

Aufgabe 1.1

Zähle die Hauptaufgaben der Kryptographie auf und beschreibe jeweils in knappen Sätzen, worum es dabei geht.

Aufgabe 1.2

Was besagt das Prinzip von *Kerckhoffs*?

Aufgabe 1.3

Was bedeutet der Ausdruck *Kryptoanalyse*?

Aufgabe 1.4

Welche der folgenden Situationen liegt vor?

- Known Ciphertext (KC)
 - Known Plaintext (KP)
 - Chosen Plaintext (CP)
- (a) Es steht das Verschlüsselungsverfahren zur Verfügung.
- (b) Es steht ein Stück Geheimtext zur Verfügung.
- (c) Es steht ein Stück Klartext und das dazu gehörende Stück Geheimtext zur Verfügung.

Aufgabe 2.1

Was ist ein symmetrisches Verschlüsselungsverfahren?

Aufgabe 2.2

Auf wie viele Arten können die 26 Zeichen des lateinischen Alphabets permutiert, d. h. umkehrbar eindeutig auf sich abgebildet werden?

Aufgabe 2.3

Dechiffriere den Geheimtext

HLQ XKU EHLN NROOHJL

wenn du weißt, dass die Verschlüsselung mit dem Cäsar-Verfahren durchgeführt wurde und der Text etwas mit dem Gymnasium in Stans zu tun hat.

Aufgabe 2.5

Warum ist eine monoalphabetische Verschlüsselung unsicher?

Aufgabe 2.6

Verschlüsse den Klartext KAFFEE mit der Vigenère-Verschlüsselung und dem Schlüssel GEHEIM. Verwende dazu das Vigenère-Quadrat.

Aufgabe 2.7

Wie kann man versuchen, die Schlüssellänge des Vigenère-Verfahrens zu bestimmen?

Aufgabe 2.8

Wie kann ein Vigenère-Chiffrierter Text entschlüsselt (geknackt) werden, wenn die Schlüsselwortlänge n bekannt ist?

Aufgabe 2.9

- (a) Nenne mindestens einen wesentlichen Nachteil des One Time Pad-Verfahrens?
- (b) Wovon hängt die Sicherheit des One Time Pad-Verfahrens ab?

Aufgabe 3.1

Wahr oder falsch?

- (a) $113 \equiv 17 \pmod{8}$
- (b) $-352\,989 \equiv 724\,692 \pmod{2}$
- (c) $107\,032 \equiv 0 \pmod{3}$

Aufgabe 3.2

Berechne das Resultat in der Restklassenmenge \mathbb{Z}_9 , sofern es überhaupt definiert ist. Die Kennzeichnung der Restklassen kann weggelassen werden.

- (a) $7 + 6$
- (b) $5 - 8$
- (c) $3 \cdot 7$
- (d) $1 : 4$
- (e) $5 : 6$
- (f) 3^{29}

Aufgabe 3.3

Berechne $(25 \cdot 13 + 44 \cdot 8) \pmod{7}$.

Aufgabe 3.12

Berechne mit Hilfe der Rechenregeln.

- (a) $\varphi(47)$ (c) $\varphi(27)$ (e) $\varphi(77)$ (g) $\varphi(120)$
(b) $\varphi(2^4)$ (d) $\varphi(3 \cdot 5)$ (f) $\varphi(50)$ (h) $\varphi(10000)$

Aufgabe 3.13

Berechne mit dem Square-and-Multiply-Algorithmus und folgender Tabelle.

