1. Grundlagen der Rechnernetze

1.1. Systeme

- **verteilt**
- **offen**
- **diensteintegriert**
- **digital**
- Rechnernetze
  > erster | zweiter Art
- Kommunikationsnetze

1.2. Schutzziele

- Was kann man schützen
- totale | partielle Korrektheit

a) Vertraulichkeit

b) Integrität

c) Verfügbarkeit & Erreichbarkeit

d) zu schützende Daten

– Technisch | inhaltlich

e) Mehrseitige Sicherheit

1.3. Angreifer

a) Angreifermodelle

- Zu beachten
- Typen
- Rechenkapazität
- Zeit-, Geldkapazitäten
- beobachtend | verändernd
- Passiv | Aktiv

– Adaptivität

b) Beispiele

- Trojanisches Pferd
- Bedienfehler

c) Angriffspunkte

d) Angriffsziele

1.4. Schutzmöglichkeiten

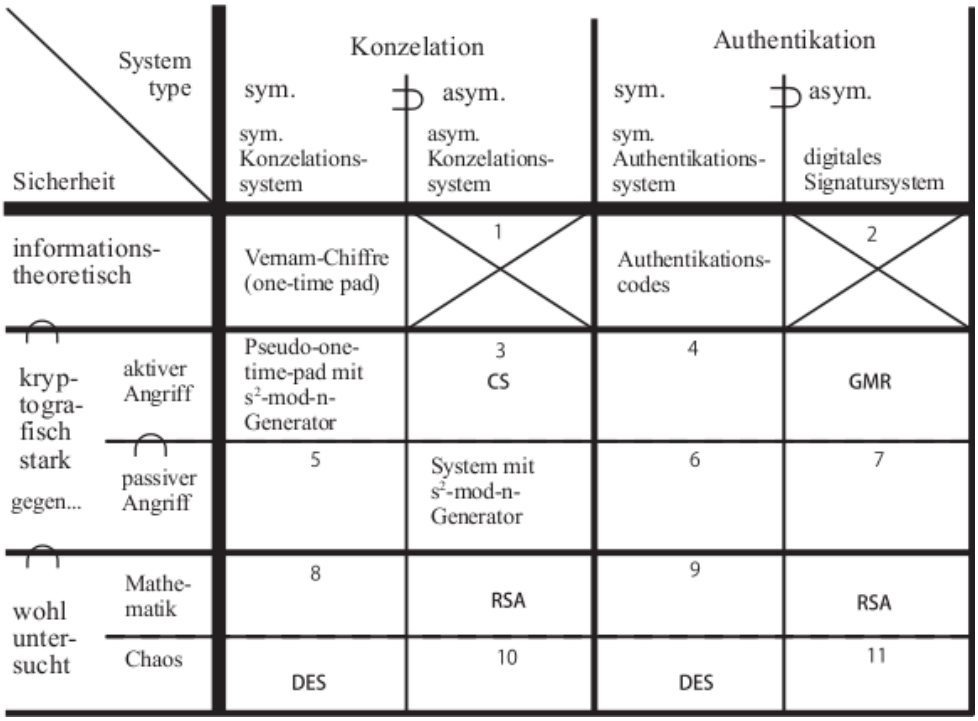
- Verbote / Gesetze
- vorbeugende technische Schutzmaßnahmen

a) physisch

- Ziel
- System
  - Schirmung, Erkennung, Bewertung, Verzögerung, Löschung
- Probleme

b) logisch

- Identifikation
- Zugangskontrolle
- Zugriffskontrolle
- Organisation
- Kryptografie
- Probleme



2. Kryptologie

- **Kryptografie**
- **Kryptoanalyse**
  - Möglichkeiten
  - zu beachten

2.1. Zweck und nötige Schlüsselverteilung

a) Konzelationssysteme

- System, Allgemeine Schutzmechanismen
- symmetrisch
  - System
  - Vertreter
- asymmetrisch
  - System
  - Vertreter

b) Authentifikationssysteme

- Ziel
- symmetrisch
  - System
  - Vertreter
- asymmetrisch

- System
  - Zertifizierungsinstanz CA
- Probleme
- Geheimhaltung des geheimen Schlüssels
- Vertreter

c) hybride kryptografische Systeme

2.2. Sicherheitsgrad

- Kerckhoffs'sches Prinzip

a) informationstheoretisch (absolut) sicher

- Bedingungen bei Konzelationssystemen
- Bedingungen bei Authentifikationssystemen

b) kryptografisch / komplexitätstheoretisch sicher

- kryptografisch stark
  - Schwierigkeit von Schlüsselgenerierung, Brechen
- wohluntersucht

