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
ABGEGEBENEN 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 $\begin{pmatrix} 3 & 4 \\ 5 & 2 \end{pmatrix} \bmod 7$ 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.

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 $\Sigma = \{\texttt{A}, \texttt{B}, \texttt{C}, \ldots, \texttt{Z}, \ddot{\texttt{A}}, \ddot{\texttt{O}}, \ddot{\texttt{U}}\}$ 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 $m = \texttt{KRYPTO}$ zu verschlüsseln.

(b) Verschlüsseln Sie die Nachricht $m = \texttt{NPHARD}$ mit Hilfe der Permutationschiffre mit der Permutation (in Zyklenschreibweise) $\pi = (145)(632)$.

(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 $\vec{s} = (1, 1, 0, 0, 1, 1, \ldots)$. 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!)

(a) (8 Punkte) Durch die Blocklänge $n = 3$, ist $m_1 = (10, 17, 24)$ und $m_2 = (15, 19, 14)$. Dann werden die Ciphertexte berechnet durch

$$c_1 = A \cdot m_1 + b = \begin{pmatrix} 17 & 19 & 18 \\ 10 & 27 & 1 \\ 23 & 5 & 11 \end{pmatrix} \cdot \begin{pmatrix} 10 \\ 17 \\ 24 \end{pmatrix} + \begin{pmatrix} 3 \\ 8 \\ 27 \end{pmatrix} = \begin{pmatrix} 928 \\ 591 \\ 606 \end{pmatrix} \equiv \begin{pmatrix} 0 \\ 11 \\ 26 \end{pmatrix} \mod 29$$

$$\text{und } c_2 = A \cdot m_2 + b = \begin{pmatrix} 17 & 19 & 18 \\ 10 & 27 & 1 \\ 23 & 5 & 11 \end{pmatrix} \cdot \begin{pmatrix} 15 \\ 19 \\ 14 \end{pmatrix} + \begin{pmatrix} 3 \\ 8 \\ 27 \end{pmatrix} = \begin{pmatrix} 871 \\ 685 \\ 621 \end{pmatrix} \equiv \begin{pmatrix} 1 \\ 18 \\ 12 \end{pmatrix} \mod 29$$

Und somit ist $c = \texttt{ALÄBSM}$.

(b) (2 Punkte) Die Permutation in Matrixschreibweise ist:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 6 & 2 & 5 & 1 & 3 \end{pmatrix}$$

Dann ist $c = x_{\pi(1)}x_{\pi(2)}x_{\pi(3)}x_{\pi(4)}x_{\pi(5)}x_{\pi(6)} = x_4x_6x_2x_5x_1x_3 = \texttt{ADPRNH}$

(c) (7 Punkte) Aus den Werten ergeben sich die Matrizen

$$X = \begin{pmatrix} 13 & 2 \\ 17 & 14 \end{pmatrix} \text{ und } Y = \begin{pmatrix} 7 & 4 \\ 16 & 24 \end{pmatrix}$$

Dann ist $\det(X) = 13 \cdot 14 - 2 \cdot 17 \equiv 3 \mod 29$, also $(\det(X))^{-1} = 3^{-1} \equiv 10 \mod 29$.

Weiterhin ist $X_{\text{adj}} = \begin{pmatrix} 14 & -2 \\ -17 & 13 \end{pmatrix} \equiv \begin{pmatrix} 14 & 27 \\ 12 & 13 \end{pmatrix} \mod 29$ mit der Formel aus der Vorlesung.

Dann ist $A = Y \cdot ((\det(X))^{-1} \cdot X_{\text{adj}}) = \begin{pmatrix} 7 & 4 \\ 16 & 24 \end{pmatrix} \cdot (10 \cdot \begin{pmatrix} 14 & 27 \\ 12 & 13 \end{pmatrix}) \equiv$

$\begin{pmatrix} 7 & 4 \\ 16 & 24 \end{pmatrix} \cdot \begin{pmatrix} 24 & 9 \\ 4 & 14 \end{pmatrix} \equiv \begin{pmatrix} 10 & 3 \\ 16 & 16 \end{pmatrix} \mod 29$

(d) (3 Punkte) (Alle Berechnungen sind modulo 2)

Zunächst werden die Koeffizienten a_1, a_2 und a_3 bestimmt. Da $k_3 = s_4 = 0$, gilt $1 = s_5 = a_3$. Dann ist $0 = s_4 = a_2 + a_3 = a_2 + 1$ und somit $a_2 = 1$. Schließlich ist $1 = s_6 = a_1$, da $k_3 = s_4 = 0$.

