Transpositionsverschlüsselung (1/5)

KURZ ERKLÄRT Bei einer Transposition werden die Zeichen eines Klartexts nach einer festgelegten Regel umgeordnet, aber nicht ersetzt. Die Buchstabenhäufigkeiten bleiben dadurch erhalten. Das macht historische Transpositionsverfahren anschaulich, aber für moderne Sicherheitsanforderungen ungeeignet.

Aufgabe 1
Dir ist dieser Pergamentstreifen in die Hände gefallen, der eine als Skytale verschlüsselte Botschaft trägt.
Du weißt natürlich nicht, wie dick der Stab war, den der griechische Dramatiker Epicharmos vor 2500 Jahren beim Verschlüsseln seiner Botschaft verwendet hat.
Brich die Verschlüsselung durch Probieren, indem du die Botschaft in Tabellen mit zwei, drei oder mehr Zeilen notierst.

T
I
D
W
A
S
A
A
L
T
S
S
E
D
Z
Z
N
A
W
U
T
S
E
L
H
B
I
E
A
E
T
R
B
S
E
N
E
T
E
E
N
E
T
N

……
……

……
……
……

……
……
……
……

Transpositionsverschlüsselung (2/5)

Fortsetzung Aufgabe 1

T
I
D
W
A
S
A
A
L
T
S
S
E
D
Z
Z
N
A
W
U
T
S
E
L
H
B
I
E
A
E
T
R
B
S
E
N
E
T
E
E
N
E
T
N

.....
.....
.....
.....
.....
.....

Aufgabe 2
Beschreibe, wie das Ver- und Entschlüsseln einer Skytale funktioniert.
Was dient dabei als Schlüssel?

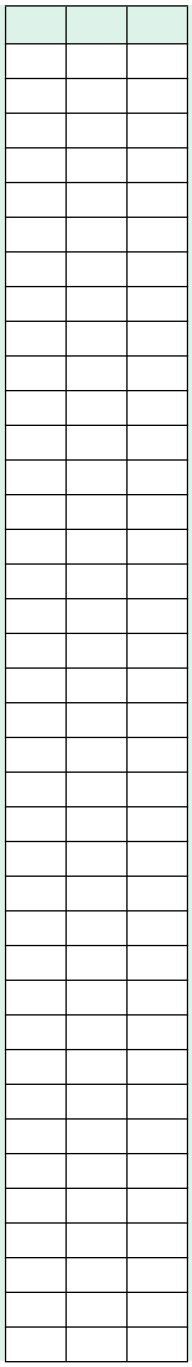
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....

Transpositionsverschlüsselung (3/5)

Aufgabe 4
Verschlüssele die Aussage des früheren Fußball-Bundestrainers Josef „Sepp" Herberger (1897 – 1977)
„Der Ball ist rund, und ein Spiel dauert 90 Minuten."
mit der Gartenzaun-Verschlüsselung über fünf Zeilen.
DERBALLISTRUNDUNDEINSPIELDAUERTNEUNZIGMINUTEN

Transpositionsverschlüsselung (4/5)

Aufgabe 5
Verschlüssele die Aussage des deutschen Journalisten und Schriftstellers Kurt Tucholsky (1890 – 1935)
„Der eigene Hund macht keinen Lärm, er bellt nur."
mit der Gartenzaun-Verschlüsselung über drei Zeilen.
DEREIGENEHUNDMACHTKEINENLAERMERBELLTNUR



Transpositionsverschlüsselung (5/5)

Aufgabe 6
Entschlüssele dieses mit der Gartenzaun-Verschlüsselung über vier Zeilen verschlüsselte Zitat des deutschen Schriftstellers Theodor Fontane (1819 – 1998)
MHGNIEWUAEAELEDDENITEAFTNHENABASSNHEGNGHCHUSOREE

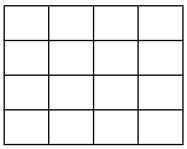
.....

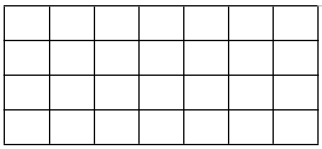
.....

