

WOLFGANGSEILER  
NPEOXFAAQEREPJCMKCTVFNJWBOSRH  
XQLOIMJGCVJARI  
ZQEOWYSQLSAAYBQLIQVHSQJRIUJODL  
NEZCLXANNAPQGGCK  
KKPAAYBBVPQGT  
HTEQKNULES  
DPDQMIQSJGNXEOG  
JZTYAHVHI  
OFFZXNDZII  
JBJMYBZJBDLZSCX  
SFINYBZJBDLZSCX  
JFHOIE  
CIXGCF  
A  
M  
C  
H  
U  
Y  
L

VORLESUNGANDE  
R  
N  
I  
V  
E  
R  
S  
I  
T  
Ä  
T  
M  
A  
N  
N  
H  
E  
I  
M  
I  
M  
W  
I  
N  
I  
N  
2  
0  
0  
4  
/  
2  
0  
0  
5

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.

Im Augenblick enthält das Skriptum um hinteren Teil auch noch teilweise sehr vorläufige Fragmente, die noch nicht mit dem Rest des Texts abgestimmt sind; bei diesen kann es auch zu Bezeichnungsinkonsistenzen und Schlimmerem kommen.

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](mailto:seiler@math.uni-mannheim.de)) mit. Auch wenn Sie Teile des Skriptums unverständlich finden, bin ich, auch im Namen der künftigen Studenten der Kryptologie-Vorlesung, für entsprechende Hinweise dankbar.

KAPITEL 0: WAS IST KRYPTOLOGIE? .....	1
KAPITEL I: KLASSISCHE VERFAHREN DER KRYPTOLOGIE .....	5
§1: Die Anfänge .....	6
§2: Arten kryptanalytischer Angriffe .....	8
§3: Kryptanalyse der Caesarchiffre .....	11
§4: VIGÈNERE-Chiffren .....	15
§5: Substitutionschiffren .....	29
§6: Permutationschiffren .....	50
§7: Polyalphabetische Substitutionen .....	51
§8: Literaturhinweise .....	54
KAPITEL II: INFORMATIONSTHEORETISCHE ANSÄTZE .....	55
§1: Die Entropie einer Quelle .....	56
§2: Kryptanalyse durch den BAYESSchen Gegner .....	69
a) Die Grundidee .....	69
b) Einführendes Beispiel .....	70
c) Der allgemeine Ansatz .....	75
d) Perfekte Sicherheit .....	78
e) Die Mehrdeutigkeit eines Schlüssels .....	79
f) Randomisierung .....	81
g) Folgen für Sicherheitsanforderungen .....	91

§3: Wie wählt man zufällige Schlüssel? .....	95
a) Was ist Zufall? .....	95
b) Physikalische Zufallsquellen .....	96
c) Pseudozufallszahlen .....	97
d) Test von Zufallszahlen .....	105
§4: Literatur .....	107
KAPITEL III: BLOCKCHIFFREN UND IHRE KRYPTANALYSE I: DES ..	108
§1: Grundlagen .....	108
a) Die Sicherheit einer Blockchiffre .....	108
b) Beispiel: HILL-Chiffren .....	110
c) Diffusion und Konfusion .....	111
§2: FEISTEL-Netzwerke und der Aufbau des DES .....	111
a) FEISTEL-Netzwerke .....	112
b) Aufbau des DES .....	112
§3: Designkriterien und Kryptanalyse des DES .....	118
a) Geschichtliche Entwicklung .....	118
b) Designkriterien .....	120
c) Differentielle Kryptanalyse .....	122
d) Lineare Kryptanalyse .....	129
e) DES-Cracker .....	129

§4: Modifikationen .....	132
<i>a)</i> Mehrfacher DES .....	132
<i>b)</i> Doppelter DES .....	134
<i>c)</i> Dreifacher DES .....	134
§5: Operationsmodi .....	135
<i>a)</i> Electronic Code Book (ECB) .....	135
<i>b)</i> Cipher Block Chaining (CBC) .....	137
<i>c)</i> Cipher Feedback (CFB) .....	140
<i>d)</i> Output feedback (OFB) .....	142
<i>e)</i> Counter mode (CTR) .....	143
§6: Literatur .....	144
KAPITEL IV: DER ADVANCED ENCRYPTION STANDARD RIJNDAEL .	145
§1: Geschichte und Auswahlkriterien .....	145
§2: Algebraische Vorbereitungen .....	148
<i>a)</i> Der Euklidische Algorithmus für natürliche Zahlen .....	149
<i>b)</i> Körper von Primzahlordnung .....	153
<i>c)</i> EUKLIDISCHE RINGE .....	154
<i>d)</i> Endliche Körper von Primzahlpotenzordnung .....	158
<i>e)</i> Der Körper mit 256 Elementen .....	161

