For a hierarchical PKI shown above

1. What are the certificates stored by D and G?
2. What certificates are produced by G (to D) in order to authenticate its public key?

(The certificate for the public key of G, signed by F, is represented as $F^{<G>}$)

Is the “Man-in-the-middle attack” possible for

1. two parties employing Kerberos?
2. two parties employing asymmetric cryptography without public key certificates?
3. two parties employing asymmetric cryptography with public key certificates?

Explain.

Briefly explain the “reflection attack” in challenge-response protocols. Suggest some techniques to address overcome this attack.

What is the main purpose of the “authenticator” sent along with Kerberos tickets?