1. Wählen Sie jeweils eine Variante des folgenden Textes, so dass die Aussage richtig ist.

Bei der Verwendung der (~~symmetrischen Kryptographie~~ / Kryptographie mit öffentlichen Schlüsseln) können Kommunikationspartner ohne eine vorhandene Sicherheitsregelung Nachrichten auf eine sichere Weise austauschen.

Um eine digitale Signatur zu verifizieren, ist (~~der geheime Schlüssel des Senders~~ / der öffentliche Schlüssel des Senders / ~~der geheime Schlüssel des Empfängers~~ / ~~der öffentliche Schlüssel des Empfängers~~) erforderlich.

Der Schlüssel in der symmetrischen Kryptographie ist (kürzer / ~~länger~~) als der Schlüssel in der Kryptographie mit öffentlichen Schlüsseln.

Der Prozess der symmetrischen Verschlüsselung ist (~~langsamer~~ / schneller) als der Prozess der Verschlüsselung mit öffentlichen Schlüsseln.

(Symmetrische Kryptographie / ~~Kryptographie mit öffentlichen Schlüsseln~~) verwendet für die Ver- und Entschlüsselung (den gleichen Schlüssel / ~~unterschiedliche Schlüssel~~).

(~~Symmetrische Kryptographie~~ / Kryptographie mit öffentlichen Schlüsseln) verwendet für die Ver- und Entschlüsselung (~~den gleichen Schlüssel~~ / unterschiedliche Schlüssel).

In der hybriden Kryptographie verschlüsselt der Benutzer die Daten (mit einem symmetrischen Algorithmus / ~~mit einem Algorithmus der öffentlichen Schlüssel~~).

In der hybriden Kryptographie wird (~~der geheime Schlüssel des Senders~~ / ~~der öffentliche Schlüssel des Senders~~ / ~~der geheime Schlüssel des Empfängers~~ / der öffentliche Schlüssel des Empfängers) zur Verschlüsselung (~~der Benutzerdaten~~ / des Sitzungsschlüssels) verwendet.

Erasmus+
Dieses Projekt wurde mit Unterstützung der Europäischen Kommission finanziert.
Die Verantwortung für den Inhalt dieser Veröffentlichung (Mitteilung) trägt allein der Verfasser; die Kommission haftet nicht für die weitere Verwendung der darin enthaltenen Angaben.

2. Markieren Sie die korrekten Varianten.

X Die Signatur muss ein Bitmuster sein, das von der unterzeichneten Nachricht abhängt.

☐ Die Realisierung und Implementierung der digitalen Signatur muss relativ einfach ohne den geheimen Schlüssel erfolgen.