Aufgabe 7
Entschlüsse diese mit der Gartenzaun-Verschlüsselung über sechs Zeilen verschlüsselte Aussage des ehemaligen deutschen Fußballspielers Mehmet Scholl zu seinem Urlaubsziel:
IREIADCIGDNVENCOEHEENS–LTHARFGNIUNLHKDSLEDOEEECAAOIWDIN
Hinweis: Der Bindestrich zählt als Buchstabe

.....

.....





Vigenère-Verschlüsselung (1/2)

KURZ ERKLÄRT Die Vigenère-Chiffre verwendet ein wiederholtes Schlüsselwort. Jeder Schlüsselbuchstabe bestimmt eine andere Verschiebung des zugehörigen Klartextbuchstabens. Buchstaben werden dazu als Zahlen von 0 bis 25 behandelt und die Ergebnisse modulo 26 berechnet.

Aufgabe 1

Verschlüssele diese Orte mit dem Schlüsselwort ROM.

MAILAND
BOLOGNA

Schlüssel							
Klartext	M	A	I	L	A	N	D
Geheimtext							

Schlüssel							
Klartext	B	O	L	O	G	N	A
Geheimtext							

Schlüssel							
Klartext	T	U	R	I	N		
Geheimtext							

TURIN
PALERMO

Schlüssel							
Klartext	P	A	L	E	R	M	O
Geheimtext							

Schlüssel							
Klartext	N	E	A	P	E	L	
Geheimtext							

Schlüssel							
Klartext	V	E	R	O	N	A	
Geheimtext							

NEAPEL
VERONA

Aufgabe 2

Welche Alpenberge sind hier verschlüsselt? (Schlüsselwort: GIPFEL)

FCVXTTZHT
SIIYICNWGS

Schlüssel										
Klartext	F	C	V	X	T	T	Z	H	T	
Geheimtext										

Schlüssel										
Klartext	S	I	I	Y	I	C	N	W	G	S
Geheimtext										

Schlüssel										

CIIEQLTV
PCCLJCGC

Schlüssel										
Klartext	P	C	C	L	J	C	G	C		
Geheimtext										

Schlüssel										
Klartext	C	Q	A	I	W	A	O	B	O	J
Geheimtext										

Schlüssel										

CQAIWAOBOJ
TMQJPSUZC

Schlüssel										

Klartext	C	I	I	E	Q	L	T	V		
Geheimtext										

Klartext	T	M	Q	J	P	S	U	Z	C	
Geheimtext										

Vigenère-Verschlüsselung (2/2)

Aufgabe 3

Verschlüssele dieses Zitat, das dem Schriftsteller Mark Twain (1835 – 1910) zugeschrieben wird: „Das Geheimnis des Vorankommens ist das Anfangen.“ Verwende das Schlüsselwort GEHEIM.

DASGE HEIMN ISDES VORAN KOMME NSIST DASAN FANGE N

Schlüssel																				
Klartext																				
Geheimtext																				

Schlüssel																					
Klartext																					
Geheimtext																					

Aufgabe 4

Entschlüssele die Aussage von Napoléon Bonaparte (1769 – 1821) über das Wetter in Deutschland. Verwende das Schlüsselwort FRANKREICH.

IZEQO LXAEO JEHNL VRAGJ MJMBX RXMYP SKEEE EHAGJ
MJMBX RXMML NEEAC FQUGY

Schlüssel																				
Klartext																				
Geheimtext																				

Schlüssel																				
Klartext																				
Geheimtext																				

Schlüssel																				
Klartext																				
Geheimtext																				

One-Time-Pad-Verfahren (OTP) (1/3)

KURZ ERKLÄRT Ein One-Time-Pad ist nur dann perfekt sicher, wenn der Schlüssel wirklich zufällig, mindestens so lang wie die Nachricht, vollständig geheim und genau einmal verwendet ist. In der Praxis ist vor allem die sichere Verteilung großer Schlüsselmengen schwierig.

Aufgabe 1

Welche Bedingungen müssen erfüllt sein,
damit das One-Time-Pad-Verfahren sicher ist?

