Aufgabe 1: Zentrale Begriffe der Kryptographie

Aufgabe 1.1: Unterschiedliche Chiffren

- Symmetrisches Kryptosystem
  - Anz. d. Schlüssel: 1
  - Verwendung für Ver- und Entschlüsselung
  - Alle involvierten Personen müssen den Schlüssel geheimhalten
- Asymmetrisches Kryptosystem
  - Anz. d. Schlüssel: 2
  - Öffentlicher Schlüssel für die Verschlüsselung
  - Privater Schlüssel für die Entschlüsselung
  - Jede Person muss nur ihren eigenen privaten Schlüssel geheimhalten

Aufgabe 1.2: Hybride Kryptosysteme

Lorem ipsum dolor sit amet, consectetur adipisicing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum.

a)

Lorem ipsum dolor sit amet, consectetur adipisicing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum.

b)

Lorem ipsum dolor sit amet, consectetur adipisicing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum.

c)

Lorem ipsum dolor sit amet, consectetur adipisicing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum.

Aufgabe 2: Parkhaus

Aufgabe 2.1: Funktionsweise

Aufgabe 2.2: Sicherheitsanalyse

Aufgabe 2.3: Umsetzung mit kryptographischen Techniken

Aufgabe 3: Authentifizierungsprotokolle

Aufgabe 3.1: Verschlüsselte Passwort-Übermittlung

Aufgabe 3.2: Authentifikationssystem auf Basis indeterministischer symmetrischer Verschlüsselung

Aufgabe 3.3: Challenge-Response-Authentifizierung

Aufgabe 3.4: Sichere Challenge-Response-Authentifizierung

Aufgabe 4: "Mensch ärgere Dich nicht"über das Telefon

Aufgabe 4.1: Protokoll

Aufgabe 4.2: Würfeln über Telefon

Aufgabe 5: RSA-Verfahren

Aufgabe 5.1: Grundlagen

Aufgabe 5.2: Anwendung

Aufgabe 5.3: Sichere Implementierung