```
MILLER-RABIN($n, s$)    // $n > 2$ is odd
for $j = 1$ to $s$
    $a = $ RANDOM($2, n - 2$)
    if WITNESS($a, n$)
        return COMPOSITE    // definitely
return PRIME    // almost surely
```

```
WITNESS($a, n$)
let $t$ and $u$ be such that $t \geq 1$, $u$ is odd, and $n - 1 = 2^t u$
$x_0 = $ MODULAR-EXPONENTIATION($a, u, n$)
for $i = 1$ to $t$
    $x_i = x_{i-1}^2 \bmod n$
    if $x_i == 1$ and $x_{i-1} \neq 1$ and $x_{i-1} \neq n - 1$
        return TRUE    // found a nontrivial square root of 1
if $x_t \neq 1$
    return TRUE    // composite, as in PSEUDOPRIME
return FALSE
```