Lucerne University of
Applied Sciences and Arts
HOCHSCHULE
LUZERN
Informatik

3-Uhr Fragen Kryptographie

1. Von welchen 2 prinzipiellen Faktoren ist die Sicherheit der verschlüsselten Daten abhängig?

   .....

2. In einem Mailprogramm stossen Sie auf das Verschlüsselungsverfahren „ROT13“ (eine Variante von Julius Cäsar). Weshalb gerade 13?

   .....

3. Bei PGP kommen symmetrische und asymmetrische Verschlüsselung zum Einsatz. Beschreiben Sie in Stichworten die Rolle der symmetrischen und der asymmetrischen Verschlüsselung beim Versand einer Datei von A an B:

   .....

   .....

   .....

4. Nennen Sie typische minimale Längen für sichere a) symmetrische und b) asymmetrische Schlüssel:

   .....

5. Welches ist die Bedeutung von „Einwegfunktionen“ bei einer Public-Key Infrastruktur?

   .....

   .....

6. Unterscheiden Sie die Begriffe Authentisierung und Autorisierung:

   .....

7. Nennen Sie 3 Elemente muss ein digitales Zertifikat *mindestens* aufweisen (die Frage ist allgemeiner Natur, die Details der Zertifikatsformate (PGP oder X.509 sind hier nicht von Belang)?

   .....

   .....

8. Welches der beiden Konzepte (PGP oder X.509) braucht zwingend eine „oberste“ Zertifizierungsinstanz? .....
9. Was muss mit einem Zertifikat geschehen, wenn jemand (versehentlich oder aus anderen Gründen) seinen privaten Schlüssel preisgibt, der zum zertifizierten öffentlichen Schlüssel gehört?

   .....

10. Was ist der Unterschied zwischen einem „Trust Center“ und einer „Root-CA“?

    .....

11. Was ist eine „Zertifikats*kette*“ und wie kann sie überprüft werden?

    .....

    .....

12. Was überprüft der Browser beim Aufruf einer mit SSL geschützten Webseite *zwingend* und was nicht?

    .....