Exercice 1:

```
dec:=proc(n,k,l)
local i,j,L,a,d;
L:=[];
for j from 1 to l do
a:=rand(2..n-2)();
for i from 2 to k do
a:=a^i mod n;
d:=gcd(a-1,n);
if d>1 and d<n then
L:=[op(L),d,n/d];
eval(L);
end if;
end do;
end do;
return (L);
end proc:
```

Exercice 2

1)

```
elgamalencrypt:= proc (m)
local k,gamma,delta;
k:=rand(2..p-2)();
gamma:=g&^k mod p;
delta:=m*(power(ga,k) mod p) mod p;
return gamma,delta,m;
end proc :
```

2)

```
L:=[98,111,110,106,111,117,114,32,109,111,110,115,105,101,117,114,32] ;
fichier:= proc(L)
local  i ,M ;
M:=[];
for i from 1 to nops(L) do
M:=[op(M),elgamalencrypt(L[i])];
end do;
return M;
end proc:
```