4 A-assignments

A-1: Explain the purpose of using a MAC instead of a digital signature in OTR.
Digital signatures provide non-repudiation. A MAC uses symmetric keys so any MAC protected message can be verified by the receiver. However, the receiving end cannot convince anybody else that is was sent from that specific sender.

A-3: Why is the Socialist Millionaire Problem not useful in TLS? Or would it be?
In TLS, the end users are typically not authenticated as this is often left to the application layer after the authentication and key agreement phase of TLS. In order to make this practical, Alice and Bob must exchange fingerprints of their public key and verify this fingerprint in order to authenticate the key exchange messages.

Without the use of digital signatures, Eve can mount a Man-in-the-Middle attack on the protocol and agree on one key with Alice, and one with Bob. She could then add, delete, or modify messages as she acts as a the Man-in-the-Middle.

A-4: How is perfect forward secrecy solved in OTR?
By using Diffie-Hellman key exchange for each message. By using it for each message the forward secrecy is true, not only for sessions, but also individual messages.

A-6: List two advantages and two drawbacks of SSO compared to "normal" password authentication.
Using different user names and passwords for all web services one uses has several disadvantages. Firstly, if all passwords are different, chances are high that a user either writes them down or chooses bad passwords. A bad password can have serious consequences if the database with hashed passwords is stolen since they would most likely be revealed through dictionary or brute force attacks. Jotting down passwords on a physical piece of paper is in that event a better solution unless the list is exposed or someone gets access to it.

Another disadvantage is that users must trust every single web service to handle the credentials in a proper way although numerous examples show that even large websites treat passwords in a very uneducated way, making the password vulnerable for hijacking. A web based single sign-on solution solves these problems. The user only has to have one password, which can be used to log into all services.

A-9: Name and describe four profiles in SAML. You should be able to provide a more detailed description for one of them.
A profile defines how the assertions, protocols and bindings are to be used in a specific usage scenario. The *Web Browser SSO Profile* is a profile used for web based single sign-on. *Enhanced Client and Proxy Profile* is a profile which supports single sign-on with clients that have more capabilities than an ordinary web browser. The *Single Logout Profile* is used to simultaneously logout from all different services that a user might be logged on to using single sign-on. The *Identity Provider Discovery Profile* specifies different ways of how a subject can be authenticated by the identity provider. If a user has more than one identity provider the service provider will need a way to discover which identity provider to use. The discovery profile relies on a *cookie* that is written in a domain that is common between identity providers and service providers in a deployment.

A-11: Describe and compare "discovery" in SAML and OpenID.
Discovery in OpenID is when the relying party uses the, by the user, presented identifier to determing which OpenID Provider to use for authentication. In SAML it isn't really specified who is to authenticate but rather how. This is specified in the Identity Provider Discovery Profile described above.

A-14: Can an SP authenticate a user through an IdP that the SP has never used before? Compare SAML and OpenID.
Sensitive user information that is accessible online also requires the web service to know the true identity of the user. In SAML this can only be provided by the web based SSO technologies if the SP can trust the IdP to collect, maintain and provide such information. OpenID doesn't need a trust relationship and is often used in online services which don't require the identity of the user. However this opens the possibility for malicious relying parties who can attempt phising attacks on users.

A-17: What is the purpose of the Yadis protocol?
The Yadis protocol is used for retrieving an XRDS document from a URL.