Organisatorisches

- Literatur: Douglas Stinson: Cryptography, Theory and Practice, 3. Auflage
- Proseminar oder Seminar
- Vorträge ca. 75min einschließlich Zwischenfragen
  - Zentrale Aspekte werden ausführlich und verständlich dargestellt
  - mathematische Grundlagen müssen bereitgestellt werden
  - Folien sollen mindestens 2 Tage vorher auf die Website gestellt werden
- Gastvortrag von einem Mitarbeiter aus dem IT-Stab des BdI

Leistungsbewertung

- Qualität des Vortrags
  - Anschaulichkeit und Verständlichkeit
  - Tiefe und Gründlickeit
  - Vertrautheit mit der Thematik (kann der Vortragende auf Rückfragen antworten?)
- Qualität der schriftlichen Ausarbeitung
  - Umfang 8-10 Seiten, Abgabetermin 27.7.2009
  - korrekte und verständliche Darstellung des Themas in guter Sprachqualität
  - saubere und vollständige Quellenangaben
- aktive Teilnahme an der Diskussion

Klassische Kryptographische Verfahren

- Begriff Kryptosystem
- klassische Verfahren
- Angriffe auf klassische Verfahren

Shannons Informationstheorie

- wahrscheinlichkeitstheoretische Grundlagen
- Begriff der perfekten Sicherheit
- Entropie und Redundanz
- Produkte von Kryptosystemen

Blockverschlüsselungen

- Substitutions-Permutations-Netzwerke
- DES und AES
- Attacken auf Blockverschlüsselungen

Kryptographische Hash-Funktionen

- Werkzeug zur Sicherung der Integrität von Daten (MAC)
- Kriterien für die Sicherheit von Hash-Funktionen, Vergleich
- MerkleDamgard Konstruktion und Iterierte Hashfunktionen
- unbedingt sichere Hashfunktionen

RSA-(zwei Vorträge)

- mathematische Grundlagen und Kryptosystem
- Primzahltest: Solovay-Strassen und Miller-Rabin-Test
- Faktorisierungsalgorithmen
- Attacken und Sicherheit von RSA
- Rabin-System

Public Key Kryptographie (zwei Vorträge)

- Diskreter Logarithmus–ElGamal
- Algorithmen für diskreten Logarithmus, untere Schranken für Komplexität
- Endliche Körper
- Elliptische Kurven

Digitale Unterschriften

- Sicherheitsanforderungen
- digitale Unterschriftensysteme
- Sicherheit
- unleugbare Unterschriften

Pseudozufallszahlen

- Pseudo-Zufallsbits-Generatoren
- Ununterscheidbarkeit von Wahrscheinlichkeitsverteilungen
- Probabilistische Verschlüsselung

Identifikation und Authentifizierung

- Identifizierungsverfahren mit geheimem Schlüssel
- Identifizierung ohne geheimen Schlüssel
- Verfahren(Schnorr, Okamoto, Guillou-Quisquater) und deren Sicherheit

Schlüsselvergabe

- Sicherheit verschiedener Verfahren zum Schlüsseltausch
- Vorabverteilung von Schlüsseln
- Kurzzeit-Schlüsselvergabe mit Hilfe interaktiver Protokolle
- verschiedene Protokolle und mögliche Angriffe

Themen

1. Klassische Kryptographische Verfahren
2. Shannons Informationstheorie
3. Blockverschlüsselungen
4. Kryptographische Hash-Funktionen
5. RSA-(zwei Vorträge)
6. Public Key Kryptographie (zwei Vorträge)
7. Digitale Unterschriften
8. Pseudozufallszahlen
9. Identifikation und Authentifizierung
10. Schlüsselverteilung
11. Multicast Sicherheit und Urheberrechtsschutz