

Heinrich-Heine-Universität  
Düsseldorf  
Institut für Informatik  
Prof. Dr. J. Rothe

Universitätsstr. 1, D-40225 Düsseldorf  
Gebäude: 25.12, Ebene: O2, Raum: 26  
Tel.: +49 211 8112188, Fax: +49 211 8111667  
E-Mail: rothe@hhu.de  
13. Dezember 2023

Vorlesung im Wintersemester 2023/24

# Kryptokomplexität 1

Probeklausur

**BITTE NICHT MIT BLEISTIFT ODER ROTSTIFT SCHREIBEN!  
TRAGEN SIE AUF JEDEM BLATT IHREN NAMEN, VORNAMEN  
UND IHRE MATRIKELNUMMER SOWIE ZUSÄTZLICH AUF DEM  
DECKBLATT STUDIENFACH MIT SEMESTER UND ANZAHL DER  
ABGEBEBENEN BLÄTTER EIN, UND UNTERSCHREIBEN SIE  
ALS STUDIERENDE/R DER INFORMATIK, DASS SIE ANGEMELDET SIND!**

- ▶ **Nachname, Vorname:**
- ▶ **Studienfach, Fachsemester:**
- ▶ **Matrikelnummer:**
- ▶ **(Nur für Studierende der Informatik) Hiermit bestätige ich, dass ich mich beim akademischen Prüfungsamt für diese Klausur angemeldet habe:**

\_\_\_\_\_  
Unterschrift

- ▶ **Anzahl der abgegebenen Blätter, inklusive der 5 Aufgabenblätter:**

**Erlaubte Hilfsmittel:** Alle Materialien in Papierform, insbesondere handgeschriebene oder gedruckte Notizen, Bücher, Vorlesungsfolien (ausgedruckt), Übungszettel und Lösungen.

**In der Klausur nicht erlaubte Hilfsmittel:** Elektronische Geräte aller Art.

**Achten Sie darauf, dass Rechenwege und Zwischenschritte vollständig und ersichtlich sind.**

Aufgabe	1	2	3	4	5	Gesamt
erreichbare Punktzahl	20	20	20	20	20	100
erreichte Punktzahl						



**Aufgabe 1 (20 Punkte)** *Multiple Choice***/20 Punkte**

Kreuzen Sie für jede der folgenden Fragen in jeder Zeile entweder „Ja“ oder „Nein“ an.

**Bewertung:** Bezeichnet  $\#R$  die Anzahl der von Ihnen richtig angekreuzten Antworten und  $\#K$  die Anzahl der von Ihnen insgesamt angekreuzten Antworten (d. h. nur solche, bei denen *entweder* „Ja“ oder „Nein“ angekreuzt wurde – Antworten, bei denen weder „Ja“ noch „Nein“ oder sowohl „Ja“ als auch „Nein“ angekreuzt wurde, zählen nicht zu  $\#K$ ), so ergibt sich die folgende Gesamtpunktzahl für diese Aufgabe:

$$\#R + \left\lfloor \frac{5 \cdot \#R}{\#K} \right\rfloor \text{ Punkte, falls } \#K > 0, \text{ und } 0 \text{ Punkte, falls } \#K = 0.$$

(a) Welche der folgenden Aussagen ist/sind wahr?

- Ja  Nein Die Vigenère-Chiffre ist monoalphabetisch.  
 Ja  Nein Die Permutationschiffre ist linear.  
 Ja  Nein Die Determinante der Matrix  $\begin{pmatrix} 3 & 4 \\ 5 & 2 \end{pmatrix} \pmod{7}$  ist gleich 1.

(b) Welche der folgenden Aussagen ist/sind wahr?

- Ja  Nein Die Matrix  $\begin{pmatrix} 3 & 4 \\ 5 & 2 \end{pmatrix}$  ist modulo 9 invertierbar.  
 Ja  Nein Die Hill-Chiffre ist sicher gegen *Known-Plaintext*-Angriffe.  
 Ja  Nein Übertragungsfehler richten im CFB-Modus weniger Schaden als im OFB-Modus an.

(c) Welche der folgenden Aussagen ist/sind wahr?

