```
IS-PRIME(n):
  prime:=true;
  for i:=2 to sqrt(n) do
    if n is divisible by i then
      prime:=false;
  return prime;
```

```
FERMAT-IS-PRIME(n):
  x := 2^(n-1) mod n;
  if (x<>1) return false;
  else return true;
```

```
RANDOM-FERMAT-IS-PRIME(n):
  a := random number between 2 and n-1;
  x := a^(n-1) mod n;
  if (x<>1) return false;
  else return true;
```

```
STRONG-WITNESS(a,n):
  decompose n-1 into 2^t.u (u is odd)
  x[0] := a^u mod n;
  for i:=1 to t
    x[i] := x[i-1]^2 mod n;
    if x[i] = 1 and x[i-1]<>1 and x[i-1]<>n-1
    then return true;
  if x[t]<>1 return true;
  return false;

MILLER-RABIN-IS-PRIME(n,s):
  repeat s times
    a := random numbet between 1 and n-1;
    if STRONG-WITNESS(a,n) return false;
  return true;
```

```
RANDOM-PRIME(b,s):
  repeat:
    x:=generate random b-bit number
    if MILLER-RABIN-IS-PRIME(x,s) return x
```