

WOLFGANGSEILER
NPEOXFAAQEREPJCH
MKCTVFNJWBOSRI
XQLOIMJGCVJAYBQ
ZQEOWYSQLSAAYBQ
LIQVHSQJRIUJODL
NEZCLXANNAPQGCK
KKPAAYBBVPQGT
HTEQKNULES
DPDQMIQSJGNXEOG
JZTYAHVHI
OFFZXNDZII
JBJMYBZJBDLZSCX
SFINYE
JFH
CIXGFAIMCHUYL

VORLESUNGANDE
NIVERSITÄT
HEIMHERBSTSEM
ESTER 2010/2011

Dieses Skriptum entstand parallel zur Vorlesung und kurz danach mit dem Ziel, daß es mit möglichst geringer Verzögerung verfügbar sein soll. Es ist in seiner Qualität auf keinen Fall mit einem Lehrbuch zu vergleichen; insbesondere sind Fehler bei dieser Entstehungsweise nicht nur möglich, sondern **sicher**. Dabei handelt es sich garantiert nicht immer nur um harmlose Tippfehler, sondern auch um Fehler bei den mathematischen Aussagen.

Das Skriptum sollte daher mit Sorgfalt und einem gewissen Mißtrauen gegen seinen Inhalt gelesen werden; falls Sie Fehler finden, teilen Sie mir dies bitte persönlich oder per e-mail (seiler@math.uni-mannheim.de) mit. Auch wenn Sie Teile des Skriptums unverständlich finden, bin ich, auch im Hinblick auf hoffentlich existierende künftige Kryptologie-Vorlesungen, für entsprechende Hinweise dankbar.

Biographische Angaben von Mathematikern beruhen größtenteils auf den entsprechenden Artikeln im *MacTutor History of Mathematics archive* (www-history.mcs.st-andrews.ac.uk/history/), von wo auch die meisten abgedruckten Bilder stammen. Bei noch lebenden Mathematikern bezog ich mich, soweit möglich, auf deren eigenen Internetauftritt.

§2: Polyalphabetische Substitutionen	54
§3: Der one time pad	64
§4: Transpositionschiffren	68
§5: Rotormaschinen	72
§6: Literaturhinweise	77

Inhalt

KAPITEL I: AUFGABEN UND UMFELD DER KRYPTOLOGIE	1
§1: Einsatzgebiete der Kryptographie	1
a) Geheimhaltung	2
b) Verfälschungssicherheit	3
c) Sicherheit gegen erneutes Einspielen	3
d) Authentizität	4
e) Beweisbarkeit	4
f) Urheberrechtsschutz	5
g) Kopierschutz	6
h) Dokumentation des Wissensstands	6
i) Rechnen mit verschlüsselten Daten	6
§2: Alternativen zur Kryptographie	7
§3: Das Umfeld der Kryptologie	12
§4: Forderungen an ein Kryptosystem	15
a) Was weiß der Gegner über die Nachricht?	15
b) Was weiß der Gegner über das Kryptoverfahren?	17
c) Was kann der Gegner?	19
§5: Literaturhinweise	24
KAPITEL II: EINIGE KLASSISCHE KRYPTOVERFAHREN	27
§1: Monoalphabetische Substitutionen	27
a) Die Nullchiffre	27
b) Die CAESAR-Chiffre	28
c) Allgemeine monoalphabetische Substitutionen	31

KAPITEL III: KLASSISCHE BLOCKCHIFFREN	79
§1: Anforderungen an eine Blockchiffre	81
§2: Der Aufbau einer Blockchiffre	85
§3: Der Data Encryption Standard DES	88
§4: Designkriterien und Kryptanalyse des DES	95
a) Geschichtliche Entwicklung	95
b) Designkriterien	96
c) Differentielle Kryptanalyse	98
d) Lineare Kryptanalyse	105
e) DES-Cracker	106
§4: Modifikationen	109
a) Mehrfacher DES	109
b) Doppelter DES	110
c) Dreifacher DES	111
d) DESX	112
e) Alternativen zu DES	113
§5: Operationsmodi	113
a) Electronic Code Book (ECB)	113
b) Cipher Block Chaining (CBC)	115
c) Cipher Feedback (CFB)	118
d) Output feedback (OFB)	120
e) Counter mode (CTR)	121
§6: Literatur	122

KAPITEL IV: DAS RSA-VERFAHREN	123
§1: New directions in cryptography	123
§2: Die Grundidee des RSA-Verfahrens	126
a) Allgemeine Vorüberlegungen	126
b) Modulararithmetik	129
c) Potenzfunktionen modulo einer Primzahl	131
d) Der erweiterte EUKLIDISCHE Algorithmus	134
e) Die RSA-Verschlüsselungsfunktion	139
§3: Praktische Anwendung von RSA	142
a) Wie groß sollten die Primzahlen sein?	142
b) Wie werden Nachrichten zu Zahlen?	145
c) Probabilistische Verschlüsselung	149
d) Wie berechnet man die RSA-Funktion effizient?	150
e) Konkrete Implementierungen	152
1.) Maple	153
2.) Maxima	153
3.) Scheme/Racket	154
4.) Java	155
5.) C, C++, . . .	156
§4: Was läßt sich mit RSA anfangen?	157
a) Identitätsnachweis	158
b) Elektronische Unterschriften	160
c) Bankkarten mit Chip	161
d) Elektronisches Bargeld	163
§5: Wie findet man Primzahlen für RSA?	165
a) Wie man es nicht machen sollte	166
b) Wie man es idealerweise machen sollte	167
c) Wie dicht liegen die Primzahlen?	169
d) Das Sieb des Eratosthenes	171
e) Der Fermat-Test	172
§6: Sicherheit und Sparsamkeit	176
a) Primzahlen sind Wegwertartikel	176

