
MODULE *dsa*

EXTENDS *Integers, Sequences, FiniteSets*

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

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

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
 $\wedge y' = \text{ModExp}(g, x, p)$
 $\wedge \text{UNCHANGED } \langle p, q, g, x, k, r, s, w, u1, u2, v, \text{hashM}, \text{signature}, \text{verified} \rangle$

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

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

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

$$\begin{aligned} \text{Init} &\triangleq \\ &\wedge p \in \text{Prime} \\ &\wedge q \in \text{Prime} \\ &\wedge p \neq q \\ &\wedge g \in 2 \dots (p-1) \\ &\wedge x \in 1 \dots (q-1) \\ &\wedge k \in 1 \dots (q-1) \\ &\wedge \text{hashM} \in 1 \dots (q-1) \\ &\wedge y = \text{ModExp}(g, x, p) \\ &\wedge r = (\text{ModExp}(g, k, p) \% q) \\ &\wedge s = (\text{InverseMod}(k, q) * (\text{hashM} + x * r)) \% q \\ &\wedge \text{signature} = \langle r, s \rangle \\ &\wedge w = \text{InverseMod}(s, q) \\ &\wedge u1 = (\text{hashM} * w) \% q \\ &\wedge u2 = (r * w) \% q \\ &\wedge v = ((\text{ModExp}(g, u1, p) * \text{ModExp}(y, u2, p)) \% p) \% q \\ &\wedge \text{verified} = (v = r) \end{aligned}$$

$$\begin{aligned} \text{Next} &\triangleq \\ &\vee \text{GenerateKeys} \\ &\vee \text{Sign} \\ &\vee \text{Verify} \end{aligned}$$

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