

I. TEIL: GRUNDLAGEN ZUR KRYPTOGRAPHIE

1. *Grundlegendes zur Kryptographie*

Die grundlegenden Aufgabenstellungen sollen besprochen und einfache Verschlüsselungstechniken (Cäsar, Blockchiffrierung) erläutert werden. Grundidee der Public-Key-Kryptographie und digitalen Signatur.

([R], Kap. 1; [W], Kap. 1)

2. *Elementare zahlentheoretische Algorithmen und deren Komplexität*

Schnelle zahlentheoretische Algorithmen (euklidischer Algorithmus, ggT, Potenzieren, (wahrscheinliche) Primzahlen finden). Langsame Algorithmen (Primfaktorzerlegung, diskreter Log). RSA-Verschlüsselung

([R], 1.3-4)

3. *Verschlüsselungsmethoden und Angriffe*

Diffie-Hellmann-Verfahren und RSA-Verfahren (Absprache mit vorhergehendem Vortrag). ElGamal-Verschlüsselung und ElGamal-Signatur, DSA.

Algorithmen für das diskrete Log-Problem: naiv, baby-step-giant-step, Index-Calculus. Pollard-Methoden.

([R], Kap. 6; [W], 4.1)

II. TEIL: GRUNDLEGENDES ZU ELLIPTISCHEN KURVEN

4. *Affine und projektive Kurven*

Der affine Raum $\mathbb{A}^n(k)$ und der projektive Raum $\mathbb{P}^n(k)$ für einen Körper k . Varietäten als Nullstellengebilde von (homogenen) Polynomen. Zerlegung von $\mathbb{P}^n(k)$ in unendliche ferne Hyperebene und $\mathbb{A}^n(k)$. Der spezielle Fall $n = 2$ und einem Polynom (also von ebenen Kurven). Singuläre Punkte.

([R], Kap. 2, [W], Kap. 2, [K] I.§1 und II. §1-3)

5. *Elliptische Kurven, I*

Definition. Weierstraß-Gleichung. Normalform der Weierstraß-Gleichung. Diskriminante. Gruppenstruktur auf $E(k)$.

([R], Kap.2, [W], Kap.2; [S]; Absprache mit vorheriger Vortragender)

6. *Elliptische Kurven über \mathbb{C}*

Gitter und doppelt-periodische meromorphe Funktionen. Elliptische Kurven über \mathbb{C} .

([S]; [R], 9.1)

7. *Die j -Invariante und Isomorphietyp*

Definition der j -Invariante. Beweis, dass diese den Isomorphietyp über dem algebraischen Abschluss von k festlegt. Isomorphieklassen für nicht algebraisch abgeschlossenes k .

([R], Kap. 4; [S], Kap. 1)

8. *Der Endomorphismenring*

Bestimmung des Endomorphismenrings. Komplexe Multiplikation und supersinguläre ell. Kurven.

([R], 9.3; [S])

9. *Punkte auf elliptischen Kurven über \mathbb{F}_q*

Das Legendre-Symbol. Quadratisches Reziprozitätsgesetz. Formel für Anzahl der Punkte von $E(\mathbb{F}_q)$. Satz von Hasse zitieren (ohne Beweis).

([R], Kap. 5.1-3)

10. *Der Frobenius-Endomorphismus*

Betrachten des Frobenius-Endomorphismus für eine ell. Kurve über \mathbb{F}_q . Tate-Modul und Frobeniuseigenwerte. Spezielle Aussagen für supersinguläre ell. Kurven ([R], Kapitel 9 ab 9.3, [W] 3.2 und 3.4)

II. TEIL: KRYPTOSYSTEME MIT ELLIPTISCHEN KURVEN

11. *Verschlüsselungsverfahren mit elliptischen Kurven, I*

Praktische Implementation von Verschlüsselungen mit elliptischen Kurven: Algorithmus zum Bestimmen eines Punktes. Einbetten von Text in ell. Kurve, Hash-Funktionen und Verschlüsselungsverfahren PSEC-1, elliptisches ElGamal-Verfahren, ECDSA (ell. curve digital signature).

([R], 5.4 und Kap. 7 und 8 (Auswahl treffen!))

12. *Verschlüsselungsverfahren mit elliptischen Kurven, II*

wie obiger Vortrag. Aufteilung nach Absprache.

13. *Berechnung von $\#E(\mathbb{F}_q)$*

Allgemeine Algorithmen. Algorithmus nach Schoof.

([R] Kap. 10, [W] 3.3)

14. *Weil-Paarung und das MOV-Verfahren*

Definition und grundlegendes zur Weil-Paarung. Das MOV-Verfahren zur effektiven Berechnung des diskreten Log auf supersingulären ell. Kurven.

([R] 11.1, [W] 4.2.1)

15. *Anomale Kurven und der SSSA-Algorithmus*

Für anomale ell. Kurven über \mathbb{F}_q hat man den SSSA-Algorithmus für den diskreten Log, diese sind also ungeeignet.

([R] 11.2, [W] 4.2.2)

[K] E. Kunz, *Einführung in die algebraische Geometrie*, vieweg-Verlag, 1997

[R] W. Ruppert, *Elliptische Kurven und Kryptographie*, Skript einer Vorlesung im Sommersemester 2003 an der Universität Erlangen, kann unter <http://www.mi.uni-erlangen.de/~ruppert/skripten/ekk.ps.gz> als gzipped-Postscript heruntergeladen werden.

[S] J. Silverman, *The arithmetic of elliptic curves*, Springer-Verlag 1986, Gard. Texts in Math. 106.

[W] A. Werner, *Elliptische Kurven in der Kryptographie*, Springer 2002