

CMSC 414 Fall 2006 Hw4 Solution

3. (4 points)

(text 11.8) Design a two-message authentication protocol that achieves both mutual authentication and establishment of a session key, assuming that Alice and Bob know each other's public keys.

Solution

Alice picks a session key K and sends a signed message containing K encrypted by Bob's public key and a timestamp ts . (nonce is not enough to detect message reply)

Bob responds with the timestamp ts encrypted with K .

(Explanation of K and ts) ----- 1

A (Alice)	B (Bob)
<ul style="list-style-type: none"> • send [$\{K\}_B, ts]_A$ to B • 	<p>send [$K\{ts\}$]</p>

(Protocol) ----- 3

5. (3 points)

(text 16.1) Which of the following properties does protocol 16-2 have: perfect forward secrecy (PFS); escrow foilage against passive attacks; escrow foilage against active attacks; identity hiding; perfect forward secrecy for identity hiding. Assume private encryption keys are escrowed and private signature keys are not escrowed.

Solution

PFS; -----1

escrow foilage against passive attacks; -----1

escrow foilage against active attacks (unless signature key is escrowed); -----1

no identity hiding.

11. (3 points)

(text 16.5) Referring to section 16.6 *Endpoint Identifier Hiding*, show a protocol that hides both identifiers from an active attacker, assuming that Alice (the initiator) already knows Bob's public key.

Solution

Alice sends: -----2

{ Alice, Alice's public key certificate, Alice's Diffie-Hellman value }_{Bob's public key}

Bob replies: -----1

{ } Alice's public key.