b) Jeder braucht seinen eigenen RSA-Modul	177
c) Der chinesische Restesatz	179
d) Kleine öffentliche Exponenten und Kettenbriefe	181
e) Kleine private Exponenten	182
§7: RSA im wirklichen Leben	184
a) Allgemeine Struktur einer public key infrastructure	185
1.) Hierarchische Modelle	185
2.) Grassroot Modelle	185
b) SSL, TLS & Co	186
c) PKCS #1v1.5	189
d) Der Angriff von BLEICHENBACHER	190
e) Elektronische Unterschriften nach PKCS#1	193
f) BLEICHENBACHERS Angriff dagegen	196
§8: Faktorisierungsverfahren	198
a) Mögliche Ansätze zur Faktorisierung	198
b) Das quadratische Sieb	200
c) Varianten des quadratischen Siebs	208
1.) Die Multipolynomialversion	209
2.) Das Zahlkörpersieb	210
d) Faktorisierungsrekorde	211
e) Faktorisierung mit Spezialhardware	214
§9: Literatur	217
KAPITEL V: VERFAHREN MIT DISKRETEN LOGARITHMEN	219
§1: Schlüsselaustausch nach Diffie und Hellman	219
a) Das Verfahren	220
b) Die <i>man in the middle attack</i>	221
§2: Verschlüsselung und elektronische Unterschriften	223
a) Verschlüsselung nach ELGAMAL	223
b) Das Verfahren von MASSEY-OMURA	225
c) DSA	227

§3: Strategien zur Berechnung diskreter Logarithmen	230
a) Probieren	230
b) Gruppentheoretische Formulierung des Problems	230
c) Anwendung des chinesischen Restesatzes	234
d) Das Verfahren von POHLIG und HELLMAN	234
e) Folgerung für die Sicherheit von Kryptosystemen	236
f) Baby step und giant step	236
g) Zahme und wilde Kängurus	237
h) Indexkalkül	240
§4: Diskrete Logarithmen in anderen Gruppen	242
a) Die abstrakte Situation	242
b) Multiplikative Gruppen beliebiger endlicher Körper	243
c) Elliptische Kurven	244
§5: Literatur	247
KAPITEL VI: DER ADVANCED ENCRYPTION STANDARD RIJNDAEL	249
§1: Geschichte und Auswahlkriterien	249
§2: Algebraische Vorbereitungen	252
a) EUKLIDISCHE RINGE	252
b) Endliche Körper von Primzahlpotenzordnung	256
c) Der Körper mit 256 Elementen	259
§3: Spezifikation von Rijndael	261
a) Terminologie und Bezeichnungen	261
b) Die Grundoperationen	261
c) Der Aufbau der Runden	263
1.) Die Bytesubstitution	264
2.) Die Zeilenshifts	266
3.) Der Spaltenmix	266
4.) Schlüsselexpansion und Rundenschlüssel	267
d) Gesamttablauf von Rijndael	268
e) Geschwindigkeitsoptimierung	268
§4: Angriffe auf Rijndael	270
§5: Literatur	272

KAPITEL VII: KRYPTOGRAPHISCH SICHERE HASHVERFAHREN	273
§1: Nochmals elektronische Unterschriften	273
§2: Das Geburtstagsparadoxon	274
§3: Die Familie der SHA-Algorithmen	277
§4: Weitere Anwendungen sicherer Hashfunktionen	285
a) Schutz der Integrität von Daten	285
b) Wie zufällig müssen unsere Schlüssel sein?	286
c) Erzeugung großer Zufallszahlen aus kleinen	287
d) Primzahlen für DSA	288
e) Wie bekommt man echte Zufallszahlen?	290
§5: Literatur	292
KAPITEL VIII: KRYPTOGRAPHISCHE PROTOKOLLE	293
§1: Werfen einer Münze per Telephone	294
§2: Poker per Telephone	296
§3: Zero Knowledge Protokolle	299
§4: Schlußbemerkung	303
§5: Literatur	304
KAPITEL IX: KRYPTOLOGIE UND QUANTENPHYSIK	305
§1: Grundzüge der Quantenmechanik	306
§2: Quantenkryptographie	312
a) Informationsübertragung mit einzelnen Photonen	313
b) Protokolle zur Quantenkryptographie	316
c) Angriffsmöglichkeiten	319
d) Fehlerkorrektur	321
e) Elimination der gegnerischen Information	323
§3: Quantencomputer	324
a) Quantenregister und QBits	324
b) Quantencomputer	326
c) Der Algorithmus von SHOR	328

d) Was können Quantencomputer?	335
e) Experimentelle Realisierung	338
§4: Andere nichtkonventionelle Rechnerarchitekturen	339
a) Die Desoxyribonucleinsäure	341
b) Die Polymerase-Kettenreaktion	343
c) ADLEMANs Experiment	344
d) Wie geht es weiter?	347
e) Literaturhinweise	350