Schwerpunkte der Klausur zum Thema "Datensicherheit"

Ich empfehle, zur Vorbereitung auf die Klausur auch die Vortragsfolien des jeweils anderen Kurses zu lesen.
Klausurschwerpunkte für GK1 (Montagkurs): Themen 1-4 und 6-9
Klausurschwerpunkte für GK2 (Freitagkurs): Themen 1-7

- Thema 1: Allgemeine Einführung in die Thematik Datensicherheit
  - Klärung des Begriffes Datensicherheit und Abgrenzung vom Begriff Datenschutz
  - Risiken und Gefahren des Datenverlustes
  - Anforderungen an die Informations-, Datensicherheit (Verfügbarkeit, Integrität, Vertraulichkeit, Authentifizierung)
  - Kenntnis geeigneter Maßnahmen zum Schutz vor Datenverlust bzw. -manipulation
- Thema 2: Einführung in die Thematik Kryptografie
  - Klärung der Begriffe Kryptologie, Kryptografie, Kryptoanalyse, Klartext, Geheimtext
  - Ziele der Kryptografie
  - Kryptologie im gesellschaftlichen Kontext (Kenntnis aktueller Beispiele, Pro und Contra Kryptologie)
  - Prinzip von Kerckhoffs
- Thema 3: Symmetrische Verschlüsselungsverfahren I
  - Prinzip der symmetrischen Verschlüsselungsverfahren
  - Kenntnis der klassischen Verfahren von Cäsar und Vigenere
  - Kryptoanalyse von Cäsar durch Brute-Force-Verfahren
- Thema 4: Symmetrische Verfahren II
  - Enigma als ein Beispiel für Hardwarekryptologie
  - Enigma als symmetrisch verschlüsselnde Maschine
  - Bestandteile des Schlüssels (Auswahl der Walzen [3 aus 5 möglichen], Reihenfolge der Walzen, Anfangsstellung der Walzen, Steckerverbindungen)
- Thema 5: Symmetrische Verfahren III
  - Das TLS(SSL)-Protokoll als ein Beispiel für ein hybrides Verfahren
  - Anwendung des Protokolls (Beispiel https)
- Thema 6: Asymmetrische Verfahren I
  - Prinzip der asymmetrischen Verschlüsselungsverfahren
  - Vergleich mit den symmetrischen Verschlüsselungsverfahren (Vor- und Nachteile)
  - Verwendung von Einwegfunktionen mit Falltürfunktion (Potenzieren vs. Logarithmieren großer Zahlen)
  - eine konkrete Kenntnis des Verfahrens von Elgamal ist nicht notwendig!
- Thema 7: Asymmetrische Verfahren II
  - RSA-Verfahren als weiteres Beispiel für asymmetrischer Verfahren
  - Verwendung von Einwegfunktionen mit Falltürfunktion (Multiplikation vs. Faktorisierung großer Primzahlen)
  - eine konkrete Kenntnis des Verfahrens RSA (mathematische Grundlagen) ist nicht notwendig
- Thema 8: Nichtkryptographische Verfahren
  - Prinzip der Steganografie
  - Vergleich Kryptografie und Steganografie
  - Verstecken von Nachrichten in Bildern
- Thema 9: Verfahren zur Gewährleistung der Integrität/Authentizität
  - Verfahren der digitalen Signatur (Ziele, Beispiele, technischer Ablauf, Vorteile, Bedenken)
  - One-Way-Hashfunktionen und deren Anwendung bei der digitalen Signatur bzw. der Verschlüsselung von Passwörtern