Kryptologie, Sommersemester 2003

Zusammenfassung des Vorlesungsstoffs

Gruppen
Untergruppe, Normalteiler, Nebenklassen, Quotientengruppe
Ordnung einer Gruppe, einer Untergruppe, eines Elements
Satz von Lagrange: $|G| = |U||G/U|$
Beispiele: Permutationsgruppen, $(\mathbb{Z}_n, +), (\mathbb{Z}_n^*, \cdot), (\mathbb{Z}_p^*, \cdot)$

Ringe und Körper
Polynomringe $R[X], K[X]$
Primzahlen, irreduzible Polynome
Euklidischer Algorithmus, Erweiterter Euklidischer Algorithmus
Berechnung multiplikativ Inverser in $\mathbb{Z}_n, \mathbb{Z}_p, K[X]/(f)$
Chinesischer Restesatz: $ggT(m,n) = 1 \quad \Rightarrow \quad \mathbb{Z}_{mn} \cong \mathbb{Z}_m \times \mathbb{Z}_n$; Berechnung der kanonischen Bijektion $\mathbb{Z}_m \times \mathbb{Z}_n \to \mathbb{Z}_{mn}$.
Das RSA-System: Public Key Verschlüsselung und Digitale Signatur

Wurzelziehen in $\mathbb{Z}_n$, quadratische Reste, Legendre- und Jacobi-Symbol, Quadratisches Reziprozitätsgesetz
Primzahltests nach Fermat und Rabin-Miller; Carmichael Zahlen
Starker Zufallsgenerator nach Blum-Blum-Shub

Diskretes Logarithmus Problem
Diffie-Hellman Schlüsseltausch

Elliptische Kurven, Gruppenstruktur, Additionsformel

Lineare Schieberegisterfolgen
Matrixdarstellung linearer Schieberegisterfolgen und deren charakteristisches Polynom.
Maximale Länge linearer Schieberegisterfolgen und primitive char. Polynome
Nicht-lineare Überlagerung linearer Schieberegisterfolgen und Anwendung für Stromchiffren

Blockchiffren und DES

———————

Kryptographische Protokolle
Faktorisierungsmethoden
Methoden zur Berechnung diskreter Logarithmen