(For multiple choice: the correct answers are marked in yellow.)

Task 1

Which of the following definitions (from the NIST) defines the term “confidentiality”:

- ○ … means ensuring timely and reliable access to and use of information.
- ○ … means guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.
- [✓ ○ … means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information.]

Task 2

Mark the statement(s) about the Diffie-Hellman Key Exchange (DHKE) that are true.
One or more options might be correct.

- ○ DHKE was invented in the middle age
- ○ DHKE ensures authenticity, i.e., to identify the sender
- [✓ ○ DHKE allows to exchange a key that can then be used for symmetric encryption]
- ○ Before DHKE, symmetric encryption was not possible

Task 3

Please explain what phishing is.

It comes from “Password fishing”, and is a way to get confidential information (such as passwords) by making victims believe they enter it on a trusted web site. The person who wants to misuse the password will send out emails to victims with links to fake web sites.

Task 4

TLS (which is also used in HTTPS) uses certificates. Mark the statements that are true.

- [✓ ○ A certificate authority issues a certificate only to the rightful owner of the domain.]
- ○ A certificate shows that the Web page is trustworthy
- [✓ ○ The certificate (used in a TLS connection) guarantees authenticity.]
- [✓ ○ Certificates are available free of charge.]