3. Funktionen / Substitutionen und deren Analyse

3.1. Bewertungskriterien

- Grad der Vollständigkeit
- (striktes) Avalanche-Kriterium
- Nichtlinearität (partiell linear)
- Korrelationsimmunität
- Chaos

3.2. MM-Substitution (Tauschchiffre)

- System
- Kryptoanalyse

3.3. PM-Substitution (Vigenere-Chiffre)

- System
- Kryptoanalyse
  - Kasiski-Test
  - Friedmann-Test (Koinzidenzindex)

a) Matrixtransposition

- System
- Kryptoanalyse
- aktiver Angriff

4. Klassifikation von Chiffren

4.1. Blockchiffre | Stromchiffre

- Zugeordnete Systeme
- synchron | selbstsynchronisierend
- Wahlfreiheit des Zugriffs
- symmetrisch | asymmetrisch → asymmetrisch
- deterministisch | indeterministisch
- Eingabelänge
- Vorausberechenbarkeit
- asymmetrisch → asymmetrisch

4.2. Betriebsarten

a) selbstsynchronisierend

- **ECB** (electronic codebook)
- **CBC** (cipher block chaining)
- **CFB** (cipher feedback)

b) synchron

- **OFB** (output feedback)
- **PCBC** (plain cipher block chaining)
- **OCFB** (output cipher feedback)

c) Kollisionsresistente Hashfunktion aus Blockchiffre

5. Kryptografische Systeme

5.1. Feistel-Chiffre (Beispiel DES)

- System (Schlüsselerzeugung, Verschlüsselung, Entschlüsselung)
- Komplementaritätseigenschaft
- Angriffe
- Sicherheitsgrad

5.2. Vernam-Chiffre

- System
- aktiver Angriff

5.3. Authentikationscodes

5.4. RSA als Konzelationssystem

- System (naiv)
- Angriffe (aktiv, passiv)
- Verbesserung
- Implementierungshilfen
- Sicherheitsgrad

5.5. RSA als Authentikationssystem

- Naives System
- Angriffe
- Verbesserung
- Sicherheitsgrad

5.6. GMR

- Einordnung
- System
  - kollisionsresistente Permutationenpaare mit Geheimnis
  - DAMGARD-Hashfunktion (+ Negation)
- Angriff → Lösung
- Authentisierung vieler Referenzen

5.7. Weitere Systeme

a) Diffie-Hellman Schlüsselaustausch

- System
- Sicherheit
- Angriff

b) unbedingte Sicherheit für den Unterzeichner

c) Undeniable Signatures

d) Blind Signatures

e) Schwellwertschema

5.8. Zero-Knowledge-Verfahren

- Commitment-Verfahren
- interaktive Beweissysteme
  - Sicherheit (Eigenschaften)
  - System
  - Beispiele
    - Beispielsysteme
    - Beweissystem für den diskreten Logarithmus:
      - System
      - Simulationsmöglichkeit
    - nicht interaktives Beweissystem
      - System
      - Verwendung
  - Kompositionsmöglichkeit
- Angriff, Lösung

6. Steganografie

- Konzelation
- Authentikation
- System
  - EInbettung
    - LSB-Methode
    - Paritäts-Methode
    - Inkrementieren
  - Effizienz
    - Einbettungskapazität
    - Einbettungsrate
    - Schwundrate
    - Änderungsrate
- Angriffe
  - ABER jeder Angriff führt zur Verbesserung des Stegosystems

