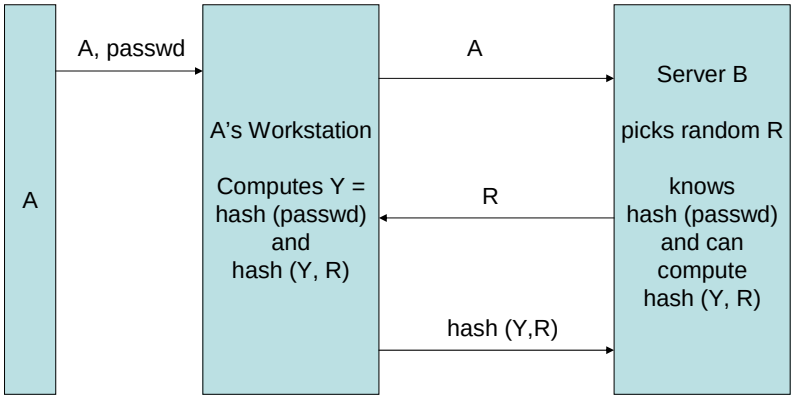
**E4.44 Network Security : Problem Sheet 3**

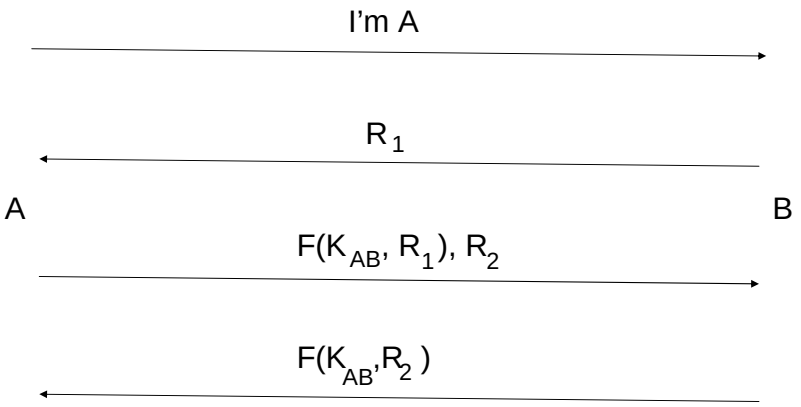
1. Figure 1 shows an authentication protocol similar to that used in Novell Version 3 Security. In the figure B authenticates the human user A through checking a hash of A's password as produced by A's workstation. Analyse the strength of this system against (a) eavesdropping and (b) server database disclosure.

Figure 1



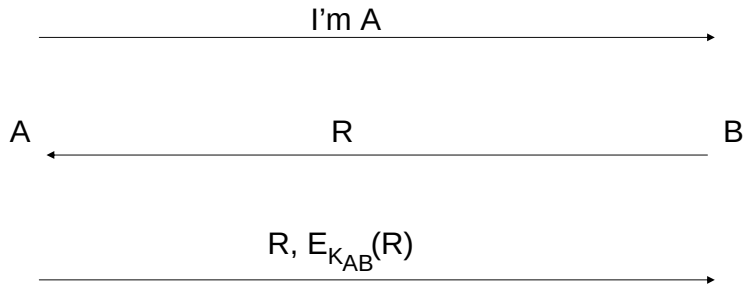

2. Figure 2 shows a mutual authentication scheme based on a secret shared by the communicating parties. Would this protocol be susceptible to a reflection attack?

# Figure 2




3. Figure 3 shows a 3-message authentication protocol in which B is a stateless server which requires its challenge to be transmitted back to it together with the response. Is this protocol secure?

# Figure 3




4. Given that the Lamport hash is sent in clear over the network, why is it more secure than a password?

5. Is the Lamport hash vulnerable to dictionary attack by an eavesdropper? Can somebody impersonating the server do a dictionary attack?

6. Design a variant of Lamport's hash which uses k times more storage at the server but which needs 1/k less processing at the client

7. In Kerberos the KDC database is not encrypted as a unit but each principal's master key is encrypted under the KDC master key. If replicated KDCs received a download from the master (i.e. without any cryptographic integrity check) how could a rogue principal registered on the KDC attack the database in transit and then impersonate another principal on the system. Assume the rogue principal cannot obtain the KDC master key.

8. In Kerberos V5 the idea behind the requirement to renew tickets before they expire is to remove the requirement for a KDC to remember blacklisted tickets indefinitely. Does this apply also to postdated tickets which may be requested with a start-time arbitrarily far into the future?

9. In a PKI why must a CRL be issued periodically even when no new certificates have been revoked?

10. If there is a revocation mechanism why do certificates need an expiration date?