Mit den Koeffizienten berechnen wir dann $s_7 = a_1 \cdot s_6 + a_2 \cdot s_5 + a_3 \cdot s_4 = 1 \cdot 1 + 1 \cdot 1 + 0 = 0$

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.

$$\begin{aligned} 8x &\equiv 2 \mod 9 \\ x &\equiv 2 \mod 11 \\ 4x &\equiv 2 \mod 13 \end{aligned}$$

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

(a) (4 Punkte) $p = 17, q = 31, e = 19, \varphi(n) = 16 \cdot 30 = 480, d \equiv 19^{-1} \mod 480$.
Erweiterter euklidischer Algorithmus:

a	b	x	y
480	19	4	-101
5	4	1	-1
4	1	0	1
1	0	1	0

$\Rightarrow 19 \cdot 379 \equiv 1 \mod 480 \Rightarrow d = 379$.

(b) (4 Punkte) $n = p \cdot q = 17 \cdot 31 = 527$, bestimme $c = m^e \mod n$, also $c = 2^{19} \mod 527$ mit *Square-and-Multiply* in $\mathbb{Z}_{527}$:

$$19 = 2^0 + 2^1 + 2^4$$

2^0	2^1	2^2	2^3	2^4
2	**4**	16	256	**188**

$\Rightarrow c = 2 \cdot 4 \cdot 188 = 450$

(c) (12 Punkte)

- $8^{-1} \equiv 8 \mod 9$ und $4^{-1} \equiv 10 \mod 13$
- $\Rightarrow$

$$\begin{aligned} x &\equiv 8 \cdot 2 \equiv 7 \mod 9 \\ x &\equiv 2 \mod 11 \\ x &\equiv 10 \cdot 2 \equiv 7 \mod 13 \end{aligned}$$

- $M = m_1 \cdot m_2 \cdot m_3 = 9 \cdot 11 \cdot 13 = 1287$

- $q_1 = {}^{M}/_{m_1} = 143$, $q_2 = {}^{M}/_{m_2} = 117$ und $q_3 = {}^{M}/_{m_3} = 99$
- $q_1^{-1} = 143^{-1} \equiv 8^{-1} \equiv 8 \mod 9$, $q_2^{-1} = 117^{-1} \equiv 7^{-1} \equiv 8 \mod 11$ und $q_2^{-1} = 99^{-1} \equiv 8{-}1 \equiv 5 \mod 13$
- $\Rightarrow x \equiv a_1 \cdot q_1 \cdot q_1^{-1} + a_2 \cdot q_2 \cdot q_2^{-1} + a_3 \cdot q_3 \cdot q_3^{-1} \equiv 7 \cdot 143 \cdot 8 + 2 \cdot 117 \cdot 8 + 7 \cdot 99 \cdot 5 \equiv 8008 + 1872 + 3465 \equiv 475 \mod 1287$.

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:

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

(a) (10 Punkte) Zunächst gilt $720 = n - 1 = 2^4 \cdot 45$, also $m = 45$ und $k = 4$.

Dann folgt für den ersten Test: $57^m = 57^{45} \equiv 617 \mod 721$, also ist a^m nicht kongruent zu 1 modulo n und der erste Test ist bestanden.

Dann folgt der zweite Test:

$j = 0$: $57^{2^0 \cdot m} = 57^m \equiv 617 \not\equiv -1 \mod 721$

$j = 1$: $57^{2^1 \cdot m} \equiv 617^2 \equiv 1 \not\equiv -1 \mod 721$

$j = 2$: $57^{2^2 \cdot m} \equiv 1 \not\equiv -1 \mod 721$

$j = 3$: $57^{2^3 \cdot m} \equiv 1 \not\equiv -1 \mod 721$

Der zweite Test ist also auch bestanden und somit folgt für a, dass es ein Miller-Rabin-Zeuge für $n = 721$ ist.

Rechnungen mit square-and-multiply ($45 = 32 + 8 + 4 + 1 = 2^5 + 2^3 + 2^2 + 2^0$):

2^0	2^1	2^2	2^3	2^4	2^5
57	365	**561**	**365**	561	**365**

Also ist $57^{45} = 57 \cdot 561 \cdot 365 \cdot 365 \equiv 617 \mod 721$

(b) (3 Punkte) Es gilt $57^{n-1} = 57^{2^4 \cdot m} = (57^{2^3 \cdot m})^2 \overset{\text{(a)}}{\equiv} 1^2 \equiv 1 \mod 721$.

