Contents

1 cryptoExercise Theory

Built: 26 March 2019
Parent Theories: string, cipher

1.1 Theorems

[exercise15_6_4_1a_thm]

⊢ ∀ *key enMsg message*.
(deciphS *key enMsg* = SOME *message*) ⟺
(*enMsg* = Es *key* (SOME *message*))

[exercise15_6_4_1b_thm]

⊢ ∀ *keyAlice k text*.
(deciphS *keyAlice* (Es *k* (SOME *text*)) =
SOME "This is from Alice") ⟺
(*k* = *keyAlice*) ∧ (*text* = "This is from Alice")

[exercise15_6_4_2a_thm]

⊢ ∀ *P message*.
(deciphP (pubK *P*) *enMsg* = SOME *message*) ⟺
(*enMsg* = Ea (privK *P*) (SOME *message*))

[exercise15_6_4_2b_thm]

⊢ ∀ *key text*.
(deciphP (pubK *Alice*) (Ea *key* (SOME *text*)) =
SOME "This is from Alice") ⟺
(*key* = privK *Alice*) ∧ (*text* = "This is from Alice")

[exercise15_6_4_3_thm]

⊢ ∀ *signature*.
signVerify (pubK *Alice*) *signature*
(SOME "This is from Alice") ⟺
(*signature* =
sign (privK *Alice*) (hash (SOME "This is from Alice")))

Index