LISTING PROGRAM DEKRIPSI ElGamal ECC

Dekripsi.m

```
p=input('\nBilangan Prima p: ');
A=input('\nKoefisien A untuk Y^2 = X^3 + AX + B : ');
V=input('\nPrivate Key V: ');
e=input('\nBanyaknya Percobaan Representasi Tiap Titik (e): ');
fprintf('\nChipertext (PC): \n');
PC=input('');
PCs=size(PC);
lps=1;
for dek=1:1:PCs(1)
   PM=eccdek(p,A,V,PC(dek,:));
   c2t{dek}=PM;
   t2n(dek)=ecctitik2num(PM,e);
   n2p{dek}=eccnum2plain(t2n(dek));
   pesan(lps:lps+length(char(n2p{dek}))-1)=char(n2p{dek});
   lps=length(pesan)+1;
end
fprintf('\n\n########## PROGRAM DEKRIPSI 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   3. Private key (V)  : %.0f',V);
fprintf('\n   4. Banyaknya Percobaan Representasi Titik (e): %.0f',e);
fprintf('\n   5. ---------- Chipertext----------\n');
for prn=1:1:PCs(1)
   fprintf('%12.0f ',PC(prn,:));
   fprintf(';\n');
end
fprintf('\n\n********** OUTPUT PROGRAM (Plaintext)
**********\n');
fprintf('\n %s',pesan);
fprintf('\n#####################################################');
```