8. Exercise sheet
Hand in solutions until Monday, 10 July 2017, 09:00

Exercise 8.1 (Project, part 4). (16+2 points)

Consider all protocols considered in course and project, ie. TLS, IPsec/IKE, ssh and Signal. Draw conclusions:

(i) What’s the year of first appearance? +2
(ii) Compare the design. Judge by features, complexity, ‘beauty’, … 4
(iii) Compare the security aspects. PFS, DoS, … 4
(iv) Compare the state of proven security. 8