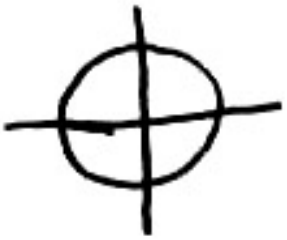
Sum of Us 2011:
Restklassen und Kryptographie

Der Zodiac-Mörder ist einer der berüchtigsten Serienmörder in der Geschichte der USA. In den 60er und frühen 70er Jahren des vergangenen Jahrhunderts tötete er nach eigenen Aussagen 37 Menschen in dem amerikanischen Staat Kalifornien. Es konnten aber nur 5 Morde, 1968 und 1969 verübt, von der Polizei sicher dem Zodiac-Mörder zugeschrieben werden. Die Untersuchungen dieser Morde laufen noch heute; der Polizei ist es nie gelungen die Identität des Täters herauszufinden. Der Zodiac-Mörder sendete bis 1974 Briefe an verschiedene amerikanische Zeitungen, darin nannte er sich selbst den Zodiac und unterzeichnete mit dem sogenannten Zodiac Zeichen.



Diese Briefe enthalten auch einige Kryptogramme, Stücke verschlüsselten Texts, die Hinweise zu den Morden und der Identität des Täters geben sollten. Nach der Veröffentlichung dieser Kryptogramme wurde eines von zwei Lehrkräften, Donald und Bettye Harden, entschlüsselt. Die restlichen bleiben bis zum heutigen Tag ein Rätsel. Die Suche nach dem Zodiac wurde 2007 von David Fincher verfilmt.

Die Untersuchungen der Morde laufen noch stets; die Polizei hat es nie geschafft den Zodiac zu identifizieren. Es gibt einige Verdächtige, aber es gibt gegen keinen von ihnen ausreichend Beweise. Ungefähr die Hälfte der Verdächtigen lebt noch. Als Kryptologen im Dienste der Polizei begebt ihr euch in den folgenden Aufgaben auf die Suche nach dem Aufenthaltsort des Zodiac, um so seine Identität zu lüften. Hierzu versucht ihr beispielsweise von der Polizei abgehörte Berichte des Zodiac, der seine Nachrichten an seine Komplizen stets sorgfältig verschlüsselt hat, zu entschlüsseln.

Die Aufgaben 1 bis 5 sind unabhängig voneinander und können in beliebiger Reihenfolge bearbeitet werden.

Schreibt eure Schule, eure Teamnummer und die Antworten zu den Aufgaben auf das Antwortblatt (Seite 8).

