



10. Juli 2002

**Semestralklausur zu**  
**Einführung in die Kryptographie**  
**SS 2002**

Name, Vorname: .....

Fachbereich: ..... Matrikelnummer: .....

Fachsemester: ..... Aufbaustudium:  Wiederholer(in):

Unterschrift: .....

**Hinweise:**

1. Prüfen Sie, ob die Klausur alle 10 Aufgaben enthält.
2. Füllen Sie das Deckblatt vollständig aus.
3. Halten Sie ihren Studenausweis und einen Lichtbildausweis bereit.
4. Kennzeichnen Sie alle verwendeten Blätter zuerst mit Name und Matrikelnr.
5. Es sind die verwendeten Formeln und die Zwischenergebnisse anzugeben.
6. Markieren Sie auf dem Deckblatt die bearbeiteten Aufgaben.
7. Zum Bestehen der Prüfung ist es hinreichend 50 Punkte zu erreichen.
8. Ihnen stehen 90 min zum Bearbeiten der Aufgaben zur Verfügung.
9. Zugelassene Hilfsmittel sind ein DIN A4 Blatt (beidseitig) handgeschriebene Formelsammlung und ein nicht programmierbarer Taschenrechner.

Aufgabe	1	2	3	4	5	6	7	8	9	10
Punkte maximal	10	10	10	10	10	10	10	10	10	10
bearbeitet										
Punkte erreicht										

### Aufgabe 1: Erweiterter euklidischer Algorithmus

1. Berechnen Sie  $\gcd(245, 193)$  samt seiner Darstellung in der Form  $x \cdot 245 + y \cdot 193$  mit dem erweiterten Euklidischen Algorithmus.
2. Berechnen Sie die kleinste positive Lösung der Kongruenz  $193x \equiv 2 \pmod{245}$ .

### Aufgabe 2: Schnelle Exponentiation

Berechnen Sie mit Hilfe der schnellen Exponentiation  $7^{27} \pmod{31}$ .

### Aufgabe 3: Chinesischer Restsatz

Finden Sie die kleinste nichtnegative Lösung der folgenden simultanen Kongruenz mit dem chinesischen Restsatz.

$$\begin{aligned}x &\equiv 2 \pmod{3} \\x &\equiv 1 \pmod{7} \\x &\equiv 7 \pmod{11}\end{aligned}$$

### Aufgabe 4: Verschlüsselungsmodi

Ein Klartext  $m$  wurde im CBC-Mode zu  $c = 110000$  verschlüsselt und im CFB-Mode zu  $\hat{c} = 100010$  verschlüsselt. Beim Verschlüsseln wurde in beiden Fällen die Permutationschiffre mit Blocklänge 3 und Schlüssel

$$\pi = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}.$$

verwendet. D.h.  $\pi(1) = 3, \pi(2) = 1, \pi(3) = 2$ , also z.B.  $E_\pi(100) = 010$ . Als Initialisierungsvektor wurde jeweils  $IV = 111$  verwendet. Im CFB-Mode wurde  $r = 2$  benutzt. **Entschlüsseln** Sie die Chiffretexte im jeweiligen Modus. Hinweis: es ist

$$\pi^{-1} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}.$$

### Aufgabe 5: Affin lineare Chiffren

Bei einer Kommunikation haben Sie die folgenden Chiffretextblöcke mitgelesen: “ZK”, “YJ”, und “XJ”. Sie haben herausgefunden, daß die zugehörigen Klartextblöcke “GE”, “HE”, und “IM” lauten. Sie gehen davon aus, daß diese Verschlüsselung durch einfache wiederholte Anwendung (ECB Mode) einer affin linearen Chiffre der Blocklänge 2 stattgefunden hat. Ausserdem wissen Sie, daß das zugrundeliegende Alphabet die Menge  $\{A - Z, ., !, ?\}$  ist, wobei die Zuordnung von Buchstaben und Zahlen anhand der angegebenen Tabelle erfolgt. Bestimmen Sie die Verschlüsselungsfunktion mittels der in der Vorlesung vorgestellten Known-Plaintext-Attacke auf affin lineare Chiffren.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
P	Q	R	S	T	U	V	W	X	Y	Z	.	!	?	
15	16	17	18	19	20	21	22	23	24	25	26	27	28	

### Aufgabe 6: RSA

Sie haben den öffentlichen RSA Schlüssel  $n = 21$  und  $e = 5$ .

1. Berechnen Sie den Entschlüsselungsexponenten  $d$  und entschlüsseln Sie  $c = 5$ .
2. Berechnen Sie alle Fixpunkte  $M \in \{0, \dots, 20\}$  von  $M \mapsto M^5 \pmod{21}$ .

### Aufgabe 7: ElGamal Signatur

Der öffentlicher ElGamal Schlüssel sei  $(p, g, A) = (17, 3, 4)$  und der private Schlüssel sei  $a = 12$ .

1. Berechnen Sie eine ElGamal Signatur für den Hashwert  $h(m) = 10$ . Wählen Sie dabei den zufälligen Wert  $k = 3$ .
2. Ist das Paar  $(r, s) = (5, 11)$  eine gültige Signatur für  $h(m) = 3$  ?

### Aufgabe 8: Shamir's secret sharing

Mit Shamir's secret sharing Verfahren wurden Anteile an einem Geheimnis an 5 Personen so verteilt, dass bereits 3 Personen zur Rekonstruktion des Geheimnisses genügen. Bei der Konstruktion der Anteile wurde die Primzahl  $p = 19$  verwendet. Person 1 erhielt dabei den Anteil  $A_1 = 11$ , Person 2 den Anteil  $A_2 = 2$ , Person 3 den Anteil  $A_3 = 14$ , Person 4 den Anteil  $A_4 = 9$  und Person 5 den Anteil  $A_5 = 6$ . Rekonstruieren sie das Geheimnis aus den Anteilen der Personen **1,2** und **5**.

### **Aufgabe 9: Ordnung**

1. Bestimmen Sie eine Primitivwurzel in  $\mathbb{Z}_{19}^*$ .
2. Bestimmen Sie ein Element der Ordnung 6 in  $\mathbb{Z}_{19}^*$ .

### **Aufgabe 10: Shank's Babystep-Giantstep Algorithmus**

Lösen Sie  $6^x \equiv 2 \pmod{13}$  mit dem Babystep-Giantstep Algorithmus.