6.3 Question 3

6.3.A What type of authentication is the following? Describe the steps of a reflection attack against it.

The picture shows a mutual authentication type with the use of a shared key between A and B.
A possible reflection attack for this type would look as the following:

1. Adversary $\mathcal{Z}$ sends $\mathcal{A}$ and R_1 to $\mathcal{B}$
2. $\mathcal{B}$ sends the encrypted $f\{K_{\mathcal{AB}}, R_1\}$ and R_2 to $\mathcal{Z}$
3. $\mathcal{Z}$ does not know shared key, hence:
   (a) $\mathcal{Z}$ opens another channel and sends $\mathcal{A}$ and R_2 (from above) to $\mathcal{B}$
   (b) $\mathcal{B}$ sends the encrypted $f\{K_{\mathcal{AB}}, R_2\}$ and another R_3 to $\mathcal{Z}$
4. $\mathcal{Z}$ can now send $f\{K_{\mathcal{AB}}, R_2\}$ to $\mathcal{B}$

$\Rightarrow$ $\mathcal{Z}$ is now authenticated as $\mathcal{A}$ to $\mathcal{B}$

6.3.B A server is using Lamport's Hash without salt. How does it work exactly? What are its main strengths and weaknesses?

A server $\mathcal{S}$ always knows the number n, which is always decremented, the user name and the corresponding password in the form of $\texttt{hash}^n(\texttt{password})$. This also means that the password itself is not leaked to the $\mathcal{S}$. The Authentication process would now look as the following:

1. $\mathcal{A}$ wants to authenticate itself
2. $\mathcal{S}$ sends $\mathcal{A}$ the current value of n
3. $\mathcal{A}$ computes $\texttt{hash}^n(\texttt{password})$
4. $\mathcal{A}$ sends the computed value to $\mathcal{B}$
5. $\mathcal{S}$ compares the received value with the stored value
6. If both values match $\mathcal{S}$ decrements the number n
7. $\mathcal{S}$ asks $\mathcal{A}$ for $\texttt{hash}^{n-1}(\texttt{password})$

As previously mentioned its main advantage is that the server $\mathcal{S}$ does not need to know the actual password itself in order to authenticate a user. The disadvantage of this approach is that the number of logins is limited by the number n as resetting it would cause some security issues and mutual authentication is not provided.

6.3.C The following protocol is based on DES encryption in CBC mode. What type of authentication does it offer? Explain what is the main vulnerability of this approach? With that in mind, how can this protocol be enhanced?

This authentication is based on the Needham-Schroeder protocol seen in the lecture. The only difference is that the nonces are not decremented.
The main problem here would be occuring if $K_{\mathcal{AB}}\{N_2, N_3\}$ can be easily split up into $K_{\mathcal{AB}}\{N_2\}$ and $K_{\mathcal{AB}}\{N_3\}$. Then this authentication protocol is prone to replay attacks. This can be counter-measured by either making it infeasible to split up the encrypted message into its subparts, i.e. not using simple concatenation or altering the nonce N_2 so that not the actual encrypted value is shared.