



Name:

Klasse:

30.03.20

AB No.:

## **Fragebogen Zertifikaten und Signaturen**

1. Wie funktioniert eine symmetrische Verschlüsselung?
2. Welchen Unterschied hat eine asymmetrische Verschlüsselung zu einer symmetrischen Verschlüsselung?
3. Stellen Sie in einer Tabelle Vor- und Nachteile der symmetrischen und asymmetrischen Verschlüsselung gegenüber.
4. Welche Aufgaben hat ein Trustcenter?
5. Was bezeichnet man als Zertifikat?
6. Erläutern Sie den grundlegenden Unterschied zwischen dem PGP Web of Trust und der Zertifikats-Hierarchie.
7. In welchem Zusammenhang stehen Signatur und Zertifikat?
8. Welche zentralen Eigenschaften muss eine digitale Signatur erfüllen?
9. Erläutern Sie das „Prinzip“ des Erstellens einer Signatur über eine Nachricht
10. Welchen Nachteil hat das Signieren einer kompletten Nachricht?
11. Wenn eine Signatur erstellt wird sie idR über einen Fingerprint der Nachricht erstellt. Was ist ein Fingerpring?
12. Erläutern Sie in einem kurzen Text wie ein Man-in-the-middle Angriff auf eine signierte Nachricht funktionieren kann.
13. Wenn ein Trustcenter (CA) einen öffentlichen Schlüssel signiert, wird dann eigentlich erstellt?