Aufgabe 2

Warum hat sich das One-Time-Pad-Verfahren trotz seiner Sicherheit
nicht als Standardverfahren durchgesetzt?

Aufgabe 3

Wie lang darf eine Nachricht sein, die man nach dem One-Time-Pad-Verfahren
mit diesem Schlüssel verschlüsseln möchte?

AQUNW SRBJP AIYJW OWTXM UMUCF FDGOU

One-Time-Pad-Verfahren (OTP) (2/3)

Aufgabe 4

Welche Inseln sind hier verschlüsselt?

Geheimtext	Schlüssel
DYPFOCAL	RYEUALYL
RZFWIOKUI	KRCTEBSQE
DAZGTMVAA	LAIDLZNWN
MEHOSKFWPHK	UPZVTJBFJDX

Schlüssel											
Klartext											
Geheimtext											

Schlüssel											
Klartext											
Geheimtext											

Schlüssel											
Klartext											
Geheimtext											

Schlüssel											
Klartext											
Geheimtext											

One-Time-Pad-Verfahren (OTP) (3/3)

Aufgabe 5

Rekonstruiere für beide Klartext-Geheimtext-Paare den Schlüssel.
Entsprechen die Schlüssel den Regeln des One-Time-Pad-Verfahrens?

Schlüssel									
Klartext	**D**	**A**	**T**	**E**	**N**	**B**	**A**	**N**	**K**
Geheimtext	S	R	H	X	B	L	O	Y	V

Schlüssel											
Klartext	**H**	**E**	**X**	**A**	**D**	**E**	**Z**	**I**	**M**	**A**	**L**
Geheimtext	S	J	R	W	I	D	Q	I	F	U	A

Aufgabe 6

Der Geheimtext lautet MXKSNU. Begründe, warum es nicht möglich ist herauszufinden, welcher dieser vier Klartexte verschlüsselt wurde.

MONACO, KANADA, MEXIKO, BHUTAN

Advanced Encryption Standard (AES) (1/3)

KURZ ERKLÄRT AES ist eine moderne symmetrische Blockchiffre. Verschlüsselung und Entschlüsselung verwenden denselben geheimen Schlüssel. AES verarbeitet 128-Bit-Blöcke und unterstützt Schlüssel mit 128, 192 oder 256 Bit; für eine sichere Anwendung sind außerdem Betriebsmodus und Schlüsselverwaltung entscheidend.

Aufgabe 1
Führe die Methode „Add round key“ der Anfangsphase aus und addiere den
Klartext mit dem Anfangsschlüssel.
Wandle den Klartext SCHOKOLADENTORTE zunächst mit Hilfe des ASCII-Codes in Dezimalzahlen und nach dem Addieren in Hexadezimalzahlen um.

Klartext

S	K	D	O
C	O	E	R
H	L	N	T
O	A	T	E

Anfangsschlüssel

1a	1b	1c	1d
2a	2b	2c	2d
3a	3b	3c	3d
4a	4b	4c	4d

Klartext → Klartext dezimal + Anfangsschlüssel dezimal = Text nach Anfangsrunde dezimal

Klartext	Klartext dezimal		Anfangsschlüssel dezimal		Text nach Anfangsrunde dezimal	

↓ Anfangsschlüssel hexadez.

↓ Text nach Anfangsrunde hexadez.

Zeichen	dezimal
A	65
B	66
C	67
D	68
E	69
F	70
G	71
H	72
I	73
J	74
K	75
L	76
M	77
N	78
O	79
P	80
Q	81
R	82
S	83
T	84
U	85
V	86
W	87
X	88
Y	89
Z	90