Aufgabe 1

Der folgende Text ist mit der Vigenére-Verschlüsselung mit einem Codewort von höchstens fünf Buchstaben verschlüsselt.

```
SA OOA GOEPSATQGPX FEKNEOA SKG OKF QLV AEMKVRC LRT NRC VBPCHYQ
RTXRD WBCNRD EZ SSYQO TPLREOA. PC TPRG OKOPS HX OVYOA QKYW, NRC
WVEDYPBJPSYP JJZOYQ TNSBR LVG TCG. MOV PSAPW YPSPSXNX GHCNRY OVYSTP
WRCUJFOEOSTP XBESMPX, BQPRYCVNRGWSPS OVY MBOO, TPPHYNRY. NVP OKAOEEOA
OOF QLV VYAYDRY SUY CRWLFE XVNRG WYRDOA FXQ DEPSDRY NVP RVWPR OOE
ZOSQOAEVVNRXPSG. MOV OOZ QKYW RNYNRWD RD CVNR HX NRY WBCN NY BVNUL
XMPZBZTMX TW WFXV YOHYJRSXUFXQPBGYOHYEAOXRFXMTQ. FPSA VYRCZRC GHCNR
TX RTXRX PRWN VY CNTXG WYHTC TPPHYNRY. NVP ZBWSMPS RYDQPMXEO MHOV
GOEDMUWERDCRWDR MBVPPR TX FPSAPB UZCRYDNDMUP, XNNR NFCXFXSE NRD
POT CVYN QTOFP LETOSP NVP OVYJVROA SSAHOVDO SFOE PSAPX ZZBQ. TX QPX
YPDMEOA UKUCOA TCG PC AZMU VOVYOZ ROYFXTPX QPX PZNR KE XYKPVOA. OSR
MBVPPR PXGSKYEOA TXFROFLWG FXTPPNPRE OBRTCFTQ MPSYPX IPBFNRYFOFDOYEOA
EOKE. OF DSRSD NFC JTO RTX MFPNPVYTQRC WVI KHD LHNRFEKOPX, MLRYPX,
XWKZXOEY EAO CGCSPSOA. OSR DDNYNNCN-RYDFNRYFOFDOYFXTDWRERBOOA
SKOPX OTC WPDME JH VOVYOZ PBTPLATC TPPHPREE. NND POT RBQPG, OKFD
OVY EAMOSLXTPXRC LYTMX LES OSR MBVPPR GSRWVRTMUE JHX NHCMUMBHNR
SFOUCOA VKAY. NVP VBPCHYQ IZX NFPTLLR KGRT LRRSAYD ZTD AFVY KGRT.
NVP LETOSP RNE ERMBVROAD XVNRG OOE XYRCNRC RVYDRCVNDCRY, CVP CVYN
ITOYXOUC FBX YCQOE ROFNRETOOPX. YLEG OOE QKZTVVP CPSBVPL RC CPSYA TX
FPSAPB WFQRYN IPBFNRYFOFDOYEO OCSRQO, QTO XPSAPB YPCRY UBYXGP. JJPS
YPREPB FZBTEOA QERC OVYOA OEENROCEPS SZ QKYW NRC JBOSNN-WBCNR TX QPX
FTOOKSTPB WLREPX VY UNWSSZBATOA. DSR WYRDDRY NVP MBOOF, YKPSNRX CVP
OVYOA LOUYVVNRRY KHQBHQ SA OOE KOVEEAR QRDOUPX ULDGPX, QPB ZZOEOOE TW
MZNVLUSLVY HEEOO NMOE YSR ROSLCFE.
```

Aufgabe 1a: *Wie viele Buchstaben besitzt das Codewort?*

Aufgabe 1b: *Wie lautet das Codewort?*

Aufgabe 2

Der Zodiac hat Informationen über seinen Aufenthaltsort an seine Komplizen mittels Verwendungszweck einer Geldüberweisung geschickt. Um die Informationen herauszufinden, begeben wir uns auf die Suche nach seiner Kontonummer und nach dem geheimen Code, der uns den Zugang zu dem Konto verschafft.

Der Zodiac ist Kunde bei einer belgischen Bank. Eine gültige belgische Kontonummer besteht aus einer Zahl Z mit 10 Ziffern (mit einem Strich nach den ersten drei Zahlen) und sowie einer Kontrollzahl K bestehend aus zwei Ziffern. Für die Kontonummer

$$091 - 0122401 - 16.$$

gilt z.B. $Z = 0910122401$ und $K = 16$. Die Kontrollzahl K ist das eindeutig bestimmte Element aus $\{1, \ldots, 97\}$, das kongruent zu Z modulo 97 ist. Die Kontrollzahl K ist also genau der Rest von Z, der beim Teilen durch 97 entsteht. Es sei denn der Rest ist 0. In diesem Fall ist die Kontrollzahl 97.

Du hast die Kontonummer des Zodiac abgefangen:

$$300 - 9032402 - 94.$$

Es scheint jedoch keine gültige Nummer zu sein. Du vermutest, dass eine der Ziffern verändert ist, um die wirkliche Nummer zu schützen.

