```
**Algorithm** gen($1^k$):
    sample large primes $p, q$
    $n := p \cdot q$
    sample $a, b \in \mathbb{Z}_n$
    sample $e > 2^n : \gcd(e, \phi(n)) = 1$
    $d := e^{-1} \pmod{\phi(n)}$
    $sk := d \| a \| b$
    $pk := e \| a \| b$
    **return** $(sk, pk)$
```

```
**Algorithm** sgn($sk, m$):
    unpack $sk =: d \| a \| b$
    **return** $\left(\frac{a}{b^m}\right)^d$
```

```
**Algorithm** vrf($pk, m, \sigma$):
    unpack $pk =: a \| b$
    **return** $b^m \sigma^e \overset{?}{=} a$
```