ElGamal ECC

Nama File	Kode Program
eccordgrup.m	<pre> function Ne=eccordgrup(p,A,B) Ne=1; for x=0:1:p-1 sqry=eccfy2(p,A,B,x); takar=eccfpangkat(sqry,(p-1)/2,p); if(takar==1) if (sqry==0) Ne=Ne+1; else Ne=Ne+2; end end end end </pre>
eccpoint.m	<pre> function PG=eccpoint(p,A,B) ulang=1; while (ulang==1) Gx=randint(1,1,[0,p-1]); sqry=eccfy2(p,A,B,Gx); takar=eccfpangkat(sqry,(p-1)/2,p); if (takar==1) Gy=eccfakar(sqry,p); ulang=0; break; end end PG=[Gx Gy(1)]; </pre>
eccordpoint.m	<pre> function Ng=eccordpoint(p,A,G) </pre>

	<pre> R=G; Ng=1; ulang=1; while ((R~='O') & (R~='o')) R=eccadd(p,A,R,G); Ng=Ng+1; end </pre>
eccbasic.m	<pre> function [Ng,G]=eccbasic(p,A,B,Ne) ulang=1;i=0; while(ulang==1) i=i+1; PG=eccpoint(p,A,B); Ng=eccordpoint(p,A,PG); if (Ng>=Ne) G=PG; ulang=0; </pre>

LANJUTAN LISTING *FUNCTION* ElGamal ECC

Nama File	Kode Program
eccbasic.m	<pre> break; end if (i>Ne) ulang=0; G=PG; fprintf('\nTitik (%.0f,%.0f) Bukan Basic Point. '); break; end end </pre>
eccparameter.m	<pre> function T=eccparameter(nkunci) ulang=1; while (ulang==1) [bb ba]=ecckunci(nkunci); ulangp=1; pi=1; while(ulangp==1) p=eccprima(bb,ba) ulangAB=1;ABi=1; while(ulangAB==1) [A B]=ecckurv(p) Ne=eccordgrup(p,A,B) ulangNG=1; </pre>

	<pre> NGi=1; while(ulangNG==1) [Ng G]=eccbasic(p,A,B,Ne) if((Ng>bb) (NGi>Ne)) ulangNG=0; break; else NGi=NGi+1 end end if((Ng>bb) (ABi>(p-1)*(p-1))) ulangAB=0; break; else ABi=ABi+1 end end if((Ng>bb) (pi>(ba-bb))) ulangp=0; break; </pre>
--	--

LANJUTAN LISTING *FUNCTION* ElGamal ECC

Nama File	Kode Program
eccparameter.m	<pre> else pi=pi+1 end end if(Ng>bb) ulang=0; break; else nkunci=input('\nMasukkan Panjang Kunci= '); end end h=Ne/Ng; T{1}=p;T{2}=A;T{3}=B;T{4}=G;T{5}=Ng;T{6}=h; </pre>
eccprivkey.m	<pre> function V=eccprivkey(nkunci,Ng) [minkey maxkey]=ecckunci(nkunci); fprintf('\n CARA MENENTUKAN PRIVATE KEY '); fprintf('\n 1. Menentukan Sendiri'); fprintf('\n 2. Komputer Menentukan Secara Random'); </pre>

	<pre> fprintf('\n PILIH 1 atau 2 : '); pilih=input(""); ulangV=1; while (ulangV==1) if (pilih==1) fprintf('Private Key [%d,%d] = ',minkey,Ng-1); V=input(""); if ((V>=minkey) & (V<=Ng-1)) ulangV=0; end end if (pilih==2) V=randint(1,1,[minkey Ng-1]); ulangV=0; end end end </pre>
eccpubkey.m	<pre> function PB=eccpubkey(p,A,V,G) PB=eccaddsub(p,A,V,G); %fprintf('\nPublic Key PB=(%d,%d)\n',PB(1),PB(2)); </pre>
eccplain2num.m	<pre> function num=eccplain2num(s) for si=1:1:length(s) s2int=uint8(s(si)); s2i=double(s2int); sbin{si}=des2bindig(s2i,8); </pre>

LANJUTAN LISTING *FUNCTION* ElGamal ECC

Nama File	Kode Program
eccplain2num.m	<pre> end c2=0; for c=1:1:length(sbin) for c1=1:1:8 c2=c2+1; cbin(c2)=sbin{c}(c1); end end num=bin2des(cbin); </pre>
eccnum2titik.m	<pre> function PM=eccnum2titik(p,A,B,m,e) while ((m*e>=p) (m<0) (e<1)) fprintf('\nSyaratnya e>0 , m> 0 serta m*e< %d ',p); e=input('\nBanyaknya Percobaan Representasi Titik (e): '); end x=eccfkali(m,e,p); </pre>

	<pre> ulangxy=1; while (ulangxy==1) j=randint(1,1,[0 e-1]); xj=eccfadd(x,j,p); sj=eccfy2(p,A,B,xj); akar=eccfakar(sj,p); if ((akar~=[]) & (xj~=0)) ulangxy=0; break end end PM=[xj akar(1)]; </pre>
eccenk.m	<pre> function PC=eccenk(p,A,G,Ng,PB,PM) %fprintf('\nPenentuan bilangan bulat K'); %fprintf('\n1. Nilai K ditentukan sendiri'); %fprintf('\n2. Nilai K ditentukan oleh komputer'); %pilih=0; %while ((pilih~=1) & (pilih~=2)) % pilih=input('\nPilih 1 atau 2 : '); %end pilih=2; ulang=1; while (ulang==1) if (pilih==1) fprintf('\nPilih bilangan bulat secara random dalam interval [1,%.0f] = ',Ng-1); K=input(""); if ((K>=1) & (K<=Ng-1)) </pre>

LANJUTAN LISTING *FUNCTION* ElGamal ECC

Nama File	Kode Program
eccenk.m	<pre> ulang=0; end end if (pilih==2) K=randint(1,1,[1,Ng-1]); ulang=0; end end P1=eccaddsub(p,A,K,G); P21=eccaddsub(p,A,K,PB); P2=eccadd(p,A,PM,P21); </pre>

	PC=[P1(1) P1(2) P2(1) P2(2)];
eccdek.m	function PM=eccdek(p,A,V,PC) C{1}=PC(1:2); C{2}=PC(3:4); M1=eccaddsub(p,A,V,C{1}); PM=eccsub(p,A,C{2},M1);
ecctitik2num.m	function m=ecctitik2num(PM,e) m=floor(PM(1)/e);
eccnum2plain.m	function psn=eccnum2plain(m) mbin=des2bin(m); mblen=length(mbin); if (mod(mblen,8)==0) mlen=mblen/8; elseif (mod(mblen,8)~=0) mlen=(floor(mblen/8))+1; end i=0; for ml=mlen:-1:1 maxps=mblen-(8*i); if (ml>1) minps=maxps-7; else minps=1; end psbin{ml}=mbin(minps:maxps); psn{1}(ml)=char(bin2des(psbin{ml})); i=i+1; end