MODULE *dsa*

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

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

Definicija prostih brojeva u ograničenom opsegu

$Prime \triangleq \{a \in 2 \,..\, 18 : \forall\, b \in 2 \,..\, (a-1) : a\%b \neq 0\}$

Definicija pomoćne funkcije za modularnu eksponencijaciju

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

Definicija rekurzivne funkcije za modularnu eksponencijaciju

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

Definicija proširenog *Euklidovog* algoritma za izračunavanje *GCD* i koeficijenata

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

Inverz modulo

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

Generisanje ključeva

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

Potpisivanje

$Sign \triangleq$
$\quad \land\ k' = k$
$\quad \land\ r' = (ModExp(g,\ k',\ p)\%q)$
$\quad \land\ hashM' = hashM$
$\quad \land\ s' = (InverseMod(k',\ q) * (hashM' + x * r'))\%q$

$\land\ signature' = \langle r',\ s' \rangle$
$\land$ UNCHANGED $\langle p,\ q,\ g,\ x,\ y,\ k,\ w,\ u1,\ u2,\ v,\ verified \rangle$

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

Inicijalno stanje
$Init \triangleq$
$\land\ p \in Prime$
$\land\ q \in Prime$
$\land\ p \neq q$
$\land\ g \in 2\ ..\ (p-1)$
$\land\ x \in 1\ ..\ (q-1)$
$\land\ k \in 1\ ..\ (q-1)$
$\land\ hashM \in 1\ ..\ (q-1)$
$\land\ y = ModExp(g,\ x,\ p)$
$\land\ r = (ModExp(g,\ k,\ p)\%q)$
$\land\ s = (InverseMod(k,\ q) * (hashM + x * r))\%q$
$\land\ signature = \langle r,\ s \rangle$
$\land\ w = InverseMod(s,\ q)$
$\land\ u1 = (hashM * w)\%q$
$\land\ u2 = (r * w)\%q$
$\land\ v = ((ModExp(g,\ u1,\ p) * ModExp(y,\ u2,\ p))\%p)\%q$
$\land\ verified = (v = r)$

Sledeće stanje sistema
$Next \triangleq$
$\lor\ GenerateKeys$
$\lor\ Sign$
$\lor\ Verify$

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