Kryptologie

Maturavorbereitung

Aufgabe 1

Was ist Kryptologie und mit welchen Teildisziplinen befasst sie sich?

Aufgabe 1

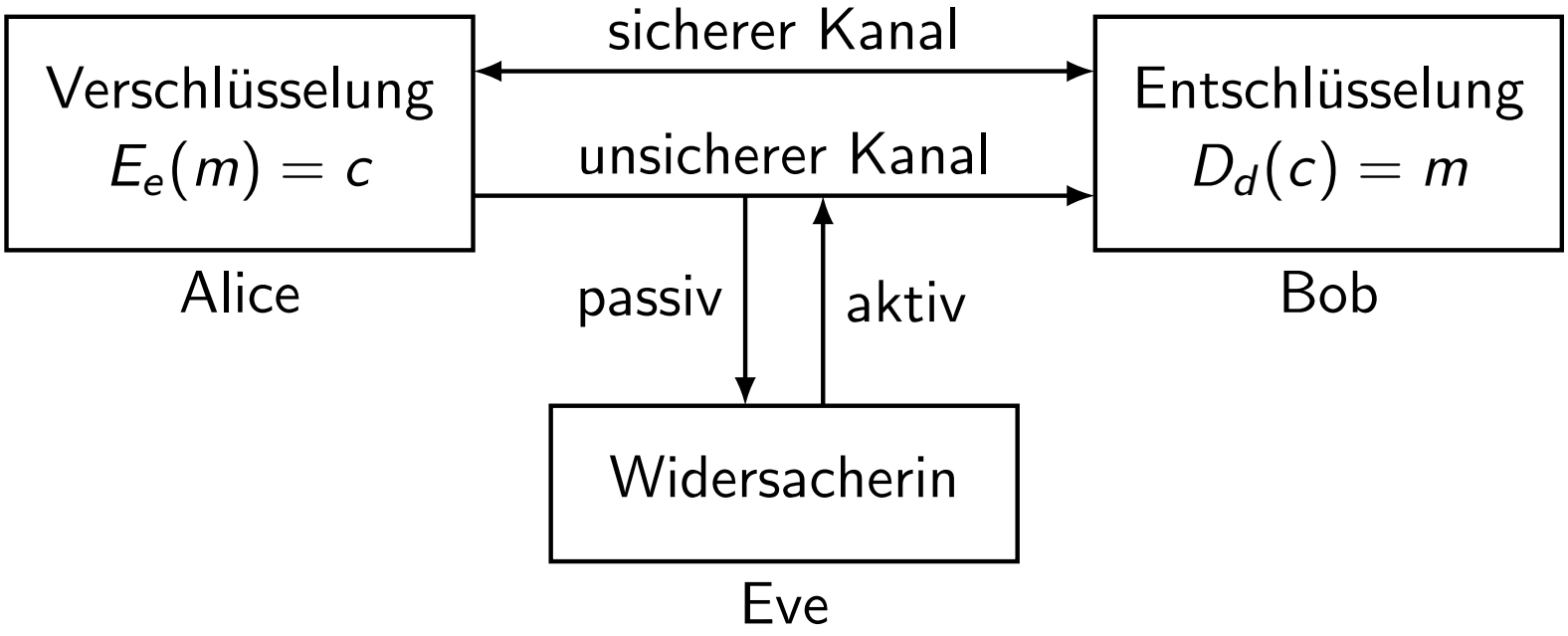
Kryptologie ist ursprünglich die Wissenschaft die sich mit der Verschlüsselung und Entschlüsselung von Informationen befasst. Neben der Kryptographie (Entwicklung kryptographischer Systeme) und der Kryptoanalyse (Untersuchen der Sicherheit kryptographischer Systeme) befasst sich die Kryptologie seit dem Computerzeitalter mit weiteren Aufgaben:

- *Vertraulichkeit:* Der Schutz von Informationen vor unbefugtem Zugriff (typischerweise durch Verschlüsselung)
- *Integrität:* Die Gewährleistung, dass die Daten während der Übertragung oder Speicherung nicht verändert wurden. (typischerweise durch Hash-Funktionen)
- *Authentifikation (oder Authentifizierung):* Der Prozess, durch den die Identität eines Benutzers oder Systems überprüft wird (Passwörter, digitale Signaturen, . . .)
- *Verbindlichkeit:* Der Urheber der Daten oder Absender einer Nachricht soll nicht in der Lage sein, seine Urheberschaft zu bestreiten.

