**Hochschule Bonn-Rhein-Sieg**

**Prof. Dr. Martin Leischner**
**Netzwerksysteme und TK**

# **Quiz** (in Vorlesung 16.10.18)

1. „One-Time-Pad“
   a. Wie sicher ist das Verschlüsselungsverfahren „One-Time-Pad“?
   b. Für welche Anwendungsszenarien ist das „One-Time-Pad“ gut geeignet und für welche weniger? Geben Sie jeweils ein Beispiel und erläutern Sie Ihre Ausführungen.

2. Blockverschlüsselung
   a. Schreiben Sie eine typische Blockverschlüsselung als mathematische Funktion.
   *b.* Wie groß ist der maximale Schlüsselraum einer symmetrischen Blockverschlüsselung der Blocklänge 1 Byte.
   c. Lässt sich bei Verwendung des maximalen Schlüsselraums (gemäß Teil b.) eine zuverlässige Verschlüsselung erreichen?
   d. Schätzen Sie die Schlüssellänge für dieses Verfahren ab.

3. Beim CBC-Verfahren wird ein Initialvektor verwendet. Warum ist der Einsatz eines Initialvektors sinnvoll und wie ist dieser Initialvektor zu bilden?

4. Zertifikate und PKI
   a. Beschreiben Sie kurz und knapp, was ein Zertifikat ist. (Erwartet und bewertet wird eine kurze, knappe und korrekte Beantwortung.)
   b. Was versteht man unter einer PKI (Publik Key Infrastructure)? Wann wird eine PKI eingesetzt?
   c. Was sind typische Angriffspunkte einer PKI?
   d. Ist es für den Einsatz asymmetrischer Verschlüsselungsverfahren immer notwendig, eine PKI aufzubauen?

   Erläutern Sie Ihre Antworten.

5. Schlüsselaustauschverfahren
   a. Was ist das Ziel des Schlüsselaustauschverfahrens nach Diffie-Hellman? Beschreiben Sie kurz den Schlüsselaustausch nach Diffie-Hellman, ohne auf ein spezielles Verschlüsselungsverfahren (RSA, elliptic curves) einzugehen.
   b. Welche alternativen Schlüsselaustauschverfahren bieten sich im Zusammenhang der asymmetrischen Verschlüsselung noch an?

6. Hash-Funktion
   a. Was ist eine Hash-Funktion?
   b. Was versteht man unter einer stark kollisionsresistenten und was unter einer schwach kollisionsresistenten Hash-Funktion.
   c. Ihnen steht eine Blockverschlüsselung zur Verfügung. Wie können Sie daraus eine Hashfunktion konstruieren? Geben Sie ein mögliches Verfahren an.

7. Digitale Signatur
   a. Beschreiben Sie kurz, wie die digitale Signatur mithilfe asymmetrischer Verschlüsselung funktioniert.
   b. Lässt sich auch mit symmetrischer Verschlüsselung ein Signaturmechanismus konstruieren? Begründen Sie Ihre Antwort.

8. Warum werden zur Konstruktion von kryptographischen Systemen Zufallszahlen benötigt? Geben Sie ein Beispiel für den sonnvollen und notwendigen Einsatz von Zufallszahlen. Wie können auf einem Rechner Zufallszahlen erzeugt werden?