Aufgabe 2a: *Wie lautet die tatsächliche Kontonummer des Zodiac, wenn du weißt, dass genau eine der Ziffern in* 300–9032402–94 *falsch ist.*

Um die Daten der Überweisung lesen zu können, brauchst du zusätzlich noch den geheimen Zugangscode zum Konto des Zodiac. Glücklicherweise hast du die folgende Information. Der Code besteht aus 4 Ziffern und hat die Form AB (hierbei ist AB kein Produkt, sondern beide Zahlen wurden hintereinandergeschrieben), wobei A und B zwei Zahlen der Menge $V = \{02, 03, 04, \ldots, 99\}$ mit $A \leq B$ sind. Wenn also z.B. $A = 02$ und $B = 99$, dann ist der Code 0299. Die Polizei hat das unten aufgeführte Gespräch zwischen zwei Komplizen des Zodiac mit den Codenamen P und S aufgeschnappt. Desweiteren verfügt sie über die Informationen: Komplize P kennt das Produkt $A \cdot B$, Komplize S kennt die Summe $A + B$. Beide Komplizen wissen, dass der andere diese Information besitzt. Sie wissen beide, dass A und B aus der Menge V stammen.

- *Komplize P*: Ich kenne die Summe $A + B$ nicht.
- *Komplize S*: Das wusste ich. Diese Summe ist kleiner als 14.
- *Komplize P*: Das wusste ich. Und jetzt kenne ich auch A und B.
- *Komplize S*: Ich auch.

Aufgabe 2b: *Wie lautet der vierstellige Zugangscode zum Konto?*

Aufgabe 3

Die Polizei hat dich als verdeckten Ermittler in das Netzwerk des Zodiac schmuggeln können. Du erhälst nun ebenfalls verschlüsselte Informationen vom Zodiac. Der geheime Schlüssel wird mit dem Diffie-Hellmansystem ausgetauscht. Als öffentlichen Schlüssel benutzt ihr die Primzahl $p = 239$ und das erzeugende Element $\overline{g} = \overline{7}$ von $\mathbb{Z}_p^\times$. Der Zodiac wählt einen geheimen Wert B aus $\{15, \ldots, 237\}$ und sagt dir, dass $\overline{g}^B = \overline{237}$ ist. Du selbst wählst nun eine natürliche Zahl A aus der Menge $\{15, \ldots, 237\}$ und schickst ihm $\overline{g}^A$. Der Zodiac schickt dir nun als Antwort eine verschlüsselte Nachricht, also ein Element $\overline{y}$ aus $\mathbb{Z}_p$. Er hat die ursprüngliche Nachricht $\overline{x}$ aus $\mathbb{Z}_p$ durch das Multiplizieren mit $\overline{g}^{AB}$ verschlüsselt, also

$$\overline{y} = \overline{x} \cdot \overline{g}^{AB}.$$

Bestimme also $\overline{g}^A$ für den von dir gewählten Wert von A. In der Tabelle auf der folgenden Seite kannst du nachschauen welchen Wert für $\overline{y}$ du daraufhin vom Zodiac erhälst.

Entschlüssle nun den verschlüsselten Bericht $\overline{y}$ (bestimme also die zugehörige Zahl $\overline{x}$ aus $\mathbb{Z}_p$).

Aufgabe 3: *Bestimme den eindeutigen Repräsentanten aus der Menge* $\{0, ..., p-1\}$ *der Restklasse* $\overline{x}$ *aus* $\mathbb{Z}_p$.

Öffentlicher Schlüssel und verschlüsselte Nachricht

$\overline{g}^A$	$\overline{y}$
2	65
3	149
4	43
5	123
6	14
8	227
9	238
10	188
12	35
13	132
14	109
15	89
16	209
17	53
18	117
19	128
20	231
21	180
22	84
23	201
24	207
25	205
26	91
27	77
28	153
29	206
30	103
31	42
32	164
33	233
34	13
35	232
36	173
37	4
38	81
39	113
40	219
41	40

$\overline{g}^A$	$\overline{y}$
42	211
43	67
44	210
45	78
46	144
47	22
48	159
50	154
51	221
52	108
53	198
54	73
55	56
56	24
57	182
58	37
59	110
60	138
62	105
63	2
64	171
65	220
66	224
67	119
68	152
69	58
70	102
71	175
72	74
73	3
74	10
75	228
76	83
78	163
79	125
80	189
81	46