Aufgabe 2

Skizziere schematisch die Situation, in der sich zwei Kommunikationspartner befinden, die eine vertauliche Informationen austauschen wollen.

Aufgabe 2



E	Encryption function
D	Decryption function
e	Dncryption key
d	Decryption key
m	Message (Klartext)
c	Ciphertext (Geheimtext)

Aufgabe 3

Beschreibe das Prinzip von Kerckhoffs.

Aufgabe 3

Das Prinzip von Kerckhoffs (1835–1903) besagt, dass die Sicherheit eines kryptographischen Systems nicht von der Geheimhaltung des Algorithmus abhängen sollte, sondern ausschliesslich von der Geheimhaltung des Schlüssels.

Aufgabe 4

Was ist das charakteristische Merkmal symmetrischer kryptographischer Verfahren?

Aufgabe 4

Bei symmetrschen kryptoraphischen Verfahren wird der gleiche geheime Schlüssel zum Verschlüsseln als auch zum Entschlüsseln der Daten verwendet.

Aufgabe 5

(a) Was ist eine monoalphabetische Substitutionschiffre?

(b) Erörtere die Sicherheit dieser Art der Verschlüsselung?

Aufgabe 5

(a) Was ist eine monoalphabetische Substitutionschiffre?

Das sind Verschlüsselungsverfahren, bei dem jedes Zeichen des Alphabets immer auf dasselbe Zeichen abgebildet wird.

Aufgabe 5

(a) Was ist eine monoalphabetische Substitutionschiffre?

Das sind Verschlüsselungsverfahren, bei dem jedes Zeichen des Alphabets immer auf dasselbe Zeichen abgebildet wird.

(b) *Sicherheit:* Obwohl bei einem Alphabet mit 26 Zeichen $(26! - 1)$ verschiedene Schlüssel möglich sind, stellen mononalphabetische Chiffrierungen für professionelle Kryptoanalytiker mit Computerunterstützung kein Hindernis dar, sofern ausreichend Geheimtext vorhanden ist. Der Grund dafür ist, dass sich die für eine Sprache charakteristischen Buchstabenhäufigkeiten durch eine Permutation der Zeichen nicht ändern.

Aufgabe 6

Nennen Sie ein Beispiel für eine monographisch-monoalphabetische Substitutionschiffre.

Aufgabe 6

Cäsar-Chiffre

Aufgabe 7

Was ist eine polyalphabetische Substitutionschiffre?

Aufgabe 7

Eine polyalphabetische Substitutionschiffre ist ein Verschlüsselungsverfahren, bei dem ein Zeichen des Alphabets auf wechselnde Zeichen abgebildet wird.

Aufgabe 29

Sie kommen in den Besitz des folgenden Geheimtexts, von dem Sie wissen, dass er mit dem Vigenère-Verfahren verschlüsselt wurde.

```
01234567890123456789012345 67
PHSRMZNHZHSRMZRIVQXWVQLSAHSR
```

Die über den Zeichen stehenden Ziffern dienen dazu, die Zeichenpositionen leichter erkennbar zu machen.

Ermitteln Sie die Kandidaten für die Schlüsselwortlänge.

Aufgabe 29

```
01234567890123456789012345 67
PHSRMZNHZHSRMZRIVQXWVQLSAHSR
```

Trigramm	Positionen	Abstände
HSR	1, 9, 25	Vielfache von 8

Also ist die Schlüsselwortlänge vermutlich ein Teiler von 8; also 8, 4 oder 2.

