Home Assignment Markings HA4 - A-level

A-2

Just states that it solves the agreement of keys, but gives no explanation on what part or how. SMP makes it possible to exchange public keys, agree on a shared secret, without knowing eachothers public keys before, using a 'shared secret'. Eve would only have 1 chance to guess that secret. Then Alice and Bob will have both verified eachothers public keys, and set a shared secret and can start talking.

Deduction: -0.75 points

A-4

Correct answer, in accordance with page 5 in the lecture notes.

Deduction: 0.0 points

A-7

Correct answer, in accordance with what was said on the lecture.

Deduction: 0.0 points

A-9

Only a partial answer. Will deduct 0.25 points per missing answer

Deduction: -0.75 points

A-11

Correct answer. See slides 7, 10, 12 and 14.

Deduction: 0.0 points

A-12

Almost fully correct. In SAML, IdP can initate the communication, and it goes via Alice, SP initiates the communication, and it goes via Alice. Or (the missing option) they use artifact binding and talk directly to each other

Deduction: -0.10 points

A-18

Correct answer, see page 14 in the lecture notes.

Deduction: 0.0 points

A-20

Correct answer, see slide 23-26 and pages 12-14 in the lecture notes.

Deduction: 0.0 points