§3: Spezifikation von Rijndael .....	163
<i>a)</i> Terminologie und Bezeichnungen .....	163
<i>b)</i> Die Grundoperationen .....	163
<i>c)</i> Der Aufbau der Runden .....	165
1.) Die Bytesubstitution .....	166
2.) Die Zeilenshifts .....	168
3.) Der Spaltenmix .....	168
4.) Schlüsselexpansion und Rundenschlüssel .....	169
<i>d)</i> Gesamtlauf von Rijndael .....	170
<i>e)</i> Geschwindigkeitsoptimierung .....	171
§4: Angriffe auf Rijndael .....	173
§5: Literatur .....	174
KAPITEL V: DAS RSA-VERFAHREN .....	175
§1: New directions in cryptography .....	175
§2: Algebraische Vorbereitungen .....	178
§3: Das RSA-Verfahren zur Verschlüsselung und für elektronische Unterschriften .....	181
<i>a)</i> Verschlüsselung .....	181
<i>b)</i> Identitätsnachweis .....	181
<i>c)</i> Elektronische Unterschriften .....	182
<i>d)</i> Blinde Unterschriften und elektronisches Bargeld .....	183
<i>e)</i> Bankkarten mit Chip .....	186

§4: Wie findet man große Primzahlen? .....	188
a) Wie groß sollten die Primzahlen sein? .....	188
b) Wie dicht liegen die Primzahlen? .....	191
c) Das Sieb des ERATOSTHENES .....	193
d) Der FERMAT-Test .....	194
e) Die multiplikative Gruppe eines endlichen Körpers .....	198
f) Anwendung auf Primzahltests .....	200
§5: Faktorisierungsverfahren .....	201
a) Mögliche Ansätze zur Faktorisierung .....	202
b) Das quadratische Sieb .....	204
c) Varianten des quadratischen Siebs .....	210
1.) Die Multipolynomialversion .....	210
2.) Das Zahlkörpersieb .....	212
d) Faktorisierungsrekorde .....	213
e) Faktorisierung durch Spezialhardware .....	217
f) Folgerungen für die Wahl der Schlüssellänge .....	219
§6: Weitere Aspekte zum RSA-Verfahren .....	222
a) Das Problem der Schlüsselübergabe .....	223
b) Primzahlen sind Wegwerfartikel .....	223
c) Kenntnis des privaten Exponenten führt zur Faktorisierung .....	224
d) Der chinesische Restesatz .....	226
e) Kleine öffentliche Exponenten .....	228
f) Kleine private Exponenten .....	229

§7: RSA in der Praxis .....	231
a) SSL & Co .....	232
b) PKCS #1v1.5 .....	234
c) Der Angriff von BLEICHENBACHER .....	236
§8: Literatur .....	240
KAPITEL VI: VERFAHREN MIT DISKRETEN LOGARITHMEN .....	242
§1: Schlüsselaustausch nach DIFFIE und HELLMAN .....	242
a) Das Verfahren .....	243
b) Die <i>man in the middle attack</i> .....	243
c) Wie sind die vereinbarten Schlüssel verteilt? .....	245
§2: Diskrete Logarithmen .....	245
a) Logarithmen in endlichen Körpern .....	245
b) Wie groß sollten die Körper sein? .....	247
c) Der allgemeine diskrete Logarithmus .....	248
d) Die Struktur zyklischer Gruppen .....	249
e) Das Verfahren von POHLIG und HELLMAN .....	250
f) Folgerungen für Kryptosysteme über endlichen Körpern .....	252
§4: Strategien zur Berechnung diskreter Logarithmen .....	254
a) Probieren .....	255
b) Das Verfahren von POHLIG und HELLMAN .....	255
c) Baby steps und giant steps .....	255

§3: Das Verfahren von ELGAMAL .....	258
c) Verschlüsselung nach ELGAMAL .....	258
d) Das Verfahren von MASSEY-OMURA .....	258
§5: Elliptische Kurven .....	260
a) Ebene algebraische Kurven .....	261
b) Singularitäten .....	268
c) Elliptische Kurven .....	268
§6: Literatur .....	276
KAPITEL VII: SHA UND DSA .....	278
§1: Nochmals elektronische Unterschriften .....	278
§2: Das Geburtstagsparadoxon .....	279
§3: Die Familie der SHA-Algorithmen .....	281
§4: DSA .....	287
§5: DSA mit elliptischen Kurven .....	288
§6: Literatur .....	289
KAPITEL VIII: KRYPTOGRAPHISCHE PROTOKOLLE .....	290
§1: Werfen einer Münze per Telephone .....	291
§2: Poker per Telephone .....	292
§x): Quadratische Reste .....	295
§y): Quadratwurzeln modulo einer Primzahl .....	300

KAPITEL IX: SPEKULATIONEN ÜBER KÜNFTIGE ENTWICKLUNGEN .....	307
§1: Quantenkryptographie .....	307
a) Informationsübertragung mit einzelnen Photonen .....	308
b) Protokolle zur Quantenkryptographie .....	311
c) Elimination der gegnerischen Information .....	313
d) Literaturhinweise .....	318
§2: Quantencomputer .....	319
a) Quantenmechanische Grundlagen .....	319
b) Quantenregister und QBits .....	322
c) Quantencomputer .....	324
d) Der Algorithmus von SHOR .....	326
e) Experimentelle Realisierung .....	332
f) Literaturhinweise .....	334
§3: DNS-Computer .....	335
a) Die Desoxyribonucleinsäure .....	336
b) Die Polymerase-Kettenreaktion .....	338
c) ADLEMANS Experiment .....	339
d) Wie geht es weiter? .....	343
e) Literaturhinweise .....	346