In der Tat wurde die Nachricht HUNDEMITRUNDEMMUNDSINDGESUND mit dem Schlüssel INFO verschlüsselt.

Aufgabe 9

Beschreiben Sie die Vigenère-Chiffere und diskutieren Sie ihre Sicherheit.

Aufgabe 9

Bei der *Vigenère-Chiffere:* wird der Schlüssel so lange wiederholt, bis er mindestens so lange wie der Klartext ist. Dann wird er zeichenweise zum Klartext addiert (modulo der Alphabetlänge). Im besten Fall wird jeder Klartextbuchstabe auf einen anderen Geheimtextbuchstaben abgebildet.

Klartext	SHE	SELLS	SEA	SHELLS	BY	THE	SEASHORE
+ Schlüssel	KEY	KEYKE	YKE	YKEYKE	YK	EYK	EYKEYKEY
Geheimtext	CLC	CIJVW	QOE	QRIJVW	ZI	XFO	WCKWFYVC

Je öfters der Schlüssel wiederholt wird, umso wahrscheinlicher ist es, dass eine kurze Folge von Klartextbuchstaben mit derselben Folge von Schlüsselbuchstaben zum gleichen Klartext verschlüsselt wird. Hat man mehrere solche Stellen im Geheimtext identifiziert, kann man mit dem grössten gemeinsamen Teiler der Abstände dieser Stellen die Schlüsselwortlänge schätzen. Dann weiss man, welche Zeichen mit demselben Schlüsselwortbuchstaben verschlüsselt wurden und kann auf diesen Zeichenmengen eine Buchstabenhäufigkeitsanalyse durchführen.

Aufgabe 10

Beschreiben Sie das One-Time-Pad-Verfahren und diskutieren Sie dessen Sicherheit.

Aufgabe 10

One-Time-Pad (OTP): Man wählt man einen Schlüssel aus zufälligen Zeichen, der genau so lange wie die Nachricht ist und addiert zu jedem Zeichen des Klartextexts das Zeichen des entsprechenden Schlüsselzeichens (modulo der Alphabetlänge).

Sicherheit: Claude Shannon (1916–2001) wies nach, dass OTP perfekte Sicherheit aufweist, wenn der Schlüssel gleichverteilt zufällig gewählt wurde und kein zweites Mal verwendet wird.

Aufgabe 11

Wandle die Nachricht $m = \texttt{MMS}$ gemäss folgender Codetabelle in eine Bitfolge um, verschlüssele sie durch XOR-Verknüpfung mit dem Schlüssel $k = 110111111001001$ und stelle den Geheimtext wieder mit den urspünglichen Zeichen dar.

A=00000	B=00001	C=00010	D=00011
E=00100	F=00101	G=00110	H=00111
I=01000	J=01001	K=01010	L=01011
M=01100	N=01101	O=01110	P=01111
Q=10000	R=10001	S=10010	T=10011
U=10100	V=10101	W=10110	X=10111
Y=11000	Z=11001	!=11010	?=11011
+=11100	*=11101	@=11110	#=11111

