8. Exercise sheet
Hand in solutions until Sunday, 29 May 2011, 23:59

Exercise 8.1 (Vulnerability of SSL (I)). (12+8 points)


(ii) Describe the attack model. 4

(iii) How does the weak variant of CBC differ from the standard one? Guess, why the weak variant is used nevertheless. 3

(iv) Which powers/sources does an attacker need? 4

(v) Describe each step of the attack along with a judgment of feasibility. +6

(vi) Quickly describe the idea behind the suggested countermeasures. +2

(vii) Is the attack still feasible in the latest version of TLS? 1

Exercise 8.2 (Vulnerability of SSL (II)). (10 points)


(ii) Describe the attack model. 4

(iii) Describe the idea behind the CertLock solution. 3

(iv) Why should sites consider the country of the CA they use? 3