Kryptografie:

4 Ziele:

- Vertraulichkeit
- Authentifizierung
- Integrität
- Verbindlichkeit

Symmetrische Verschlüsselung:

- Ver- und Entschlüsseln mit dem gleichen Schlüssel
- Vorteile
  - Hohe Geschwindigkeit
- Nachteile
  - Schlüssel kann abgefangen werden
  - Hohe Schlüsselanzahl (steigt quadratisch)

Asymmetrische Verschlüsselung:

- Schlüsselpaar wird generiert (Private- und Public-Key)
- Public Key muss anderen zugänglich sein
- Verschlüsselt wird mit Public Key des Empfängers
- Entschlüsselt wird mit eigenem Private Key
- Vorteile
  - Hohe Sicherheit
- Nachteile
  - Hoher Rechenaufwand

Ein Algorithmus gilt als sicher, wenn das Ausprobieren weitaus länger dauert, als die Zeit in der die zu lesende Nachricht bedeutsam ist.

RSA-Funktionsweise:

Schlüsselerzeugung:

1. Zwei Primzahlen P und Q generieren
2. Berechnung des Produktes: N = P · Q
3. Berechnung von M = Φ(N) = (P-1) · (Q-1)
4. Zahl E auswählen, wobei gelten muss:
   a. E < N
   b. E hat keinen gemeinsamen Teiler mit M
5. Wahl einer Zahl K, sodass d eine Ganzzahl wird:

$$d = \frac{k * \Phi(n) + 1}{e}$$

6. Public Key besteht aus **N** und **E**
7. Private Key besteht aus **N** und **D**

Verschlüsseln:

1. Zu verschlüsselnden Text in eine Zahl umwandeln
2. Public Key des Empfängers besorgen
3. Berechnung des Chiffre-Textes:

$$C = K^E \bmod N$$

4. Versenden des Verschlüsselten Textes

Entschlüsseln:

1. Berechnung des Klartextes:

$$K = C^D \bmod N$$

2. Zahlen wieder in Text zurückumwandeln

Handout, Präsentation und Quellen unter:
https://edu.rho2.eu/it/verschluesselung/