MODULE *dsa*

EXTENDS *Integers*, *Sequences*, *FiniteSets*

VARIABLES p, q, g, k, r, x, y, s, w, $u1$, $u2$, v, *hashM*, *signature*, *verified*

$Prime \triangleq \{a \in 1 \,..\, 20 : \forall\, b \in 2 \,..\, (a-1) : a\%b \neq 0\}$

$ModExpHelper(base,\ half\_exp,\ mod,\ half\_result) \triangleq$
  $(half\_result * half\_result)\%mod$

RECURSIVE $ModExp(\_,\ \_,\ \_)$
$ModExp(base,\ exp,\ mod) \triangleq$
  IF $exp = 0$ THEN 1
   ELSE
    IF $exp\%2 = 0$ THEN
      $ModExpHelper(base,\ exp \div 2,\ mod,\ ModExp(base,\ exp \div 2,\ mod))$
     ELSE
      $(base * ModExp(base,\ exp - 1,\ mod))\%mod$

RECURSIVE $GCDWithCoef(\_,\ \_,\ \_,\ \_,\ \_,\ \_)$
$GCDWithCoef(a,\ b,\ x0,\ x1,\ y0,\ y1) \triangleq$
  IF $b = 0$ THEN $\langle a,\ x0,\ y0\rangle$
   ELSE
    $GCDWithCoef(b,\ a\%b,\ x1,\ x0 - (a \div b) * x1,\ y1,\ y0 - (a \div b) * y1)$

$InverseMod(a,\ m) \triangleq$
  IF $GCDWithCoef(a,\ m,\ 1,\ 0,\ 0,\ 1)[2] < 0$ THEN
    $GCDWithCoef(a,\ m,\ 1,\ 0,\ 0,\ 1)[2] + m$
   ELSE
    $GCDWithCoef(a,\ m,\ 1,\ 0,\ 0,\ 1)[2]$

$GenerateKeys \triangleq$
  $\land\ y' = ModExp(g,\ x,\ p)$
  $\land$ UNCHANGED $\langle p,\ q,\ g,\ x,\ k,\ r,\ s,\ w,\ u1,\ u2,\ v,\ hashM,\ signature,\ verified\rangle$

$Sign \triangleq$
  $\land\ k' = k$
  $\land\ r' = (ModExp(g,\ k',\ p)\%q)$
  $\land\ hashM' = hashM$
  $\land\ s' = (InverseMod(k',\ q) * (hashM' + x * r'))\%q$
  $\land\ signature' = \langle r',\ s'\rangle$
  $\land$ UNCHANGED $\langle p,\ q,\ g,\ x,\ y,\ k,\ w,\ u1,\ u2,\ v,\ verified\rangle$

$Verify \triangleq$
  $\land\ w' = InverseMod(s,\ q)$
  $\land\ u1' = (hashM * w')\%q$
  $\land\ u2' = (r * w')\%q$
  $\land\ v' = ((ModExp(g,\ u1',\ p) * ModExp(y,\ u2',\ p))\%p)\%q$

$\land\ verified' = (v' = r)$
$\land$ UNCHANGED $\langle p,\ q,\ g,\ x,\ y,\ k,\ r,\ s,\ hashM,\ signature\rangle$

$Init\ \triangleq$
$\land\ p \in Prime$
$\land\ q \in Prime$
$\land\ p \neq q$
$\land\ g \in 1\ldots(q-1)$
$\land\ x \in 1\ldots(q-1)$
$\land\ k \in 1\ldots(q-1)$
$\land\ hashM \in 1\ldots(q-1)$
$\land\ y = ModExp(g,\ x,\ p)$
$\land\ r = (ModExp(g,\ k,\ p)\%q)$
$\land\ s = (InverseMod(k,\ q) * (hashM + x * r))\%q$
$\land\ signature = \langle r,\ s\rangle$
$\land\ w = InverseMod(s,\ q)$
$\land\ u1 = (hashM * w)\%q$
$\land\ u2 = (r * w)\%q$
$\land\ v = ((ModExp(g,\ u1,\ p) * ModExp(y,\ u2,\ p))\%p)\%q$
$\land\ verified = (v = r)$

$Next\ \triangleq$
$\lor\ GenerateKeys$
$\lor\ Sign$
$\lor\ Verify$

$Spec\ \triangleq\ Init \land \Box[Next]_{\langle p,\ q,\ g,\ x,\ y,\ k,\ r,\ s,\ w,\ u1,\ u2,\ v,\ hashM,\ signature,\ verified\rangle}$