```
> restart;
> p:=nextprime(3252);
                              p := 3253                               (1)
> g:=rand(1..p)(): g;
                                 1574                                 (2)
> flag:=1: for i from 1 to p-2 do if(g&^i mod(p)=1) then flag:=0:
  fi: od: flag; #Flag is equal to 1 if g is a primitive element
                                  1                                   (3)
> #if g is a primitive element, then:
> #for i from 1 to 36 do g^i mod p: od:
> a:=rand(1..p)():a;
                                 2650                                 (4)
> b:=rand(1..p)():b;
                                 2525                                 (5)
> Public_a:=g^a mod (p);
                          Public_a := 2267                            (6)
> Public_b:=g^b mod (p);
                          Public_b := 1492                            (7)
> m:=rand(1..p)();
                              m := 3122                               (8)
> encoded_m:= m*(Public_b)^a mod (p);
                         encoded_m := 2997                            (9)
> encoded_m*(Public_a^b)&^(-1) mod (p);
                                 3122                                (10)
```