I5020 Computer Security

Quizz 3: Security concepts and cryptographic tools

This assessment evaluates the following competencies:

- *CS002 – Define and explain the basic security concepts and the relations between them*
- *CS001 – Understand the CIA triad and use it to explain the key objectives of computer security*
- *CS102 – Make connections between cryptographic tools and the CIA triad*

For the first assessed competency (CS002), you have to fill in the following text with the correct basic security concept. To get a star for the competency, you must have the correct answer for the four missing words in the following text.

To ⬚, that is, the probability that a ⬚

exploit a vulnerability so that to affect some assets of the company, one possible

solution is to set up some ⬚ that can either prevent

or detect a particular type of attack, to avoid it to succeed or to recover from

its effects, of course taking into account ⬚, that is,

new vulnerabilities introduced that should clearly be minimised.

For the two last assessed competencies (CS001 and CS102), you have to link the six following sentences, describing either a problem or a cryptographic tool (three sentences for each), with the correct component of the CIA triad. To get the stars for the competencies, you must have the correct answer for the set of three sentences (one set for each competency).

1. Someone stole my USB memory stick and I do not want him/her to be able to read its content. ◯

2. My website is not responding fast enough and some customers are leaving it before buying anything on the webstore. ◯

3. I want to send the admin password of a server to a friend but do not want anyone to eavesdrop the communication and intercept it. ◯

4. Advanced Encryption Standard (AES) ◯

5. CBC-MAC ◯

6. SHA-256 ◯

◯ C

◯ I

◯ A