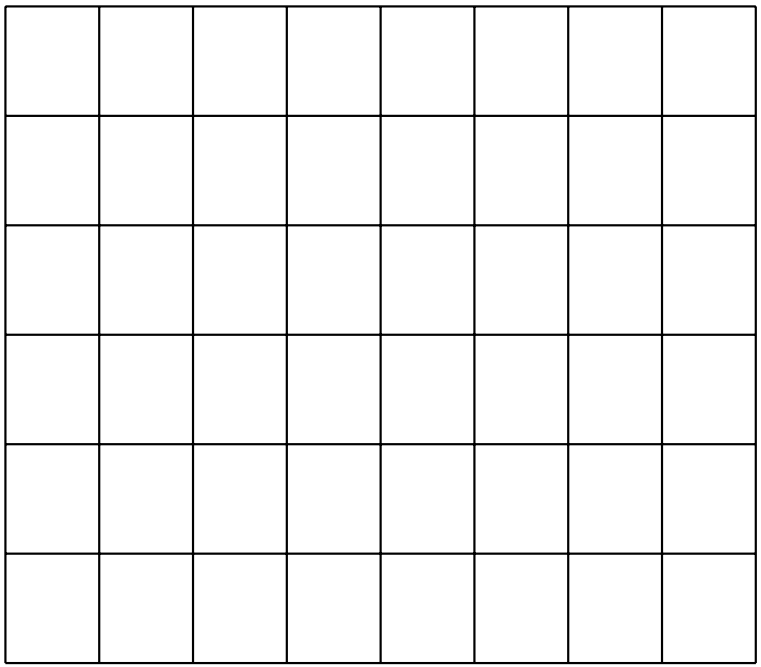
Aufgabe 11

A=00000	B=00001	C=00010	D=00011
E=00100	F=00101	G=00110	H=00111
I=01000	J=01001	K=01010	L=01011
M=01100	N=01101	O=01110	P=01111
Q=10000	R=10001	S=10010	T=10011
U=10100	V=10101	W=10110	X=10111
Y=11000	Z=11001	!=11010	?=11011
+=11100	*=11101	@=11110	#=11111

$$
\begin{array}{lllll}
\texttt{MMS} \Rightarrow & 01100 & 01100 & 10010 & \\
\oplus & 11011 & 11110 & 01001 & k \\
\hline
 & 10111 & 10010 & 11011 & \Rightarrow \texttt{XS?}
\end{array}
$$

Aufgabe 30

Verschlüssle den Text `BRUTUSISTDERVERRAETER` mit der Transpositionschiffre und dem Schlüsselwort `ANANAS`.



Aufgabe 30

BRUTUSISTDERVERRAETER

0	3	1	4	2	5		
A	**N**	**A**	**N**	**A**	**S**		
B	R	U	T	U	S		
I	S	T	D	E	R		
V	E	R	R	A	E		
T	E	R					

$\Rightarrow$ BIVTUTRRUEARSEETDRSRE

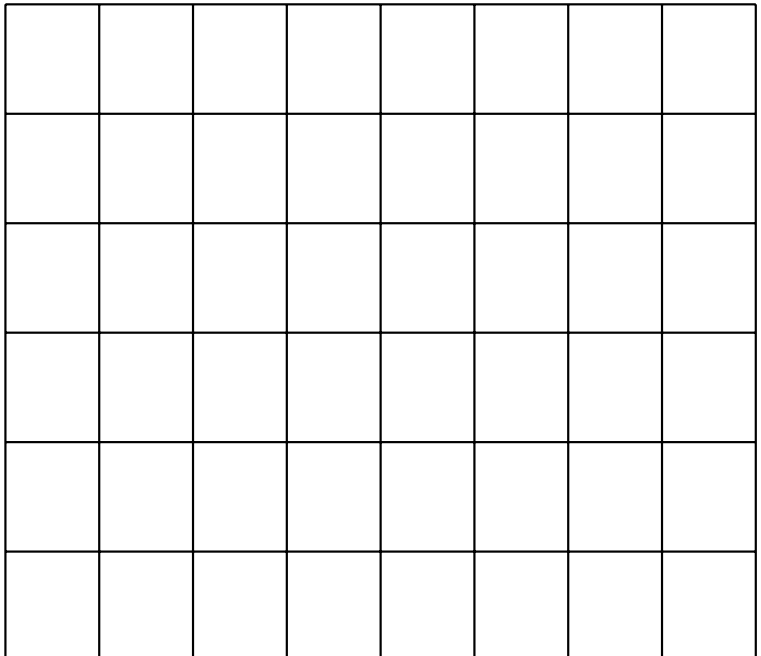
Aufgabe 31

Du hast mit jemandem das Schlüsselwort `HAMSTER` vereinbart und bekommst den Geheimtext

`RMAEF TALED TNPFO ZFR`

der mit der einfachen Transpositionschiffre verschlüsselt wurde. Zur Verschleierung der Schlüsselwortlänge wurden die Zeichen des Geheimtexts in 5er-Gruppen gegliedert.