Da n keine Primzahl ist, ist 57 also ein Fermat-Lügner.

(c) (7 Punkte) Da a ein Fermat-Zeuge von n ist, wissen wir, dass n zusammengesetzt ist und $a^{(n-1)}$ nicht kongruent zu 1 modulo n ist. Für einen Widerspruch nehmen wir an, dass a kein Miller-Rabin-Zeuge ist. Wir unterscheiden drei Fälle:

1. n ist eine Primzahl: Das führt direkt zum Widerspruch.
2. $a^m \equiv 1 \mod n$. Dann ist $a^{n-1} = a^{2^k \cdot m} \equiv 1^{2^k} \equiv 1 \mod n$ ein Widerspruch.
3. Es gibt ein $j \in \{0, \ldots, k-1\}$, sodass $a^{2^j \cdot m} \equiv -1 \mod n$. Dann ist $(a^{2^j \cdot m})^2 = a^{2^{j+1} \cdot m} \equiv 1 \mod n$ und somit ist $a^{2^k \cdot m} \equiv a^{n-1} \equiv 1 \mod n$ ein Widerspruch.

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

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

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

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!)

(a) (9 Punkte) Fall 1: Unterscheidbar (3 Punkte). Es gilt

$$\mathcal{H}(M) = -\sum_{j=1}^{36} \frac{1}{36} \cdot \log_2\left(\frac{1}{36}\right) = 36 \cdot \frac{1}{36} \cdot \log_2(36) = 1 \cdot \log_2(36) = \log_2(2^2 \cdot 3^2)$$
$$= 2(\log_2(2) + \log_2(3)) = 2 \cdot 1 + 2\log_2(3) = 2 + 2\log_2(3) \quad (\approx 5,17)\,.$$

Fall 2: Nicht unterscheidbar (6 Punkte). Es gilt

$$\mathcal{H}(M) = -\sum_{j=1}^{6} \frac{1}{36} \cdot \log_2\left(\frac{1}{36}\right) - \sum_{j=1}^{15} \frac{1}{18} \log_2\left(\frac{1}{18}\right) = 6 \cdot \frac{1}{36} \cdot \log_2(36) + 15 \cdot \frac{1}{18} \cdot \log_2(18)$$
$$= \frac{1}{6}\log_2(36) + \frac{5}{6}\log_2(18) = \frac{1}{6}(2 + 2\log_2(3)) + \frac{5}{6}\log_2(2 \cdot 3^2)$$
$$= \frac{1}{3} + \frac{1}{3}\log_2(3) + \frac{5}{6}\log_2(2) + \frac{5}{3}\log_2(3) = \frac{7}{6} + 2\log_2(3) \quad (\approx 4,34)\,.$$

(b) (5 Punkte) Für die Wahrscheinlichkeitsverteilung auf C gilt

$$\begin{aligned}
\Pr(a) &= \Pr(0,x) = \Pr(0)\cdot\Pr(x) = \frac{1}{12},\\
\Pr(b) &= \Pr(1,x) = \Pr(1)\cdot\Pr(x) = \frac{1}{6},\\
\Pr(c) &= \Pr(0,y) = \Pr(0)\cdot\Pr(y) = \frac{1}{4},\\
\Pr(d) &= \Pr(1,y) = \Pr(1)\cdot\Pr(y) = \frac{1}{2}.
\end{aligned}$$

(c) (6 Punkte) Die Entropie berechnet sich dann durch

$$\begin{aligned}
\mathcal{H}(C) &= -\frac{1}{12}\log_2\left(\frac{1}{12}\right) - \frac{1}{6}\log_2\left(\frac{1}{6}\right) - \frac{1}{4}\log_2\left(\frac{1}{4}\right) - \frac{1}{2}\log_2\left(\frac{1}{2}\right)\\
&= \frac{1}{12}\log_2(12) + \frac{1}{6}\log_2(6) + \frac{1}{4}\log_2(4) + \frac{1}{2}\log_2(2)\\
&= \frac{1}{12}\log_2(12) + \frac{1}{6}\log_2(6) + \frac{1}{2} + \frac{1}{2}\\
&= 1 + \frac{1}{6} + \frac{1}{12}\log_2(3) + \frac{1}{6} + \frac{1}{6}\log_2(3)\\
&= \frac{4}{3} + \frac{1}{4}\log_2(3) \quad (\approx 1,73)\,.
\end{aligned}$$