- Ja  Nein Der One-time Pad von Vernam ist unsicher gegen *Known-Plaintext*-Angriffe.  
 Ja  Nein Die Entropie des Ausgangs eines Pferderennens mit vier „gleich schnellen“ Pferden ist gleich 3.  
 Ja  Nein Mit der Entropie einer natürlichen Sprache wächst ihre Redundanz.

(d) Welche der folgenden Aussagen ist/sind wahr?

- Ja  Nein Die Anzahl der Primzahlen ist unendlich.  
 Ja  Nein Ein Fermat-Zeuge für  $n$  bezeugt die Primalität von  $n$ .  
 Ja  Nein 168 ist ein Fermat-Lügner für 169.

(e) ► Welche der folgenden Aussagen ist/sind wahr?

- Ja  Nein Die Menge der Fermat-Lügner für eine Carmichael-Zahl  $n$  ist verschieden von  $\mathbb{Z}_n^*$ .  
 Ja  Nein Wieners Angriff auf RSA benutzt Kettenbruch-Approximationen.  
 Ja  Nein Kennt ein Angreifer auf RSA  $\varphi(n)$ , wobei  $(n, e)$  der öffentliche RSA-Schlüssel ist, so kann er die Primfaktoren  $p$  und  $q$  von  $n$  effizient bestimmen und somit RSA brechen.

Name:

Matrikelnummer:

4

**Aufgabe 2 (20 Punkte)** Chiffren

**/20 Punkte**

Sie dürfen bei allen Aufgabenteilen davon ausgehen, dass gültige Schlüssel verwendet werden.

- (a) Benutzen Sie die affin lineare Blockchiffre mit dem Alphabet  $\Sigma = \{A, B, C, \dots, Z, \ddot{A}, \ddot{O}, \ddot{U}\}$  über  $\mathbb{Z}_{29}$  sowie

$$A = \begin{pmatrix} 17 & 19 & 18 \\ 10 & 27 & 1 \\ 23 & 5 & 11 \end{pmatrix} \quad \text{und} \quad b = \begin{pmatrix} 3 \\ 8 \\ 27 \end{pmatrix},$$

um den Klartext  $m = \text{KRYPTO}$  zu verschlüsseln.

- (b) Verschlüsseln Sie die Nachricht  $m = \text{NP HARD}$  mit Hilfe der Permutationschiffre mit der Permutation (in Zykelschreibweise)  $\pi = (145)(632)$ .
- (c) Sei die Blocklänge  $n = 2$ . Es werden die Ciphertexte  $c_1 = (7, 16)$  und  $c_2 = (4, 24)$  zu den Klartexten  $m_1 = (13, 17)$  und  $m_2 = (2, 14)$  abgefangen. Führen Sie nun mit diesen Werten einen *Known-Plaintext*-Angriff auf die Hill-Chiffre durch, um den benutzten Schlüssel herauszufinden.
- (d) Betrachten Sie die Stromchiffre basierend auf einem linear rückgekoppelten Schieberegister mit Alphabet  $\Sigma = \{0, 1\}$ ,  $n = 3$  und dem Schlüssel  $\vec{k} = (1, 1, 0)$ . Die ersten sechs Schlüssel des Schlüsselstroms sind  $\vec{s} = (1, 1, 0, 0, 1, 1, \dots)$ . Berechnen Sie den nächsten Schlüssel des Schlüsselstroms, also  $s_7$ , und verschlüsseln Sie den Klartext  $\vec{m} = (0, 1, 1, 0, 0, 1)$ .

**(Bitte geben Sie alle Argumente vollständig und verständlich an!)**

Name:

Matrikelnummer:

5

Name:

Matrikelnummer:

6

**Aufgabe 3 (20 Punkte) RSA**

**/20 Punkte**

- (a) Betrachten Sie für das RSA-Kryptosystem die Primzahlen  $p = 17$  und  $q = 31$  sowie den öffentlichen Exponenten  $e = 19$ .
- ▶ Zeigen Sie, dass  $d = 379$  der passende private Exponent ist, indem Sie den erweiterten euklidischen Algorithmus anwenden.
- (b) ▶ Verschlüsseln Sie für das RSA-Kryptosystem aus (a) die Nachricht  $m = 2$ . Verwenden Sie dabei den *Square-and-Multiply*-Algorithmus.
- (c) ▶ Zeigen Sie, dass  $x = 475$  eine Lösung zu folgendem Kongruenzensystem ist, indem Sie den chinesischen Restesatz aus der Vorlesung anwenden. Die Berechnung von inversen Elementen muss dabei nicht angegeben werden.