dez.	HEX	dez.	HEX	dez.	HEX	dez.	HEX	dez.	HEX	dez.	HEX	dez.	HEX
0	00	32	20	64	40	96	60	128	80	160	a0	192	c0	224	e0
1	01	33	21	65	41	97	61	129	81	161	a1	193	c1	225	e1
2	02	34	22	66	42	98	62	130	82	162	a2	194	c2	226	e2
3	03	35	23	67	43	99	63	131	83	163	a3	195	c3	227	e3
4	04	36	24	68	44	100	64	132	84	164	a4	196	c4	228	e4
5	05	37	25	69	45	101	65	133	85	165	a5	197	c5	229	e5
6	06	38	26	70	46	102	66	134	86	166	a6	198	c6	230	e6
7	07	39	27	71	47	103	67	135	87	167	a7	199	c7	231	e7
8	08	40	28	72	48	104	68	136	88	168	a8	200	c8	232	e8
9	09	41	29	73	49	105	69	137	89	169	a9	201	c9	233	e9
10	0a	42	2a	74	4a	106	6a	138	8a	170	aa	202	ca	234	ea
11	0b	43	2b	75	4b	107	6b	139	8b	171	ab	203	cb	235	eb
12	0c	44	2c	76	4c	108	6c	140	8c	172	ac	204	cc	236	ec
13	0d	45	2d	77	4d	109	6d	141	8d	173	ad	205	cd	237	ed
14	0e	46	2e	78	4e	110	6e	142	8e	174	ae	206	ce	238	ee
15	0f	47	2f	79	4f	111	6f	143	8f	175	af	207	cf	239	ef
16	10	48	30	80	50	112	70	144	90	176	b0	208	d0	240	f0
17	11	49	31	81	51	113	71	145	91	177	b1	209	d1	241	f1
18	12	50	32	82	52	114	72	146	92	178	b2	210	d2	242	f2
19	13	51	33	83	53	115	73	147	93	179	b3	211	d3	243	f3
20	14	52	34	84	54	116	74	148	94	180	b4	212	d4	244	f4
21	15	53	35	85	55	117	75	149	95	181	b5	213	d5	245	f5
22	16	54	36	86	56	118	76	150	96	182	b6	214	d6	246	f6
23	17	55	37	87	57	119	77	151	97	183	b7	215	d7	247	f7
24	18	56	38	88	58	120	78	152	98	184	b8	216	d8	248	f8
25	19	57	39	89	59	121	79	153	99	185	b9	217	d9	249	f9
26	1a	58	3a	90	5a	122	7a	154	9a	186	ba	218	da	250	fa
27	1b	59	3b	91	5b	123	7b	155	9b	187	bb	219	db	251	fb
28	1c	60	3c	92	5c	124	7c	156	9c	188	bc	220	dc	252	fc
29	1d	61	3d	93	5d	125	7d	157	9d	189	bd	221	dd	253	fd
30	1e	62	3e	94	5e	126	7e	158	9e	190	be	222	de	254	fe
31	1f	63	3f	95	5f	127	7f	159	9f	191	bf	223	df	255	ff

Advanced Encryption Standard (AES) (2/3)

Aufgabe 2

Führe die Methode „Substitute bytes“ aus und ersetze die 16 Bytes des folgenden Blocks mit Hilfe der Byte-Ersetzungstabelle (S-Box).

a)									b)								
	1d	6e	84	71						20	43	b4	91				
	4d	03	35	25						33	5e	c0	1b				
	f1	36	04	75						70	36	ef	60				
	46	24	53	2f						cd	fc	1a	17				

Byte-Ersetzungstabelle (S-Box)

	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
0	63	7c	77	7b	f2	6b	6f	c5	30	01	67	2b	fe	d7	ab	76
1	ca	82	c9	7d	fa	59	47	f0	ad	d4	a2	af	9c	a4	72	c0
2	b7	fd	93	26	36	3f	f7	cc	34	a5	e5	f1	71	d8	31	15
3	04	c7	23	c3	18	96	05	9a	07	12	80	e2	eb	27	b2	75
4	09	83	2c	1a	1b	6e	5a	a0	52	3b	d6	b3	29	e3	2f	84
5	53	d1	00	ed	20	fc	b1	5b	6a	cb	be	39	4a	4c	58	cf
6	d0	ef	aa	fb	43	4d	33	85	45	f9	02	7f	50	3c	9f	a8
7	51	a3	40	8f	92	9d	38	f5	bc	b6	da	21	10	ff	f3	d2
8	cd	0c	13	ec	5f	97	44	17	c4	a7	7e	3d	64	5d	19	73
9	60	81	4f	dc	22	2a	90	88	46	ee	b8	14	de	5e	0b	db
a	e0	32	3a	0a	49	06	24	5c	c2	d3	ac	62	91	95	e4	79
b	e7	c8	37	6d	8d	d5	4e	a9	6c	56	f4	ea	65	7a	ae	08
c	ba	78	25	2e	1c	a6	b4	c6	e8	dd	74	1f	4b	bd	8b	8a
d	70	3e	b5	66	48	03	f6	0e	61	35	57	b9	86	c1	1d	9e
e	e1	f8	98	11	69	d9	8e	94	9b	1e	87	e9	ce	55	28	df
f	8c	a1	89	0d	bf	e6	42	68	41	99	2d	0f	b0	54	bb	16

