MODULE *rsa*

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

VARIABLES p, q, n, phi, e, d, m, c, $message$, $ciphertext$, $plaintext$

Definicija prostih brojeva u ograničenom opsegu

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

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
$\quad\quad\quad (base * ModExp(base,\ exp - 1,\ mod))\%mod$

Generisanje ključeva

$GenerateKeys \triangleq$
$\quad \land\ d' =$ CHOOSE $x \in 1 \,..\, (phi - 1) : (e * x)\%phi = 1$
$\quad \land$ UNCHANGED $\langle p,\ q,\ n,\ phi,\ e,\ m,\ c,\ plaintext,\ ciphertext,\ message\rangle$

Enkripcija

$Encrypt \triangleq$
$\quad \land\ c' = ModExp(m,\ e,\ n)$
$\quad \land$ UNCHANGED $\langle p,\ q,\ n,\ phi,\ e,\ d,\ m,\ plaintext,\ ciphertext,\ message\rangle$

Dekripcija

$Decrypt \triangleq$
$\quad \land\ plaintext' = ModExp(c,\ d,\ n)$
$\quad \land$ UNCHANGED $\langle p,\ q,\ n,\ phi,\ e,\ d,\ m,\ c,\ ciphertext,\ message\rangle$

Izlaz

$Output \triangleq$
$\quad \land\ ciphertext' = c$
$\quad \land\ message' = plaintext$
$\quad \land$ UNCHANGED $\langle p,\ q,\ n,\ phi,\ e,\ d,\ m,\ c,\ plaintext\rangle$

Sledeće stanje sistema

$Next \triangleq$
$\quad \lor\ GenerateKeys$
$\quad \lor\ Encrypt$
$\quad \lor\ Decrypt$

$\lor$ *Output*

Inicijalno stanje

$Init \triangleq$

$\land\ p \in Prime$
$\land\ q \in Prime$
$\land\ p \neq q$
$\land\ n = p * q$
$\land\ phi = (p-1) * (q-1)$
$\land\ e \in 1 \,..\, (phi-1)$
$\land\ \exists\, x \in 1 \,..\, (phi-1) : (e * x)\%phi = 1$
$\land\ d\ = \text{CHOOSE}\ x \in 1 \,..\, (phi-1) : (e * x)\%phi = 1$
$\land\ m \in 1 \,..\, (n-1)$
$\land\ c\ = ModExp(m,\ e,\ n)$
$\land\ plaintext = ModExp(c,\ d,\ n)$
$\land\ ciphertext = c$
$\land\ message = plaintext$

Specifikacija

$Spec \triangleq$

$Init \land \Box[Next]_{\langle p,\ q,\ n,\ phi,\ e,\ d,\ m,\ c,\ plaintext,\ ciphertext,\ message \rangle}$