```
print "RSA-Schluesselerzeugung";
print "";

print "Gib Deinen Namen ein:";
read Name;
print "";

//Die Erzeugung zweier zufaelliger großer (geheimer) Primzahlen
p := NextPrime(Random(2^512));
print "Primzahl p:", p;
print"";

q := NextPrime(Random(2^512));
print "Primzahl q:", p;
print"";

//n=p*q wird oeffentlich bekannt gegeben
n   :=  p*q;
print "Oeffentlicher Modul n:", n;
print"";


//Erzeugung eines (zufaelligen) Paares von geheimem Exponenten d
//und oeffentlichem Exponenten e

phi :=  (p-1)*(q-1);
R := IntegerRing(phi);

d := 0;
while GCD(d,phi) ne 1 do
    d := Random(phi);
end while;
print "Geheimer Exponent d:", d;
print"";

e := IntegerRing()!((R!d)^(-1));
print "Oeffentlicher Exponent e:", e;
print "";


//Der oeffentliche Schluessel (n,e) wird in eine allgemein lesbare
//Datei geschrieben

Write("public_key_" cat Name cat ".mg",
      "n_send := " cat IntegerToString(n) cat ";": Overwrite);
Write("public_key_" cat Name cat ".mg",
      "e_send := " cat IntegerToString(e) cat ";");
```