

Contents

1	cryptoExercise Theory	3
1.1	Theorems	3

1 cryptoExercise Theory

Built: 26 March 2019

Parent Theories: string, cipher

1.1 Theorems

[exercise15_6_4_1a_thm]

$$\begin{aligned} \vdash \forall key\ enMsg\ message. \\ (\text{deciphS } key\ enMsg = \text{SOME } message) \iff \\ (enMsg = \text{Es } key\ (\text{SOME } message)) \end{aligned}$$

[exercise15_6_4_1b_thm]

$$\begin{aligned} \vdash \forall keyAlice\ k\ text. \\ (\text{deciphS } keyAlice\ (\text{Es } k\ (\text{SOME } text)) = \\ \text{SOME "This is from Alice"}) \iff \\ (k = keyAlice) \wedge (text = \text{"This is from Alice"}) \end{aligned}$$

[exercise15_6_4_2a_thm]

$$\begin{aligned} \vdash \forall P\ message. \\ (\text{deciphP } (\text{pubK } P)\ enMsg = \text{SOME } message) \iff \\ (enMsg = \text{Ea } (\text{privK } P)\ (\text{SOME } message)) \end{aligned}$$

[exercise15_6_4_2b_thm]

$$\begin{aligned} \vdash \forall key\ text. \\ (\text{deciphP } (\text{pubK } Alice)\ (\text{Ea } key\ (\text{SOME } text)) = \\ \text{SOME "This is from Alice"}) \iff \\ (key = \text{privK } Alice) \wedge (text = \text{"This is from Alice"}) \end{aligned}$$

[exercise15_6_4_3_thm]

$$\begin{aligned} \vdash \forall signature. \\ \text{signVerify } (\text{pubK } Alice)\ signature \\ (\text{SOME "This is from Alice"}) \iff \\ (signature = \\ \text{sign } (\text{privK } Alice)\ (\text{hash } (\text{SOME "This is from Alice"}))) \end{aligned}$$

Index

cryptoExercise Theory, 3

 Theorems, 3

 exercise15_6_4_1a_thm, 3

 exercise15_6_4_1b_thm, 3

 exercise15_6_4_2a_thm, 3

 exercise15_6_4_2b_thm, 3

 exercise15_6_4_3_thm, 3