Example solutions / correct answers are marked in yellow.

Task 1

One important security goal in information security is confidentiality. Pick an example from your daily (digital) life where confidentiality is important. Explain what might happen if an attacker could get access to the confidential data.

Online shopping -> transfer of credit card number should be confidential -> attacker might sell/misuse the credit card number.

Task 2

Mark the statement(s) about symmetric encryption that are true.
One or more options might be correct.

- ○ Symmetric encryption is a rather new concept invented in the 20th century.
- ○ Symmetric encryption uses the same key for encryption and decryption.
- ○ The security of symmetric encryption algorithm depends on the number of possible keys.
- ○ Symmetric encryption ensures authenticity, i.e., to identify the sender

Task 3

Please explain what phishing is and how it can be detected.

(Check lecture slides).

Task 4

You are visiting the Web page https://www.online-shop.com/ (i.e., you are using TLS). Mark the statements that are true.

- ○ The Web page is guaranteed a phishing page
- ○ The Web page is guaranteed not a phishing page
- ○ The connection is guaranteed with the host www.online-shop.com
- ○ If you enter your credit card number on the Web page, an adversary eavesdropping on the wire can see it.

Task 5

You are visiting the Web page https://www.online-shop.com/ a week later. This time the browser shows a warning message "The certificate is for www.online-ship.com. Do you want to continue and visit the site?" What might be reason? What should you do?

The reason is most probably an attack. An attacker owns the domain www.online-ship.com, received a certificate for this and installed it on his/her web server. In addition, he/she was able to redirect you from www.online-shop.com to his/her server. You should not continue.