3-Uhr-Fragen zur Kryptographie

1. Von welchen zwei prinzipiellen Faktoren ist die Sicherheit der verschlüsselten Daten abhängig?
    1. Schlüsselstärke
    2. Verschlüsselungsverfahren
2. In einem Mailprogramm stossen Sie auf das Verschlüsselungsverfahren „ROT13“ (eine Variante von Julius Cäsar). Weshalb gerade 13?
    - Da unser Alphabet 26 Zeichen lang ist, kann bei „ROT13“ die gleiche Funktion für die Ver- und Entschlüsselung verwendet werden.
3. Bei PGP kommen symmetrische und asymmetrische Verschlüsselungen zum Einsatz. Beschreiben Sie in Stichworten die Rolle der symmetrischen und der asymmetrischen Verschlüsselung beim Versand einer Datei von A an B:
    - symmetrisch:
        1. A und B haben den gleichen Schlüssel K
        2. A verschlüsselt die Nachricht M mit dem Schlüssel K und enthält den Ciphertext C
        3. A schickt C an B
        4. B entschlüsselt C mit K und erhält wieder M
    - asymmetrisch:
        1. A hat den öffentlichen Schlüssel von B K_{pubB}
        2. B hat zusätzlich einen eigenen privaten Schlüssel K_{privB}
        3. A verschlüsselt die Nachricht M mit K_{pubB} und erhält C
        4. A schickt C an B
        5. B entschlüsselt C mit K_{privB} und enthält wieder M
4. Nennen Sie typische minimale Längen für sichere a) symmetrische und b) asymmetrische Schlüssel!
    a) 128 Bit (z.B. für AES)
    b) 2048 Bit (z.B. für RSA)
    - Symmetrische Schlüssel sind kürzer, weil sie nur Schutz vor Brute-Force bieten müssen, während es bei asymmetrischen Keys genügt, ihn zu faktorisieren.
5. Welches ist die Bedeutung von „Einwegfunktionen“ bei einer Public-Key-Infrastruktur?
    - Zwei grosse Primzahlen lassen sich sehr einfach multiplizieren, das Ergebnis aber nur sehr schwer faktorisieren. Die Verschlüsselung ist also um ein Vielfaches effizienter als ein unautorisierter Entschlüsselungsversuch (Brute Force).
6. Unterscheiden Sie die Begriffe Authentisierung und Autorisierung:
    - Authentisierung: Der Benutzer weist seine Identität nach.
    - Autorisierung: Der Benutzer hat aufgrund seiner Identität bestimmte Berechtigungen.
7. Welche Sie drei Elemente muss ein digitales Zertifikat *mindestens* aufweisen?
    1. Subject: Verwendungszweck der Signatur
    2. Validity: Gültigkeitszeitraum des Zertifikats (von/bis)
    3. Issuer: Herausgeber des Zertifikats
8. Welches der beiden Konzepte (PGP oder X.509) braucht zwingend eine „oberste“ Zertifizierungsinstanz?
    - X.509, da es hierarchisch aufgebaut ist. PGP verwendet ein „Network of Trust“.

9. Was muss mit einem Zertifikat geschehen, wenn jemand (versehentlich oder aus anderen Gründen) seinen privaten Schlüssel preisgibt, der zum zertifizierten öffentlichen Schlüssel gehört?
    - Das Zertifikat muss schnellstmöglich invalidiert bzw. zurückgezogen werden.
10. Was ist der Unterschied zwischen einem „Trust Center“ und einer „Root-CA“?
    - Die „Root-CA“ ist die höchste aller Hierarchiestufen, ein „Trust Center“ ist weiter unten, aber genug hoch, um selber Zertifikate ausstellen zu können.
11. Was ist eine „Zertifikatskette“ und wie kann sie überprüft werden?
    - Eine Zertifikatskette ist der Pfad von einem Zertifikat zu seinen übergeordneten Zertifikaten bis hin zum Root-Zertifikat, wobei die übergeordneten Zertifikate die untergeordneten Zertifikate als vertrauenswürdig bestätigen.
12. Was überprüft der Browser beim Aufruf einer mit SSL geschützen Webseite zwingend und was nicht?
    - Adresse: stimmt die Adresse des Webservers mit dem Zertifikat überein?
    - Vertrauenswürdigkeit: wurde es von einer vertrauenswürdigen Zertifizierungsstelle herausgegeben?
    - Gültigkeit: ist das Zertifikat (bereits/immer noch) gültig?