- (a) $13^{10} \bmod 19$ (b) $3^{16} \bmod 19$

\times	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
1	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
2	2	4	6	8	10	12	14	16	18	1	3	5	7	9	11	13	15	17
3	3	6	9	12	15	18	2	5	8	11	14	17	1	4	7	10	13	16
4	4	8	12	16	1	5	9	13	17	2	6	10	14	18	3	7	11	15
5	5	10	15	1	6	11	16	2	7	12	17	3	8	13	18	4	9	14
6	6	12	18	5	11	17	4	10	16	3	9	15	2	8	14	1	7	13
7	7	14	2	9	16	4	11	18	6	13	1	8	15	3	10	17	5	12
8	8	16	5	13	2	10	18	7	15	4	12	1	9	17	6	14	3	11
9	9	18	8	17	7	16	6	15	5	14	4	13	3	12	2	11	1	10
10	10	1	11	2	12	3	13	4	14	5	15	6	16	7	17	8	18	9
11	11	3	14	6	17	9	1	12	4	15	7	18	10	2	13	5	16	8
12	12	5	17	10	3	15	8	1	13	6	18	11	4	16	9	2	14	7
13	13	7	1	14	8	2	15	9	3	16	10	4	17	11	5	18	12	6
14	14	9	4	18	13	8	3	17	12	7	2	16	11	6	1	15	10	5
15	15	11	7	3	18	14	10	6	2	17	13	9	5	1	16	12	8	4
16	16	13	10	7	4	1	17	14	11	8	5	2	18	15	12	9	6	3
17	17	15	13	11	9	7	5	3	1	18	16	14	12	10	8	6	4	2
18	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1

Aufgabe 3.14

Wie viele Schlüssel sind bei einem symmetrischen Verschlüsselungsverfahren nötig, wenn 41 Teilnehmer eines Kommunikationsnetzes mit jedem anderen Teilnehmer separat verschlüsselt kommunizieren möchten?

Aufgabe 3.15

Beschreibe allgemein, worum es beim Diffie-Hellman-Merkle-Schlüsselaustausch geht.

Aufgabe 3.16

Zeige schrittweise, wie der Diffie-Hellman-Merkle-Schlüsselaustausch konkret funktioniert, wenn folgende Parameter verwendet werden. Welche dieser Zahlen dürfen nicht öffentlich erscheinen?

- Primzahl $p = 13$
- Primitivwurzel $g = 2$
- Exponent von Alice $a = 4$
- Exponent von Bob $b = 5$

Aufgabe 3.17

Worauf beruht die Sicherheit des Diffie-Hellman-Merkle-Schlüsselaustauschs?

Aufgabe 3.18

- (a) Beschreibe ein Szenario, mit dem der Diffie-Hellman-Schlüsselaustausch angegriffen werden kann.
- (b) Wie können sich Alice und Bob grundsätzlich gegen diese Art von Angriff schützen?

Aufgabe 3.19

Erkläre in wenigen Sätzen, worum es beim RSA-Verfahren geht.

Aufgabe 3.20

Worauf beruht die Sicherheit des RSA-Verfahrens?

Aufgabe 3.21

Bestimme den $\text{ggT}(a, b)$ mit dem euklidischen Algorithmus.

- (a) $a = 258, b = 45$
- (b) $a = 392, b = 135$

Aufgabe 3.22

Bestimme eine Darstellung von $\text{ggT}(a, b) = x \cdot a + y \cdot b$ mit Hilfe des erweiterten euklidischen Algorithmus. ($a, b, x, y \in \mathbb{Z}$)

- (a) $a = 36, b = 15$
- (b) $a = 47, b = 20$

Aufgabe 3.23

Bestimme die modulare multiplikative Inverse der Zahl a in \mathbb{Z}_p^* mit Hilfe des erweiterten euklidischen Algorithmus.

- (a) $p = 7, a = 3$
- (b) $p = 19, a = 11$

Aufgabe 3.24

- (a) Wie lautet der Satz von Euler-Fermat?
- (b) Überprüfe seine Gültigkeit anhand von selber gewählten Zahlen.

Aufgabe 3.25

Für das RSA-Verfahren, wurden der öffentliche Schlüssel $(e, n) = (3, 33)$ und der private Schlüssel $(d, n) = (7, 33)$ erzeugt.

- (a) Verschlüsse die Nachricht $m = 2$ mit dem RSA-Verfahren.
- (b) Entschlüsse die Nachricht $c = 10$ mit dem RSA-Verfahren.
- (c) Signiere die Nachricht $m = 5$ mit dem RSA-Verfahren.

Verwende, falls nötig eine Multiplikationstabelle für \mathbb{Z}_{33}^* .

Aufgabe 3.26

Zeige, wie beim RSA-Verfahren der geheime Schlüssel d aus den Primzahlen $p = 5$, $q = 11$ und dem öffentlichen Schlüssel $e = 7$ berechnet wird.

Aufgabe 3.27

Zeige, wie beim RSA-Verfahren der geheime Schlüssel d aus den Primzahlen $p = 11$, $q = 17$ und dem öffentlichen Schlüssel $e = 3$ berechnet wird.