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

Eines der Hauptprobleme (der symmetrischen Kryptographie / ~~der Kryptographie mit öffentlichen Schlüsseln~~) ist der Prozess der Schlüsselverteilung.

(Symmetrische Kryptographie / ~~Kryptographie mit öffentlichen Schlüsseln~~) (~~kann~~ / kann nicht) zur Erzeugung der digitalen Signatur verwendet werden.

(~~Symmetrische Kryptographie~~ / Kryptographie mit öffentlichen Schlüsseln) (kann / ~~kann nicht~~) zur Erzeugung der digitalen Signatur verwendet werden.

Im (ECB-Betriebsmodus / ~~CBC-Betriebsmodus~~) ist die Struktur des Klartextes offen.

Im CBC-Betriebsmodus (gibt es eine begrenzte Fehlerfortpflanzung / ~~gibt es eine begrenzte Fehlerfortpflanzung nicht~~).

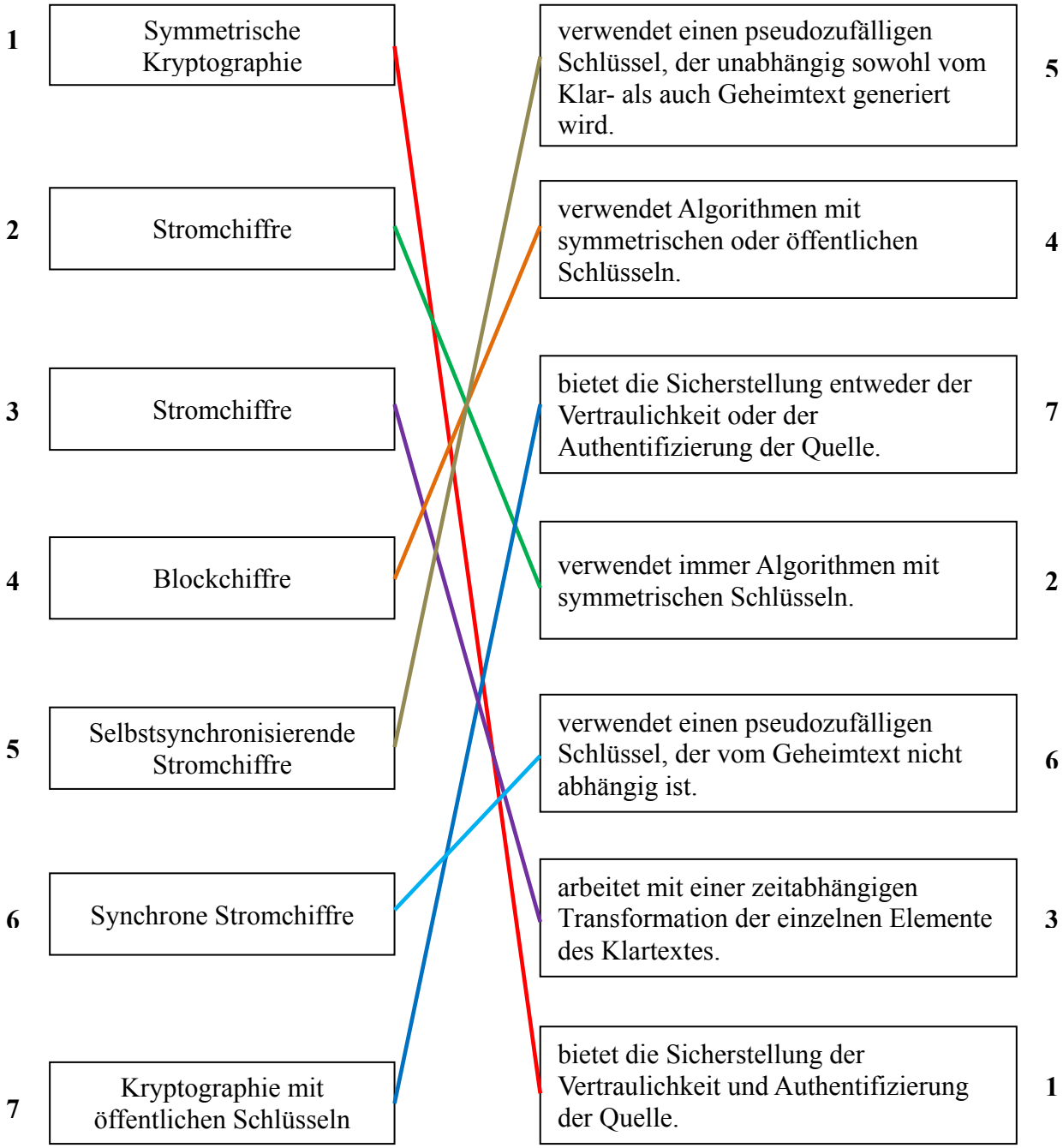
Falls ein Fehler im Geheimtext auftritt, pflanzt sich der Fehler im (CFB-Betriebsmodus / ~~OFB-Betriebsmodus~~ / ~~CTR-Betriebsmodus~~) (fort / ~~nicht fort~~).

Falls ein Fehler im Geheimtext auftritt, pflanzt sich der Fehler im (~~CFB-Betriebsmodus~~ / OFB-Betriebsmodus / ~~CTR-Betriebsmodus~~) (~~fort~~ / nicht fort).

Falls ein Fehler im Geheimtext auftritt, pflanzt sich der Fehler im (~~CFB-Betriebsmodus~~ / ~~OFB-Betriebsmodus~~ / CTR-Betriebsmodus) (~~fort~~ / nicht fort).

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. Ordnen Sie den Begriffen in der linken Spalte die entsprechende Definition 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.

3. Markieren Sie die korrekten Varianten.

☐ Eine digitale Signatur hängt nur vom Autor ab, nicht von der Nachricht.

X Eine digitale Signatur muss einige unikale Informationen des Senders umfassen, um Fälschung und Leugnen vorzubeugen.

X Der Ausgang der Hashfunktion hat eine fixe Länge.

☐ Von der Nachricht kann ihr Hashwert leicht abgeleitet werden und umgekehrt.

X Es ist rechnerisch unmöglich, zwei unterschiedliche Nachrichten mit dem gleichen Hashwert zu finden.

☐ Unterschiedliche Nachrichten haben immer unterschiedliche Hashwerte.

---

4. Teilen Sie die folgenden Angriffe in der Gruppe der aktiven oder passiven Angriffe in der folgenden Tabelle auf.

Abhören, Masquerading, Verkehrsanalyse, Replay, Denial-of-Service, Modifizierung der Nachricht

Aktive	**Masquerading, Replay, Denial-of-Service, Modifizierung der Nachricht**
Passive	**Abhören, Verkehrsanalyse**

---

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

2
4

1 – Ein digitales Zertifikat beinhaltet den geheimen Schlüssel des Subjektes oder des Inhabers des Zertifikats und gleichzeitig die Identifikationsdaten des Inhabers des Zertifikats.

2 – Ein digitales Zertifikat ist mit dem privaten Schlüssel der Zertifizierungsstelle unterzeichnet.

3 – Der geheime, vom Zertifikat zertifizierte Schlüssel wird nur zum entsprechenden öffentlichen Schlüssel der Zertifizierungsstelle passen, welche das Zertifikat ausgegeben hat.

4 – Ein digitales Zertifikat verbindet den öffentlichen Schlüssel mit der Identität.

5 – Ein digitales Zertifikat beinhaltet den öffentlichen Schlüssel der entsprechenden Zertifizierungsstelle.

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.