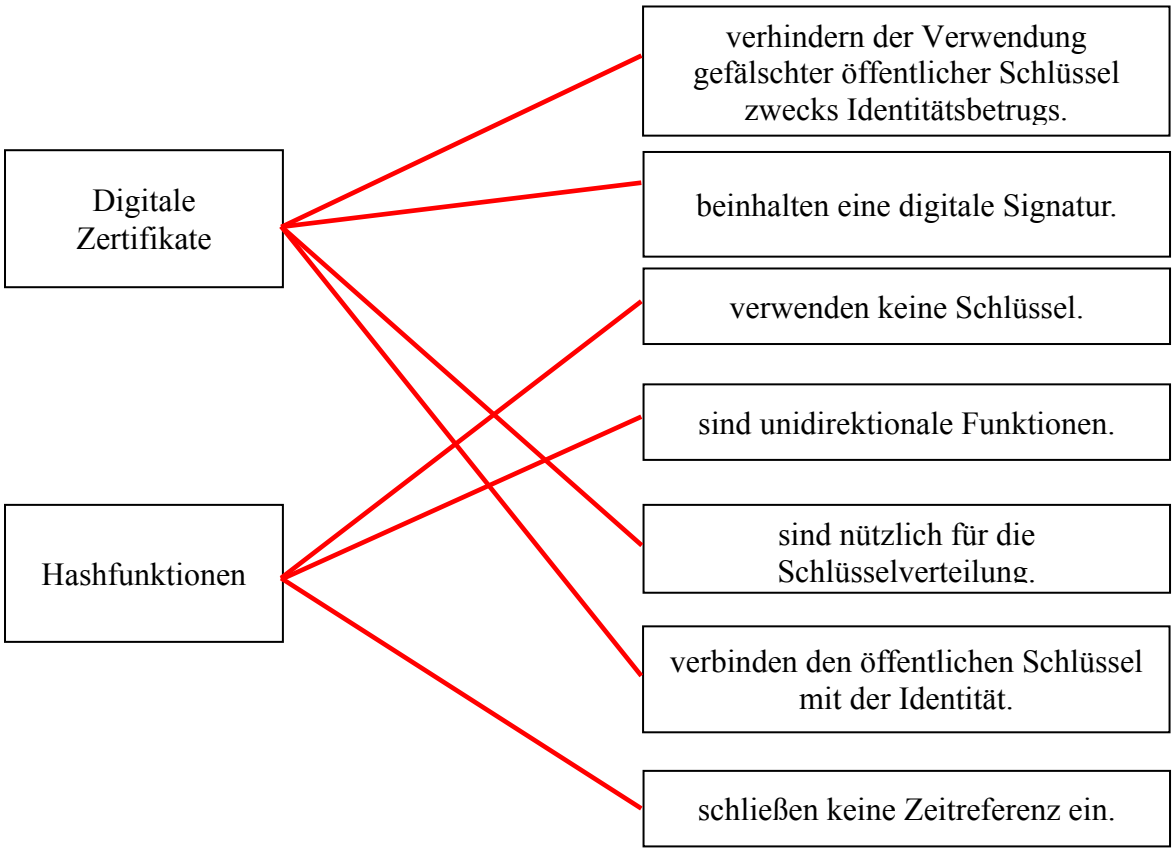
X Die Fälschung der digitalen Signatur muss rechnerisch unmöglich sein, und zwar entweder durch Erzeugung einer neuen Nachricht zur bestehenden digitalen Signatur oder durch Erzeugung einer betrügerischen digitalen Signatur zu einer bestehenden Nachricht.

☐ Mit der digitalen Signatur ist es möglich, die Nachricht zu entdecken.

X Der öffentliche Schlüssel des Unterzeichners ist für die Verifizierung seiner Signatur erforderlich.

---

3. Ordnen Sie dem Begriff in der linken Spalte die entsprechende(n) Definition(en) in der rechten Spalte zu.



Erasmus+
Dieses Projekt wurde mit Unterstützung der Europäischen Kommission finanziert.
Die Verantwortung für den Inhalt dieser Veröffentlichung (Mitteilung) trägt allein der Verfasser; die Kommission haftet nicht für die weitere Verwendung der darin enthaltenen Angaben.

4. Ergänzen Sie die Nummern der richtigen Aussagen in die folgende Tabelle.

1
3
4

1 – Die Verkehrsanalyse bezeichnet den Prozess des Abhörens und der Analyse der Nachrichten mit dem Ziel, über die Kommunikation Informationen zu erhalten.

2 – Angriffe auf Hosts bezeichnen alle Angriffe, die Computer oder Netzwerke ändern möchten, so dass ihre legitimen Benutzer sie nicht nutzen können.

3 – Angriffe mittels Protokollen nutzen die bekannten (oder auch unbekannten) Schwachstellen der Netzwerkdienste aus.

4 – Bei dem Man-in-the-Middle-Angriff fängt der Angreifer die Kommunikation zwischen zwei Parteien ab, üblicherweise zwischen dem Benutzer und dem Webserver.

5 – Denial-of-Service-Angriffe nutzen die Verwundbarkeiten in Computer-Betriebssystemen, in der Einstellung oder Verwaltung der Systeme aus.

Erasmus+
Dieses Projekt wurde mit Unterstützung der Europäischen Kommission finanziert.
Die Verantwortung für den Inhalt dieser Veröffentlichung (Mitteilung) trägt allein der Verfasser; die Kommission haftet nicht für die weitere Verwendung der darin enthaltenen Angaben.