Grundlagen Informationsicherheit und Datensicherheit, Blatt 6

Lukas Baur, 3131138
Felix Bühler, 2973410
Marco Hildenbrand, 3137242

29. Januar 2018

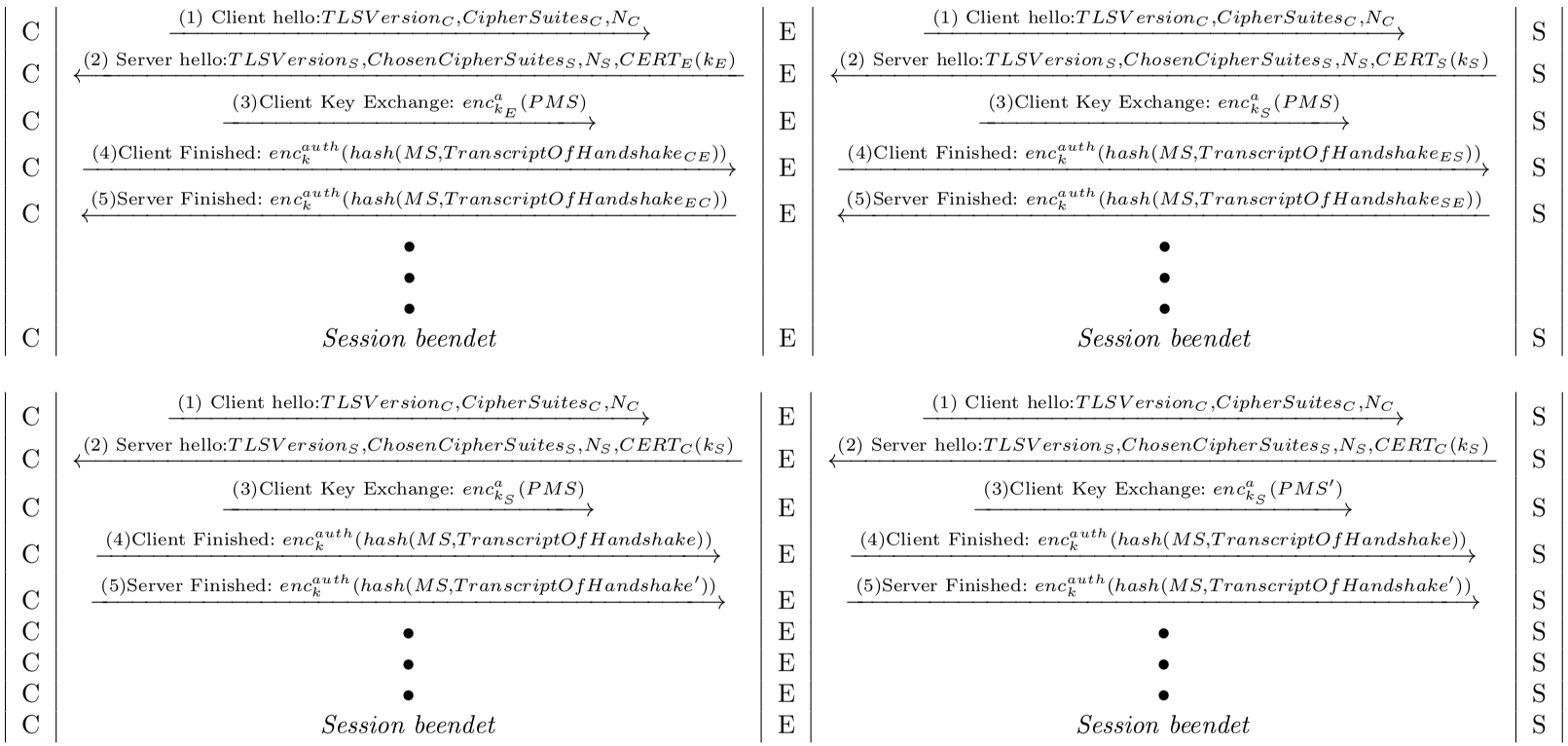
Problem 1

(a)

Problem 2:

(a)

Problem 3


C
E
S
(1) Client hello:$TLSVersion_C$,$CipherSuites_C$,N_C
(2) Server hello:$TLSVersion_S$,$ChosenCipherSuites_S$,N_S,$CERT_E(k_E)$
(3)Client Key Exchange: $enc^a_{k_E}(PMS)$
(4)Client Finished: $enc^{auth}_k(hash(MS,TranscriptOfHandshake_{CE}))$
(5)Server Finished: $enc^{auth}_k(hash(MS,TranscriptOfHandshake_{EC}))$
Session beendet
(2) Server hello:$TLSVersion_S$,$ChosenCipherSuites_S$,N_S,$CERT_S(k_S)$
(3)Client Key Exchange: $enc^a_{k_S}(PMS)$
(4)Client Finished: $enc^{auth}_k(hash(MS,TranscriptOfHandshake_{ES}))$
(5)Server Finished: $enc^{auth}_k(hash(MS,TranscriptOfHandshake_{SE}))$
Session beendet
(2) Server hello:$TLSVersion_S$,$ChosenCipherSuites_S$,N_S,$CERT_C(k_S)$
(3)Client Key Exchange: $enc^a_{k_S}(PMS)$
(4)Client Finished: $enc^{auth}_k(hash(MS,TranscriptOfHandshake))$
(5)Server Finished: $enc^{auth}_k(hash(MS,TranscriptOfHandshake'))$
Session beendet
(2) Server hello:$TLSVersion_S$,$ChosenCipherSuites_S$,N_S,$CERT_C(k_S)$
(3)Client Key Exchange: $enc^a_{k_S}(PMS')$
(4)Client Finished: $enc^{auth}_k(hash(MS,TranscriptOfHandshake))$
(5)Server Finished: $enc^{auth}_k(hash(MS,TranscriptOfHandshake'))$
Session beendet