A-1: Explain the purpose of using a MAC instead of a digital signature in OTR.
Answer: A digital signature would link the communication to the person signing it, which would defeat the purpose of OTR (Off The Record) communication. The MAC could however only be computed by Alice or Bob and to mitigate this the MAC is sent in the next message in the communication. This gives both Alice and Bob the possibility to deny having sent the message since anyone could have listened to the following message and made a new fake message.
A-10: Describe the purpose of RelayState and show how it is used.
Answer: The purpose of RelayState is so that the service provider (SP) to get back to the state it was in (when sending a request) when receiving a response. This is done so that the SP does not have to remember every single request.

The parameter is included in the request sent via either a GET or a POST request. An example of each can be seen below:
GET:

```
http://IdP-example.com/redirect?SAMLRequest=req&RelayState=token
```

POST:

```
<form method="post" action="https://IdP-example.com/redirect>
<input type="hidden" name="SAMLRequest" value="req" />
<input type="hidden" name="RelayState" value="token" />
<input type="submit" value="Submit" />
</form>
```

A-11: Describe and compare "discovery" in SAML and OpenID.
Answer: In both cases discovery refers to the SP/RP trying to determine which IDP/OP to communicate with. In SAML it is not specified how this should be done, however there is a SAML specified profile called *SAML identity provider discovery profile* that may be used for this. In OpenID the RP uses the identifier given by the user to determine which OP to use.
A-13: Describe two use cases — one where SAML and one where OpenID appears to be the best choice, respectively.
Answer: In the case of logging in to a blog or forum OpenID is the more suitable protocol it gives a bit more lightweight authentication in that the RP does not necessarily know the true identity of the user.

In the case of logging in to a online bank we need strong authentication of the users real identity and SAML is therefore preferable. SAML requires trust between the SP and IdP which makes the authentication more trustworthy.
A-14: Can an SP authenticate a user through an IdP that the SP has never used before? Compare SAML and OpenID.
Answer: No. SAML does not specify how the SP should determine which IdP to use, this could for instance be done by another service. Also there are no specified way to authenticate the user, this is left to the IdP to decide. However the SP can not verify that the IdP has authenticated the user unless the SP and IdP have a prior agreement that specifies how that should be done.

In OpenID this is possible since the there is an optional step in the protocol where an association for the RP and OP can be created even if they have not communicated before.
A-15: Briefly explain what an XRI is, and why it is a good idea to use it in the context of OpenID.
Answer: An XRI (Extensible Resource Identifier) is an identifier. The main point is to use one XRI that can be resolved to many different thing s such as name, email, web page and so on. A XRI points to a XRDS document containing the information thus making it easy to change things without having to change the XRI. This can be used in the context of OpenID to change

OP (OpenID Provider) without changing the XRI.

A-16: Describe how XRDS-based discovery and HTML-based discovery differ. In which context are they used?

Answer: When the RP gets the identifier from the user there are two possibilities XRDS- or HTML-based discovery. The XRDS based discovery can be done if the user identifier is an XRI or a URL, whereas HTML based can only be done with a URL. Should XRDS be used the XRI or URL will lead to a XRDS document where the RP can find the necessary information. In the case of HTML based discovery the URL will lead to a HTML document with the information.

Both of these methods are used in the OpenID protocol to allow the RP to determine the OP to use when authenticating. Both methods will lead the RP to a Endpoint URL that the RP should use for authentication.

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

Answer: A grant is a permission issued by a resource owner to give to a client so that the client can request a access to a resource on a resource server. The grant can contain information on e.g. what the client is allowed to access.

The most common grant is the authorization code where the resource owner issues a grant with a code that the client can give to the resource server in exchange for an access token. Another type of grant is the implicit grant where the client skips the step of receiving a grant i.e. the grant is implicit. Yet another grant type is the *Resource Owner Password Credentials Grant*. If this type is used the resource owner gives their credentials to the client and the client can then use these to get an access token. The last type of grant is the *Client Credentials Grant* where the client receives an access token after sending its credentials to the resource server thus skipping the resource owner.