Home Assignment 4

Rasmus Olofzon, 9104192472

Complete the eight A-assignments below and solve them individually.

- A-2 What problem in OTR is solved using the Socialist Millionaire Problem?
- A-4 How is perfect forward secrecy solved in OTR?
- **A-7** Why does not an IdP send a response to an authentication request with the HTTP GET method? What alternatives are there?
- **A-9** Name and describe four profiles in SAML. You should be able to provide a more detailed description for one of them.
- A-11 Describe and compare "discovery" in SAML and OpenID.
- **A-12** In a certain sense, there are three different types of communication in SAML and two in OpenID. Describe them and explain the difference.
- A-18 In OAuth, explain why the access token must not be cached, and how this is achieved.
- A-20 What is a grant? Name and describe a few different grants.