University of Padua
Department of Information Engineering

Implementation and weakness evaluatation of a challenge-response scheme for entity authentication

Authors:
Sara Bardi
Simone Favaro
Alessandro Rizzo

Teacher:
Nicola Laurenti

20th December 2020

Abstract

General settings

Task implementation

Task 1 - Implement the protocol

Task 2 - Implement the first attack

Task 3 - Implement the second attack