Aufgabe 3

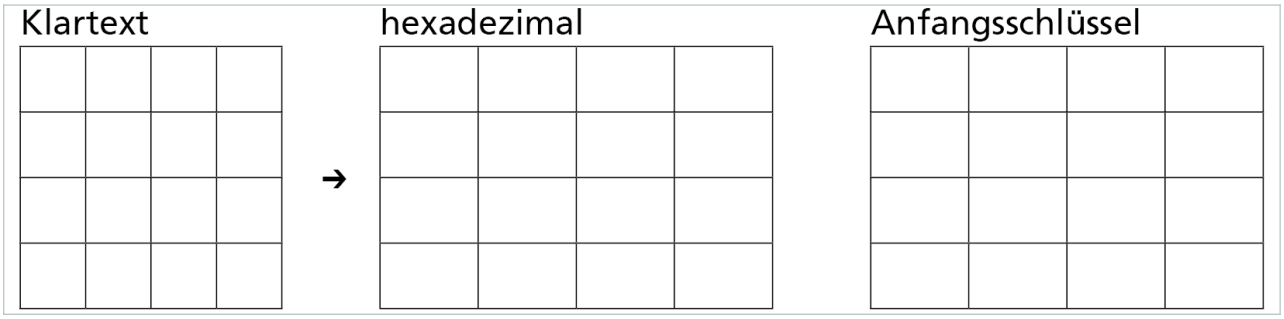
Führe die Methode „Shift rows“ an den folgenden Blöcken aus.

a)									b)								
	43	16	5d	de						2f	26	33	1d				
	89	82	31	86						ff	cf	1f	b1				
	91	08	5d	6f						b4	13	d5	f6				
	56	8d	b8	2d						7e	13	d6	1c				

Advanced Encryption Standard (AES) (3/3)

Aufgabe 4

- Wähle einen Text von 16 Zeichen, notiere ihn als Block
  und wandle ihn in Hexadezimalcode um.
- Wähle einen passenden Anfangsschlüssel.
- Rufe in CrypTool 1 den Rijndaelinspektor auf
  (Einzelverfahren > Visualisierung von Algorithmen > AES > Rijndael-Inspektor...).
- Verschlüssele und entschlüssele deinen Text.
  Hinweis: Der Klartext muss als Hexadezimalcode eingegeben werden.
- Betrachte die Umformungen, die durch die vier Methoden
  in den einzelnen Teilschritten am Block vorgenommen werden.



Kerckhoffs‘ Prinzip (1/2)

KURZ ERKLÄRT Nach Kerckhoffs soll ein Verschlüsselungssystem auch dann sicher bleiben, wenn Angreifer das Verfahren vollständig kennen. Geheim bleiben muss nur der Schlüssel. Öffentliche, intensiv geprüfte Algorithmen sind deshalb vertrauenswürdiger als Sicherheit, die allein auf einem geheimen Verfahren beruht.

Aufgabe 1

Welcher Grundsatz wird heute als Prinzip von Kerckhoffs bezeichnet?

Aufgabe 2

Warum haben Anwender (vermutlich zu Recht) wenig Vertrauen in Verschlüsselungsverfahren, deren Funktionsweise geheim ist?

Aufgabe 3

Welche praktischen Gründe sprechen auch in der modernen Kryptographie für Kerckhoffs‘ Prinzip?

