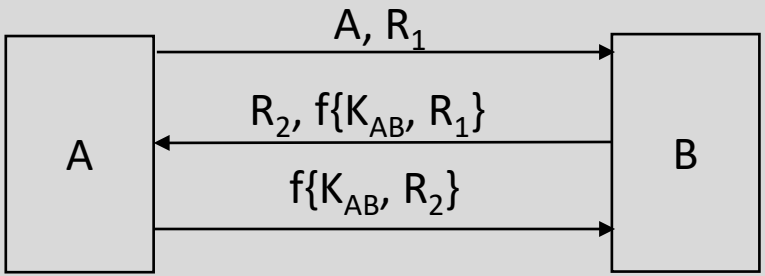
Question 2:

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



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

Question 2:

- **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?