Durchgang durch die Themen der Kryptologie-Vorlesung („Was kann in der Klausur dran-kommen?")

- Begriffserklärungen: Kerckhoff-Prinzip, Arten von Angriffen (ciphertext only, etc.), Unterschied klassische/moderne Krypto, Sicherheitsniveau
- Historische Chiffren, z.B. Cäsar, affin, allgemein monoalphabetisch, homophon (schon ~~homopha~~), Vigenère (polyalphabetisch) und die Möglichkeiten, diese zu brechen (Kasiski, Friedman), Autokey
- Definition von Entropie bzw. Koinzidenzindex (+ Renyi-Entropie) bei gegebener W'Verteilung, Schätzung des IC-Werts aus gegebenem Text.
- Funktionsweise von rückgekoppeltem Schieberegister, linearer Kongruenzgenerator, quadratischer wie bei Pollard-ρ, bzw. bei Blum-Blum-Shub, Pseudozufallsgenerator
- absolute Sicherheit: Kryptosystem als stochast. Modell

- Begriff: Unizitätsmaß
- Feistel-Netzwerk (DES): grundsätzlicher Aufbau
- Begriffe aus Komplexitätstheorie: worst-case, average-case, Konzept Einwegfunktion, P, NP, O-Notation, Orakel-Reduzierbarkeit, $\leq_{eff}$, NP-vollständig, Fehlerrate bei probab. Algorithmus reduzieren, Komplexität elementarer Algorithmen
- Einwegfunktion, ggf. mit Falltür, homomorph
- Grundlagen der (algorithmischen) Zahlentheorie: Restklassen, (reduziertes) Restsystem, ggT mittels Euklid, Bezout, erweitert Euklid, inverse Elemente in $\mathbb{Z}_n^*$,
- zyklische Gruppen, erzeugendes Element, Wann ist $\mathbb{Z}_n^*$ zyklisch? Primitivwurzelkriterium, Initialisieren eines Diskret. Log-basierten Systems mit n (Primzahl) und a (Prim. Wurzel). → sichere Primzahl

Definition und Berechnung von $\varphi(n)$;

Anzahl der Erzeuger bei zyklischer Gruppe.

Untergruppe, Satz von Lagrange

Satz von Euler, „kleiner Fermat": $a^{n-1} \equiv 1 \pmod n$

Rechnen auf der „Grundlinie" versus Rechnung mit den Exponenten: $a^x \equiv a^y \pmod n \iff x \equiv y \pmod{\varphi(n)}$

Pohlig-Hellman-Chiffrierung: sowohl als klassisches System bzw. Anwendung bei Shamirs No-key-Protokoll.

Diffie-Hellman-Schlüsselvereinbarung, Diffie-Hellman-Problem

Quadratische (Nicht-) Reste, Chinesischer Restsatz,
Profil von a modulo n (regulières/irrégulières), Miller-Rabin-Primzahltest (Carmichael-Zahl),
Berechnen der Quadratwurzel, speziell wenn $n \equiv 3 \pmod 4$
modulare Exponentiation (square + multiply)

RSA-System, Konzept eines Public-Key-Systems:
$E(k, m)$, $D(k', c)$, geheimer/öff. Schlüssel

Legendre-Symbol, Euler-Kriterium, Jacobi-Symbol,
quadr. Reziprozitätssatz, Algorithmus für Jac. Symbol,
Primzahltest v. Solovay-Strassen, Quadr. Rest-Problem
„Blob"

Rabin-System, Faktorisieren $\equiv_{eff}$ Quadratwurzel berechnen (mit Chin. Restsatz)

El Gamal-Public Key System als Erweiterung von Diffie-Hellman

- Konzept: Elektr. Unterschrift, speziell bei RSA-System; speziell bei El Gamal.
- Blinde Unterschrift mittels RSA-System

Konzept: kryptogr. sichere Hashfunktion

Geburtstagsproblem, Geburtstagsangriff gegen eine Hashfunktion

Möglichkeiten des Verschlüsselns „mit Commitment"

- Faktorisierungsalgorithmen: Pollard-ρ (Cycle-Detection), $(p-1)$-Algorithmus, Fermat-Algorithmus, Quadr. Sieb
- Algorithmen für Diskret-Log: Baby-Step-Giant-Step, Cycle Detection Pollard-ρ
- Konzept: Zero Knowledge-Protokoll, allgemein mit Einwegfunktion, die homomorph ist (Bsp: mod. Exponentiation und Quadrieren, Fiat-Shamir)

Zero Knowledge mittels Graph Isomorphie

Definition von Zero-Knowledge: effizienter Simulator

Schnorr Identifikations Protokoll,

Zero Knowledge für 3-COLOR.

- Aufteilen von Geheimnis, Schwellenwertsystem mit Polynom

  Spezialfall: $n=k=2$ (Visuelle Krypto.)

- Konzept von Ellipt. Kurve (Def. von $E_{a,b}$)

  als Verallgemeinerung von Diskr. log - Protokollen

  Wie definiert man PoQ (graphisch)

  Gruppenstruktur durch Erweiterung mit $\mathcal{O}$