Entschlüssle die Nachricht und bestimme den Treffpunkt.



Aufgabe 31

Geheimtext: `RMAEF TALED TNPFO ZFR` (18 Zeichen)

Schlüssel: `HAMSTER` (7 Zeichen)

Anzahl Zeilen: $\lceil 18/7 \rceil = 3$

Anzahl lange Spalten: $\lceil 18 \bmod 7 \rceil = 4$

2	0	3	5	6	1	4	
H	**A**	**M**	**S**	**T**	**E**	**R**	
T	R	E	F	F	E	N	
A	M	D	O	R	F	P	
L	A	T	Z				

$\Rightarrow$ `TREFFENAMDORFPLATZ`

Aufgabe 16

Beschreibe das Konzept asymmetrischer Kryptosysteme.

Aufgabe 16

Bei einem asymmetrischen Kryptosystem besitzt jeder Teilnehmer ein Schlüsselpaar, das aus einem öffentlichen Schlüssel k_e und einem (geheimen) privaten Schlüssel k_d besteht.

Diese Schlüssel sind so konstruiert, dass man aus dem öffentlichten Schlüssel nicht den geheimen privaten Schlüssel berechnen kann und dass die Anwendung beider Schlüssel (in jeder Reihenfolge) wieder die ursprüngliche Nachricht erzeugt.

Mit dem öffentliche Schlüssel kann man Nachrichten verschlüsseln und an den Herausgeber des Schlüssel senden. Nur dieser kann die verschlüsselte Nachricht mit seinem privaten Schlüssel wieder entschlüssseln.

Umgekehrt kann man mit seinem privaten Schlüssel ein Dokument (oder einen Hashwert davon) verschlüsseln. Durch Entschlüsseln mit dem öffentlichen Schlüssel kann der Empfänger erkennen, ob das Dokument manipuliert wurde.

Aufgabe 19

Stelle $(\mathbb{Z}_6, \times)$ tabellarisch dar. Welche Elemente in $(\mathbb{Z}_6, \times)$ sind invertierbar?

Aufgabe 19

$\times$	**0**	**1**	**2**	**3**	**4**	**5**
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

Nur die Elemente 1 und 5 sind in $\mathbb{Z}_6$ invertierbar.

Aufgabe 20

Stelle $\mathbb{Z}_8^*$ tabellarisch dar.

Aufgabe 20

$\mathbb{Z}_8^*$:

$\times$	**1**	**3**	**5**	**7**
1	1	3	5	7
3	3	1	7	5
5	5	7	1	3
7	7	5	3	1

Aufgabe 22

Prüfe, ob

(a) $a = 2$

(b) $b = 3$

ein Generator von $\mathbb{Z}_7$ ist.

Aufgabe 22

(a) $2^1 = 2,\ 2^2 = 4,\ 2^3 = 1 \quad \Rightarrow \quad$ Nein

(b) $3^1 = 3,\ 3^2 = 2,\ 3^3 = 6,\ 3^4 = 4,\ 3^5 = 5,\ 3^6 = 1 \quad \Rightarrow \quad$ Ja

Aufgabe 23

(a) Löse die Gleichung $2^a = 1$ in $\mathbb{Z}_5$.

(b) Wie wird die Lösung dieser Art von Gleichung genannt?

Aufgabe 23

(a) Löse $2^a = 1$ in $\mathbb{Z}_5$.

$$2^2 \bmod 5 = 4$$
$$2^3 \bmod 5 = 3$$
$$2^4 \bmod 5 = 1 \quad \Rightarrow \quad a = 4$$

Aufgabe 23

(a) Löse $2^a = 1$ in $\mathbb{Z}_5$.

$$2^2 \bmod 5 = 4$$
$$2^3 \bmod 5 = 3$$
$$2^4 \bmod 5 = 1 \quad \Rightarrow \quad a = 4$$

(b) diskreter Logarithmus

Aufgabe 24

Berechne $3^9 \bmod 11$ mit Square and Multiply.