$$8x \equiv 2 \pmod{9}$$

$$x \equiv 2 \pmod{11}$$

$$4x \equiv 2 \pmod{13}$$

**(Bitte geben Sie alle Argumente vollständig und verständlich an!)**

**Name:**

**Matrikelnummer:**

7

Name:

Matrikelnummer:

8

**Aufgabe 4 (20 Punkte)** *Primzahltests*

**/20 Punkte**

- (a) Führen Sie den Miller-Rabin-Test für  $n = 721$  durch und wählen Sie dabei  $a = 57$ . Geben Sie an, ob  $a$  ein Miller-Rabin-Zeuge oder ein Miller-Rabin-Lügner ist. Verwenden Sie für die Berechnungen Square-and-Multiply.
- (b) Führen Sie den Fermat-Test für  $n = 721$  durch und wählen Sie dabei erneut  $a = 57$ . Geben Sie an, ob  $a$  ein Fermat-Zeuge oder ein Fermat-Lügner ist. Verwenden Sie für die Berechnungen Square-and-Multiply. Sie dürfen auch Rechnungen aus Aufgabenteil (a) wiederverwenden.
- (c) Zeigen Sie:

$a$  ist ein Fermat-Zeuge von  $n \Rightarrow a$  ist ein Miller-Rabin-Zeuge von  $n$

**(Bitte geben Sie alle Argumente vollständig und verständlich an!)**

Name:

Matrikelnummer:

9

**Aufgabe 5 (20 Punkte)** *Wahrscheinlichkeit und Entropie***/20 Punkte**

In dieser Aufgabe dürfen Logarithmen im Ergebnis stehen, wenn die Terme so weit wie möglich vereinfacht sind. Logarithmen, die sich auch ohne Taschenrechner einfach bestimmen lassen, sollten dagegen in jedem Fall ausgerechnet werden.

- (a) Für ein Online-Würfelspiel soll die Übertragung der gewürfelten Ergebnisse verschlüsselt werden. Gewürfelt wird jeweils mit zwei sechsseitigen Würfeln. Der Klartextraum  $M$  besteht also aus den Ergebnissen der Würfelwürfe.

Fassen Sie  $M$  als Zufallsvariable auf und berechnen Sie deren Entropie für den Fall, dass . . .

- ▶ die beiden Würfel unterscheidbar sind – in diesem Fall gibt es 36 verschiedene Klartexte, die alle gleichwahrscheinlich sind;
- ▶ die beiden Würfel nicht unterscheidbar sind – in diesem Fall gibt es 21 verschiedene Klartexte: jeder Pasch hat die Wahrscheinlichkeit von  $1/36$ , jeder andere Wurf von  $1/18$ .

- (b) Gegeben sei ein Kryptosystem  $S = (M, C, K, \mathcal{E}, \mathcal{D})$  mit

$$\begin{aligned} M &= \{0, 1\}, & \Pr(0) &= 1/3, & \Pr(1) &= 2/3, \\ K &= \{x, y\}, & \Pr(x) &= 1/4, & \Pr(y) &= 3/4 \\ & \text{und } C &= \{a, b, c, d\}. \end{aligned}$$

Die Schlüssel werden unabhängig von den Klartexten gezogen. Weiterhin sei  $\mathcal{E}$  gegeben durch:

$\mathcal{E}$	0	1
$x$	$a$	$b$
$y$	$c$	$d$

- ▶ Bestimmen Sie die Wahrscheinlichkeitsverteilung auf dem Schlüsseltextraum  $C$ , der durch die Verteilungen auf  $M$  und  $K$  induziert wird.
- (c) ▶ Fassen Sie  $C$  aus Teilaufgabe (b) als Zufallsvariable auf und bestimmen Sie ihre Entropie.

**(Bitte geben Sie alle Zwischenschritte der Rechnungen in allen Teilaufgaben an!)**

Name:

Matrikelnummer:

11