7. Kommunikationsnetze

7.1. Einsatz von Verschlüsselungen

a) Verbindungs-Verschlüsselung

- Wer
- Wie
- Nachteile

b) Ende-zu-Ende-Verschlüsselung

- Wer
- Nachteile

7.2. Schutzmaßnahmen

a) technische Sicht

b) Verteilung

- Sicherheit (Angriff)
- Adressierung
  - öffentlich | privat
  - implizit | explizit
  - offen | verdeckt
- Fehlertoleranz

c) Abfragen und Überlagern

- Ziel
- System

d) dummy traffic

- Ziel
- System

e) digitale Signalregenerierung

- Ziel
- System

7.3. Physische Netzarten

a) RING-Netz

- System
- Fehlertoleranz

b) BAUM-Netz

- System
- Vorteile

7.4. DC-Netz

a) Funktionsweise

- verallgemeinertes überlagerndes Senden
- überlagerndes Empfangen
- Kollisionsauflösung
- Reservierungsschema

b) Sicherheit

c) Optimierung

- Ziele
- Optimierung der Schlüssellänge
- RING-Netz
- BAUM-Netz

d) Fehlertoleranz

- Fehlervermeidungssysteme
- Fehlererkennung und -lokalisierung
  - Knack-Schnapp-Verteilung
    - System
    - Sicherheit
    - deterministisch
    - probabilistisch
  - lineares Prüfzeichen
  - Fehlerlokalisierungs und -behebungs – Protokoll

7.5. MIX-Netz

a) Funktionsweise

- Mixreihenfolge
- Schlüsselverteilung
- **Pufferung**
  - Batchmodus | Poolmodus
  - wichtigste Sicherheitsbedingung
- **Umcodierung**
  - direktes Umcodierungsschema zum Schutz der Senderanonymität
  - indirektes Umcodierungsschema zum Schutz der Empfängeranonymität
  - indirektes längengetreues Umcodierungsschema

- **Umsortierung**

b) Optimierung

- Verschlüsselungstechnik
- Kanalaufbau
- Sendung von Inhaltsdaten
- MIX-Kanal

c) Sicherheit

- maximale Sicherheit
- Ziele → Realisation
- Angriff
  - aktiv
  - passiv

d) Fehlertoleranz

- Wahrnehmung
- transiente Fehler
- permanente Fehler:
  - zwei-Phasen-Konzept
  - Austausch von Mixen
  - Auslassen von Mixen

7.6. Angriffe

- verändernd
- aktiv

7.7. Einordnung ins Schichtenmodell

- RING, BAUM, Verteilung, Mehrfachzugriffsverfahren, Ende-zu-Ende-Verschlüsselung, Verbindungs-Verschlüsselung, DC-Übertragung und -Überlagerung, MIX-Pufferung und -Umcodierung, digitale Signalregenerierung, Verteilung über Kanalselektion, Generierung und Auswertung von impliziten Adressen

8. Zufallszahlenerzeugung

8.1. Allgemeines

- Gute | schlechte Erzeugung
- Zufallszahlenkombination (XOR)

8.2. Pseudozufallsbitfolgengenerator (PBG)

a) Grundlagen

- Sicherheitsparameter
- weitere Grundsicherheiten

b) Anforderungen

- Sicherheit

c) Verwendung

- Pseudo-one-time-pad (Vigenere-Chiffre)
- s^2-mod-n-Generator:
  - System
  - Sicherheit
  - asymmetrisch (= BIG-System):
    - System
    - Sicherheit (aktiver Angriff)

d) Primzahlenerzeugung

- Primzahlsatz
- Erzeugung → RABIN MILLER-Test

9. Rechnen mod n

- Teilbarkeit, Kongruenz, mod-Operator, div-Operator
- Additives Inverse | Multiplikatives Inverse
- abelsche Gruppe
- Kürzungsregel
- $a_{0,} a_{1,} \ldots, a_{n-1}$
- $\mathbb{Z}_n$
- Generator in multiplikativer Gruppe G
- zyklische Gruppe
- diskreter Logarithmus
- $\mathbb{Z}_n^*$

- Eulersche ϕ - Funktion
- Satz von Euler | kleiner Satz von Fermat
- SMA
- Chinesischer Restsatz | CRA
- Quadrate & Wurzeln
- quadratische Reste
  - in $\mathbb{Z}_p$:
    - Anzahl der quadratischen Reste
    - Legendre-Symbol
    - Euler-Kriterium
  - in $\mathbb{Z}_n$:
    - Jakobi-Symbol
    - Bestimmen der wesentlich verschiedenen Wurzeln
    - Faktorisierung durch wesentlich verschiedene Wurzeln
- BLUM-Zahlen

10. Komplexitätstheorie

- Probleme in P
- Probleme in NP
- NP-vollständiges Problem
- Addition, Subtraktion, Multiplikation, Exponentation

11. OSI/ISO Schichtenmodell

- Schicht 0-4

°)° → '}'