Kerckhoffs‘ Prinzip (2/2)

Aufgabe 4

Betrachte unter den Verschlüsselungsverfahren, die du kennst, diejenigen, die auch der Kryptologe Auguste Kerckhoffs bereits kannte.

Beantworte für jedes dieser Verfahren diese zwei Fragen:

a)	Erfüllt das Verfahren den heute als Kerckhoffs’ Prinzip bekannten zweiten Grundsatz?	
	…… …… …… …… ……	…… …… …… …… ……

b)	Warum war Kerckhoffs der Meinung, dass das Verfahren seinen Grundsätzen nicht entspricht?	
	……	…… ……
	……	…… ……
	……	…… ……
	……	…… ……
	……	…… ……

Ende-zu-Ende-Verschlüsselung (1/2)

KURZ ERKLÄRT Bei Ende-zu-Ende-Verschlüsselung wird eine Nachricht auf dem Gerät des Absenders verschlüsselt und erst auf dem Gerät des Empfängers entschlüsselt. Transportserver erhalten nur den Geheimtext. Metadaten und ungeschützte Endgeräte können dennoch Sicherheitsrisiken darstellen.

Aufgabe 1

Stell dir vor, ihr würdet in eurer Klasse über einen Messengerdienst symmetrisch verschlüsselte Nachrichten austauschen.

Wie viele unterschiedliche symmetrische Schlüssel wären notwendig, damit jede Schülerin und jeder Schüler mit allen anderen Schülerinnen und Schülern deiner Klasse Nachrichten austauschen kann?

Aufgabe 2

Beschreibe den Ablauf der Ende-zu-Ende-Verschlüsselung bei einem Messengerdienst.

Ende-zu-Ende-Verschlüsselung (2/2)

Aufgabe 3

Warum kann der Betreiber des Messengerdienstes die auf seinem Server zwischengespeicherten Nachrichten nicht lesen?

Aufgabe 4

Worin besteht der wichtigste Unterschied zwischen symmetrischen und asymmetrischen Verschlüsselungen?

Hypertext Transfer Protocol Secure (HTTPS) (1/3)

KURZ ERKLÄRT HTTPS verbindet HTTP mit TLS. Ein Zertifikat hilft dem Browser, die Identität des Servers zu prüfen; anschließend wird die Verbindung verschlüsselt und gegen unbemerkte Veränderungen geschützt. Das Schlosssymbol bestätigt den geschützten Übertragungsweg, nicht automatisch die Seriosität einer Website.

Aufgabe 1

Beschreibe den Aufbau einer Verbindung zwischen einem Client (Webbrowser) und einem Webserver.

Aufgabe 2

Warum ist es sinnvoll, nach dem Aufbau der Verbindung mit Hilfe einer asymmetrischen Verschlüsselung für die Datenübertragung eine symmetrische Verschlüsselung zu verwenden?

Hypertext Transfer Protocol Secure (HTTPS) (2/3)

Aufgabe 3

Ruf die Website www.beispiel.de auf.
Probiere dabei beide Schreibweisen der URL aus:

http:// www.beispiel.de

https:// www.beispiel.de

Was fällt dir in der Adresszeile deines Browsers auf?

Aufgabe 4

Rufe die folgenden Webseiten auf und notiere die jeweiligen Zertifizierungsstellen.

https://www.scfreiburg.com	……
https://www.schwarzwald-tourismus.info/	……
https://www.google.com/	……
https://www.telekom.de	……
https://www.zu.de/ (Zeppelin Universität)	……

Hypertext Transfer Protocol Secure (HTTPS) (3/3)

Aufgabe 5

Öffne die Website deiner Schule.

a)	Verwendet die Website HTTPS? .....
b)	Welche Zertifizierungsstelle hat das Zertifikat ausgestellt? ....

Aufgabe 6

Ruf die Internetpräsenz von Baden-Württemberg mit der URL https://www.baden-wuerttemberg.de auf und lass dir das Zertifikat anzeigen.

Notiere die Zertifizierungsstelle und das Ende des Gültigkeitszeitraums des aktuellen Zertifikats.