**Checkliste für die 2. Kursarbeit 12-2**

Kryptographie:

a) einfache Verfahren erklären und verwenden können :

- Skytala, hebr. Chiffre, Cäsar, Verschlüsseln mit Schlüsselwort, Vigenère

- Klassifizierung: Transposition / Substitution, mono/polyalphabetisch, symmetrisch/asymmetrisch

- Analyseverfahren (Häufigkeitsanalyse, Krasiski, etc), Angriffsarten

- Sicherheit nach Kerckhoffs

- CIA-Regel

b) RSA

- Anlegen eines Kryptosystems nach Vorgaben

- Errechnen der modularen Inversen d

- Ver-/Entschlüsseln einer Zahl mit RSA

- Digitale Signatur erklären können

Netzwerke:

- Begriffe klären können: LAN, WLAN, Netzwerk, WWW, Backbone, Dienst , Protokoll, Port, Router

- Adressierung in Netzwerken erklären und Netz-ID und Host-ID berechnen können

- 4 Schichtenmodell erklären können

- Dienste + Protokolle + Funktionen der Schichten kennen