AB 1 | Das Caesar-Verfahren

1) a) Nenne die möglichen Schlüssel.
   b) Beschreibe, wie man den zu einem Klarbuchstaben gehörenden Geheimbuchstaben erhält.
   c) Beschreibe, wie man den zu einem Geheimbuchstaben gehörenden Klarbuchstaben erhält.

2) a) Beurteile die Sicherheit dieses Verschlüsselungsverfahrens. Nenne dabei verschiedene Risiken.
   b) Beschreibe Möglichkeiten, wie man ausgehend von der Cäsar-Verschlüsselung zu sichereren Verfahren kommen kann.

AB 2 | Das Caesar-Verfahren hacken

ASCII-Codetabelle										
+	0	1	2	3	4	5	6	7	8	9
30				!	"	#	$	%	&	'
40	(	)	*	+	,	-	.	/	0	1
50	2	3	4	5	6	7	8	9	:	;
60	<	=	>	?	@	A	B	C	D	E
70	F	G	H	I	J	K	L	M	N	O
80	P	Q	R	S	T	U	V	W	X	Y
90	Z	[	\	]	^	_	`	a	b	c
100	d	e	f	g	h	i	j	k	l	m
110	n	o	p	q	r	s	t	u	v	w
120	x	y	z	{	|	}	~			

1) Das Symbol m stehe für den ASCII-Code eines beliebigen Großbuchstabens, das Symbol m* für den ASCII-Code des zugehörigen Geheimbuchstabens und das Symbol e für den Schlüssel.
   a) Verschlüsseln: Beschreibe, wie man m* aus m und e berechnen kann.
   b) Entschlüsseln: Beschreibe, wie man m aus m* und e berechnen kann.

2) Beschreibe das Brute-Force-Verfahren zum Brechen einer Caesar-Verschlüsselung.

3) Eine Häufigkeitsanalyse ergibt, dass der häufigste Buchstabe in einem Geheimtext das B ist.
   a) Bestimme den Schlüssel, der vermutlich verwendet wurde.
   b) Erläutere, warum man auf diese Weise nicht immer den richtigen Schlüssel erhältst.

4) Das Verschlüsselungsverfahren wird geändert. Anstelle einer Zahl als Schlüssel wird ein ganzes Geheimalphabet als Schlüssel verwendet. Dieses besteht aus allen Buchstaben des Alphabets in einer zufälligen Reihenfolge. Beim Verschlüsseln ersetzt man jeden Klarbuchstaben so, dass der Geheimbuchstabe und der Klarbuchstabe an gleicher Stelle im Geheimalphabet bzw. im normalen Alphabet steht.
   Beurteile die Sicherheit dieses Verschlüsselungsverfahrens.

AB 3 | Die Vigenère-Verschlüsselung

1) Beschreibe das Verschlüsselungsverfahren.
2) Beurteile die Sicherheit des Verfahrens.
3) Begründe: Wenn der Schlüssel genauso lang wie die Nachricht ist, dann kann die Vigenère-Verschlüsselung nicht gebrochen werden.
4) Den in 3 beschriebenen Fall nennt man Einmalverschlüsselung oder One-Time-Pad (OTP). Hat man damit die Lösung für einen sicheren Datentransfer gefunden?

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

AB 4 | Das RSA-Verfahren: Public Key

Notiere hier nach und nach die von dir gewählten bzw. bestimmten Werte:

p = ; q = ; (e; N) =

0) Erkläre, was man unter asymmetrischen Verschlüsselungsverfahren versteht und welchen Vorteil ein gegenüber einem symmetrischen Verfahren hat.

1) a) Definiere den Begriff Primzahl. Beschreibe einen Algorithmus, mit dem man prüfen kann, ob eine Zahl prim ist.
   b) Erkläre an einem Beispiel die Bestimmung des öffentlichen Schlüssels (e, N).

2) a) Bestimme die Primfaktorzerlegungen von 52 und 108.
   Zusatz: Beschreibe einen Algorithmus zur Bestimmung der Primfaktorzerlegung einer Zahl n.
   b) Erkläre an einem Bespiel, wie man den ggT zweier Zahlen mithilfe ihrer Primfaktorzerlegungen ermitteln kann.
   c) Definiere die Eulersche Phi-Funktion und trage die fehlenden Werte in die Tabelle ein:

n	1	2	3	4	5	6	7	8	9	10	11	12	13
$\varphi(n)$													

   Was fällt dir auf, wenn du die Funktionsargumente n und die Funktionswerte $\varphi(n)$ anschaust?

   d) Beschreibe, welche Zahlen für die Zahl e des öffentlichen Schlüssels infrage kommen

3) Fasse die Vorgehensweise zur Bestimmung des öffentlichen Schlüssels zusammen.

AB 5 | Das RSA-Verfahren: Nachrichten verschlüsseln

Öffentlicher Schüssel von AB 4:

Klartext m: Geheimtext c:

1) a) Heute ist Sonntag. Bestimme den Wochentag in 346 Tagen.
   b) Gib alle Zahlen in der Restklasse 3 zum Modul 10 an.
   c) Erkläre die Bedeutung von $6 \bmod 4 = 2$ und von $6 \equiv 2 \pmod 4$.

2) a) Berechne m^e.
   b) Bestimme $m^e \bmod N$ mit deinen Zahlenwerten.

AB 6 | Das RSA-Verfahren: Nachrichten entschlüsseln

Öffentlicher Schüssel von AB 4:

Geheimtext c von AB 5:

Privater Schlüssel:

Klartext zu c:

1) a) Erkläre den Begriff „Modulares Inverses“. Bestimme das Inverse von 3 für den Modul 8 und das Inverse von 5 für den Modul 13.
   b) Bestimme den privaten Schlüssel (d; N) von Bob und notiere ihn oben.
2) Bestimme den zu c gehörenden Klartext.
3) a) Vergleiche das Caesar-Verschlüsselungsverfahren mit dem RSA-Verschlüsselungsverfahren.
   b) Eve will eine RSA-Verschlüsselte Botschaft knacken. Neben dem Geheimtext hat er sich natürlich den öffentlichen Schlüssel besorgt: (e, N) = (5, 15). Wie könnte der private Schlüssel lauten?
   c) Beurteile die Sicherheit des RSA-Verfahrens, wenn man für einen längeren Text jeden einzelnen Buchstaben wie beschrieben verschlüsselt.

AB 7 | Das RSA-Verfahren: Nachrichten austauschen

1) a) Gib an, auf was die Sicherheit des RSA-Verfahrens beruht.
   b) Erkläre, was man unter einem Seitenkanalangriff versteht.
   c) Erläutere, wie das RSA-Verfahren früher für die Kommunikation mit Webservern genutzt wurde und warum man davon abgekommen ist.
2) Erkläre, warum die Anwendung des RSA-Verfahrens auf jedes einzelne Zeichen nicht sinnvoll ist und wie man stattdessen vorgeht.
3) Beschreibe kurz alle Schritte des RSA-Verfahrens.
4) Recherchiert und diskutiert: Wer hat Interesse am unbefugten Zugriff auf Daten? Welche Ziele werden hierbei verfolgt?