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

Eines der Hauptprobleme ist der Prozess der Schlüsselverteilung.

zur Erzeugung der digitalen Signatur verwendet werden.

zur Erzeugung der digitalen Signatur verwendet werden.

Im ist die Struktur des Klartextes offen.

Im CBC-Betriebsmodus .

Falls ein Fehler im Geheimtext auftritt, pflanzt sich der Fehler im .

Falls ein Fehler im Geheimtext auftritt, pflanzt sich der Fehler im .

Falls ein Fehler im Geheimtext auftritt, pflanzt sich der Fehler im .

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

verwendet einen pseudozufälligen Schlüssel, der unabhängig sowohl vom Klar- als auch Geheimtext generiert wird.

**7**

**6**

**5**

**4**

**3**

**2**

**1**

Symmetrische Kryptographie

verwendet Algorithmen mit symmetrischen oder öffentlichen Schlüsseln.

Stromchiffre

Stromchiffre

bietet die Sicherstellung entweder der Vertraulichkeit oder der Authentifizierung der Quelle.

verwendet immer Algorithmen mit symmetrischen Schlüsseln.

verwendet einen pseudozufälligen Schlüssel, der vom Geheimtext nicht abhängig ist.

arbeitet mit einer zeitabhängigen Transformation der einzelnen Elemente des Klartextes.

Blockchiffre

Selbstsynchronisierende Stromchiffre

Kryptographie mit öffentlichen Schlüsseln

bietet die Sicherstellung der Vertraulichkeit und Authentifizierung der Quelle.

**5**

**4**

**7**

**2**

**6**

**3**

**1**

Synchrone Stromchiffre

1. 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.

1. 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** |

1. 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.