Aufgabe 24

$3^9 = 3^{1+8} = 3^1 \cdot 3^8$

Square:	Multiply: $x = 1$
$3^1 \bmod 11 = 3$	$x = (1 \cdot 3) \bmod 11 = 3$
$3^2 \bmod 11 = 9 \bmod 11 = 9$	
$3^4 \bmod 11 = 81 \bmod 11 = 4$	
$3^8 \bmod 11 = 16 \bmod 11 = 5$	$x = (3 \cdot 5) \bmod 11 = 4$

Aufgabe 25

Erkläre, wie der Diffie-Hellman-Merkle-Schlüsselaustausch funktioniert und worin seine Sicherheit besteht.

Aufgabe 25

1. Alice und Bob einigen sich [öffentlich] auf eine grosse Primzahl p und einen Generator g von $\mathbb{Z}_p^*$.
2. (a) Alice wählt eine Zahl $1 < a < p$, die sie geheim hält, berechnet damit
   $A = g^a \bmod p$ und sendet A an Bob.
   (b) Bob wählt eine Zahl $1 < b < p$, die er geheim hält, berechnet damit
   $B = g^b \bmod p$ und sendet B an Alice.
3. (a) Alice berechnet die Zahl $K_a = B^a \bmod p$.
   (b) Bob berechnet die Zahl $K_b = A^b \bmod p$.
4. Wegen

$$K_a \equiv B^a \equiv (g^b)^a \equiv g^{b \cdot a} \equiv g^{a \cdot b} \pmod{p} \quad \text{und}$$

$$K_b \equiv A^b \equiv (g^a)^b \equiv g^{a \cdot b} \pmod{p}$$

gilt $K_a \equiv K_b \pmod{p}$. Somit haben Alice und Bob dieselbe grosse Zahl, die sie als Schlüssel für eine Kommunikation mit einem symmetrischen Verschlüsselungsverfahren verwenden können.

Sicherheit des Verfahrens: Die Widersacherin Eve kennt die Primzahl p und den Generator g von $\mathbb{Z}_p^*$ (Schritt 1).

Sie kennt auch die Potenzen $A = g^a$ und $B = g^b$ (Schritt 2a, 2b).

Da es nach heutigem Wissensstand keinen effizienten Algorithmus gibt, um aus den Zahlen A und B sowie der Basis g die Exponenten zu bestimmen (Problem des diskreten Logarithmus), kann sie die Rechnungen in Schritt 3 nicht nachvollziehen, um ebenfalls den gemeinsamen Schlüssel von Alice und Bob zu berechnen.

Aufgabe 26

Alice und Bob einigen sich auf die Primzahl $p = 17$ und den Generator $g = 10$. Alice wählt die Zahl $a = 2$ und Bob die Zahl $b = 16$. Wie lautet der gemeinsame Schlüssel aufgrund des Diffie-Hellman-Schlüsselautauschprotokolls?

Verwende den Taschenrechner so weit es geht.

Aufgabe 26

1. $p = 19$; $g = 10$ ist ein Generator von $\mathbb{Z}_{19}^*$
2. (a) Alice wählt $a = 2$, berechnet $A = 10^2 \bmod 19 = 5$ und sendet $A = 5$ an Bob.
   (b) Bob wählt $b = 16$, berechnet damit
   $B = 10^{16} \bmod 19$
   $10^2 \bmod 19 = 5$
   $10^4 \bmod 19 = (10^2)^2 \bmod 19 = 5^2 \bmod 19 = 6$
   $10^8 \bmod 19 = (10^4)^2 \bmod 19 = 6^2 \bmod 19 = 17$
   $10^{16} \bmod 19 = (10^8)^2 \bmod 19 = 17^2 \bmod 19 = 11$
   und sendet B an Alice.
3. (a) Alice berechnet $K_a = B^a = 11^2 \bmod 19 = 7$
   (b) Bob berechnet $K_b = A^b = 5^{16} \bmod 19 = 16$
4. Der Schlüssel lautet $K = 11$.