Vorlesung „Kryptographie II“ (Sommersemester 2025)

Fragen zur Prüfungsvorbereitung

(1) Quadrate und Quadratwurzeln modulo n
  (a) Legendre-Symbol
    (i) Definition und grundlegende Eigenschaften.
    (ii) Schnelle Berechnung des Legendre-Symbols mit dem Satz von Euler.
    (iii) Das quadratische Reziprozitätsgesetz (mit den Formeln für $\left(\frac{-1}{p}\right)$ und $\left(\frac{2}{p}\right)$).
    (iv) Wie findet man eine Quadratwurzel von -1 modulo p?
  (b) Der Zwei-Quadrate-Satz von Fermat
  (c) Jacobi-Symbol
    (i) Definition und grundlegende Eigenschaften.
    (ii) Das quadratische Reziprozitätsgesetz (mit den Formeln für $\left(\frac{-1}{n}\right)$ und $\left(\frac{2}{n}\right)$).
    (iii) Wie kann man das Jacobi-Symbol schnell berechnen?
  (d) Primzahltests
    (i) Fermat-Test und Miller-Rabin-Test.
    (ii) Solovay-Strassen-Test.
    (iii) Wie verhält sich der Solovay-Strassen-Test zum Fermat-Test und zum Miller-Rabin-Test?
  (e) Quadratwurzeln modulo p
    (i) Wie kann man schnell testen, ob eine Zahl $a \in \mathbb{Z}$ ein Quadrat modulo einer Primzahl p ist?
    (ii) Beschreibung eines Verfahrens zum Wurzelziehen modulo p.
    (iii) Formel zum Wurzelziehen modulo einer Primzahl $p \equiv 3 \bmod 4$ (mit Beweis).
  (f) Quadratwurzeln modulo einer RSA-Zahl $N = pq$
    (i) Wann ist eine Zahl $a \in \mathbb{Z}$ ein Quadrat modulo einer RSA-Zahl $N = pq$? (Welche Rolle spielt hier das Jacobi-Symbol $\left(\frac{a}{N}\right)$?)
    (ii) Wie kann man Quadratwurzeln modulo einer RSA-Zahl $N = pq$ berechnen? Was braucht man dazu?
    (iii) Wie kann man eine RSA-Zahl N faktorisieren, wenn man Quadratwurzeln modulo N berechnen kann?
  (g) Kryptographische Anwendungen. Worauf beruht die Sicherheit?
    (i) Rabin-Verschlüsselung. Vergleich mit RSA. Ein Angriff mit dem chinesischen Restsatz.
    (ii) Wie kann man die Entschlüsselung bei der Rabin-Verschlüsselung eindeutig machen?
    (iii) Goldwasser-Micali-Verschlüsselung.
    (iv) Fiat-Shamir-Identifikationsprotokoll.
    (v) Blum-Goldwasser-Verschlüsselung.

(2) Lucas-Folgen ($U_i(P,Q)$ und $V_i(P,Q)$)
  (a) Definition, ein paar grundlegende Formeln, Beschreibung mit Hilfe der Wurzeln von $x^2 - Px + Q$.
  (b) Eine (schnelle) Berechnungsmöglichkeit für $U_i(P,Q) \bmod n$ und $V_i(P,Q) \bmod n$.
  (c) Was ist $U_{p-\left(\frac{D}{p}\right)}(P,Q) \bmod p$ (mit $D = P^2 - 4Q$)?
  (d) Beschreibung des Lucas-Primzahltests zum Parameterpaar (P,Q). Was ist eine Lucas-Pseudoprimzahl?
  (e) Eine kurze Erläuterung des Baillie-PSW-Primzahltests.
  (f) Wie kann man beweisen, dass eine ungerade Zahl $n \geq 3$ eine Primzahl ist, wenn man die Primfaktorzerlegung von $n-1$ oder $n+1$ kennt.
  (g) Der Lucas-Lehmer-Test für Mersenne-Zahlen.
  (h) Kryptographische Anwendungen. Worauf beruht die Sicherheit?
    (i) Lucas-RSA-Verschlüsselung. Wie funktioniert dies? Vergleich mit RSA.

Datei: kii_prf. Version vom 31.7.2025

(ii) Ein Angriff auf Lucas-RSA mit dem chinesischem Restsatz.
(i) Zeckendorf-Zerlegung.
(j) Chebyshev-Polynome und Lucas-Folgen.

(3) Elliptische Kurven
(a) Wie definiert man eine elliptische Kurve in Weierstraß-Normalform über einem Körper K der Charakteristik $\neq 2, 3$?
(b) Was sind K-rationale Punkte von E? Was ist $E(K)$? Was ist O?
(c) Wie definiert man eine Addition auf $E(K)$? (Was ist die dahinterstehende geometrische Idee? Wie erhält man daraus algebraische Formeln? Skizzen) Wozu braucht man O? Was ist das neutrale Element? Wie sieht das Inverse eines Punkt $P \in E(K)$ aus?
(d) Wie ist für $n \in \mathbb{N}$ und $P \in E(K)$ der Punkt $n \cdot P \in E(K)$ definiert? Wie kann man $n \cdot P$ schnell berechnen?
(e) Für welche Punkte $P \in E(K)$ gilt $2 \cdot P = O$?
(f) Wie testet man für eine über $\mathbb{F}_p$ definierte elliptische Kurve E, ob es zu $x \in \mathbb{F}_p$ einen Punkt mit x-Koordinate x gibt, d.h. $P = (x, \dots) \in E(\mathbb{F}_p)$? Wie findet man gegebenenfalls $y \in \mathbb{F}_p$ mit $P = (x, y) \in E(\mathbb{F}_p)$?
(g) Wie kann man die Anzahl $|E(\mathbb{F}_p)|$ mit einer Formel bestimmen?
(h) Was kann man über $|E(\mathbb{F}_p)|$ sagen? (Satz von Hasse)
(i) Punktkompression: Berechnung von $P = (x, y) \in E(\mathbb{F}_p)$ aus $(x, y \bmod 2)$.
(j) Wie funktioniert der Diffie-Hellman-Schlüsselaustausch mit elliptischen Kurven? Wovon hängt die Sicherheit ab?
(k) Wie funktioniert die ElGamal-Verschlüsselung mit elliptischen Kurven? Wovon hängt die Sicherheit ab?
(l) Wie funktioniert ECDSA? Schlüssel, Signieren, Verifizieren, Beweis für die Richtigkeit.
(m) Wie kann man diskrete Logarithmen in $E(\mathbb{F}_p)$ berechnen, wenn in der Primfaktorzerlegung von $|E(\mathbb{F}_p)|$ nur lauter kleine Primzahlpotenzen vorkommen?
(n) ECM - Faktorisieren mit elliptischen Kurven. Was sind die Grundideen?
(o) Wie kann man $|E(\mathbb{F}_p)|$ für Kurven $y^2 = x^3 + ax$ bestimmen?
(p) Wann sind elliptische Kurven über einem Körper K isomorph?
(q) Was ist die j-Invariante einer elliptischen Kurve? Was hat die j-Invariante mit Isomorphie zu tun?
(r) Wie sehen die elliptischen Kurven mit j-Invariante 0 und 1728 aus?
(s) Was ist ein Gitter Λ in $\mathbb{C}$?
(t) Was ist der Endomorphismenring eines Gitters? Wie sieht er aus?
(u) Beschreibung elliptischer Kurven über $\mathbb{C}$ durch Gitter $\Lambda \subseteq \mathbb{C}$.