AuthenticationOverview (A)
1) What options are available in authentication protocols?

Multiple choice:
1) The following capabilities can be provided by an authentication protocol except
a) Mutual
b) Preserve privacy
c) Encryption
d) Unilateral

2) Two-stage authentication refers to
a) Using an n-digit PIN to verify the user to the token, and then the token uses an internal secret to verify to the server
b) Using two token-generated internal secrets in a row
c) Using two user-generated secrets in a row
d) Using a random number in the second stage of the authentication

AuthenticationOverview (B)
1) Why is necessary for the challenge and secret in a challenge-response authentication protocol be inseparably bound in the response?

Multiple choice:
1) Why is necessary for the challenge and secret in a challenge-response authentication protocol be inseparably bound in the response?
a) To ensure that the secret is unique in the response
b) To make it very difficult or impossible for the adversary to reverse engineer the secret from the response
c) To protect the challenge from reverse engineering attacks
d) To ensure the combination of the challenge and secret are unique

2) Why is a clear text field r-sub-A sent in a hash-based challenge-response authentication scheme?
a) To allow party B to compute a random nonce
b) To allow party B to generate a witness
c) To allow party B to carry out mutual authenication
d) To allow party B to confirm that the locally computed hash is the same as the value received