A-2 What problem in OTR is solved using the Socialist Millionaire Problem?

Grading: 1.0
Motivation:
Good answer. Agrees with the lecture notes about Secure Messaging

A-3 Why is the Socialist Millionaire Problem not useful in TLS? Or would it be?

Grading: 1.0
Motivation:
Very good answer and motivation. The lecture notes as well as wikipedia page about TLS (https://en.wikipedia.org/wiki/Transport_Layer_Security) provides the same information.

A-5 How would security in the OTR authentication be affected if the Diffie-Hellman values were encrypted using the recipient's public key (instead of being signed by the sender's private key)?

Grading: 1.0
Motivation:
True! The perfect forward secrecy would be compromised during the authentication. Similar information can be found here: https://blog.securegroup.com/otr-encryption-for-chat-explained

A-7 Why does not an IdP send a response to an authentication request with the HTTP GET method? What alternatives are there?

Grading: 1.0
Motivation:
Not sure if this is the correct answer. According to the lecture notes the response cannot use the HTTP redirect binding since a response is too large to fit within the maximum URL length supported by user-agents. However, the answer provided here also makes sense. In fact, when thinking about it, it's pretty obvious that the response can't be an HTTP GET because of the arguments given in your answer.

A-10 Describe the purpose of RelayState and show how it is used.

Grading: 1.0
Motivation:
Good answer. Agrees with the information in the lecture notes (page 4-5) as well as on this page: https://blogs.sap.com/2019/02/19/what-is-relaystate-in-saml-and-how-to-configure-relaystate-on-as-abap/

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.

Grading: 0.5
Motivation:
I had the same question and got confused about what the three different types of communications in SAML are. He responded to me saying that it is the different bindings, i.e. HTTP POST binding, HTTP redirect binding and HTTP artifact binding. Therefore, the answer provided here might be wrong in the context. The communications in OpenID are correct however (according to the lecture notes).

A-14 Can an SP authenticate a user through an IdP that the SP has never used before? Compare SAML and OpenID.

Grading: 1.0
Motivation:
Well-put answer that agrees with the information in the lecture notes as well as this page for example: https://spin.atomicobject.com/2016/05/30/openid-oauth-saml/

A-20 What is a grant? Name and describe a few different grants.

Grading: 1.0
Motivation:
Correct answer once again. Corresponds with the information on this page for example: https://alexbilbie.com/guide-to-oauth-2-grants/

Total score: 7.5