$\overline{g}^A$	$\overline{y}$
82	100
83	190
84	169
85	168
86	48
87	151
88	47
89	147
90	195
91	214
92	121
93	112
94	55
95	54
96	39
97	160
98	21
99	223
100	146
101	94
102	194
103	98
105	61
106	17
107	157
108	63
109	167
110	140
111	170
112	60
113	234
114	216
115	96
116	212
117	142
118	36
119	133

$\overline{g}^A$	$\overline{y}$
120	106
122	97
123	27
124	143
125	23
126	5
127	179
128	69
129	99
131	176
132	82
133	222
134	178
135	208
137	45
138	145
139	93
140	16
141	218
142	79
143	200
144	185
145	184
146	127
147	118
148	25
149	44
150	92
151	192
152	88
153	191
154	71
155	70
157	139
158	193
159	50
160	114

$\overline{g}^A$	$\overline{y}$
161	76
162	115
163	156
164	11
165	229
166	236
167	165
168	64
169	137
170	181
171	87
172	120
173	15
174	19
175	68
176	237
177	134
178	9
179	101
180	129
181	202
182	57
183	215
184	183
185	166
186	41
187	131
189	85
190	135
191	80
192	217
194	161
195	29
196	172
197	28
198	199
199	20

$\overline{g}^A$	$\overline{y}$
200	126
201	158
202	235
203	66
204	7
205	226
206	6
207	75
208	197
209	136
210	33
212	162
213	148
214	34
215	32
216	38
217	155
218	59
219	8
220	111
221	122
222	186
223	30
224	150
225	130
226	107
227	204
228	62
229	51
230	1
231	12
232	52
233	225
234	116
236	90
237	174
238	213

Aufgabe 4

Mit dem gleichen System wie in Aufgabe 3 kommuniziert der Zodiac auch mit seinen echten Komplizen. Wir möchten daher gerne herausfinden welchen geheimen Schlüssel B der Zodiac benutzt. Hierzu verwenden wir den sogenannten Silver-Pohlig-Hellman Algorithmus, der in günstigen Fällen eine schnelle Möglichkeit bietet diskrete Logarithmen zu berechnen.

Im folgenden wird dieser Algorithmus kurz erklärt: Sei p eine Primzahl und $\overline{g}$ ein erzeugenden Element aus $\mathbb{Z}_p^\times$. Betrachte die Primfaktorzerlegung

$$\varphi(p) = p_1 \cdots p_r$$

der Euler-Zahl $\varphi(p) = p - 1$. Wir nehmen der Einfachheit halber an, dass die Primfaktoren p_i alle verschieden sind.

Setze weiter voraus, dass $\overline{g}^B$ gegeben ist, wobei B ein Element aus $\{0, \ldots, p-2\}$ ist. Wir wollen den Exponenten B ermitteln. Um B zu kennen genügt es, die Restklasse von B modulo p_i für jeden Primfaktor p_i von $p-1$ zu bestimmen. Der chinesische Restsatz besagt, dass B durch diese Restklassen eindeutig bestimmt ist.

Wir notieren mit B_i das eindeutige Element aus $\{0, \ldots, p_i - 1\}$ mit

$$B \equiv B_i \mod p_i.$$

Wir erinnern uns jetzt daran, dass

$$(\overline{g}^B)^{\varphi(p)/p_i} = (\overline{g}^{\varphi(p)/p_i})^B = (\overline{g}^{\varphi(p)/p_i})^{B_i}$$

in $\mathbb{Z}_p$ ist, wobei die letzte Gleichung aus Folgerung 2.8.2 aus den Vorbereitungsunterlagen folgt. B_i ist außerdem das einzige Element aus $\{0, ..., p_i - 1\}$, dass diese Gleichung erfüllt (erkennst du warum?). Wir können B_i also finden, indem wir alle möglichen Werte ausprobieren.

Diese Technik wenden wir nun auf die Daten aus Aufgabe 3, bei der $p = 239$, $\overline{g} = \overline{7}$ und $\overline{g}^B = \overline{237}$ sind, an. Die Euler-Zahl $\varphi(239) = 238$ ist durch die Primzahl $p_3 = 17$ teilbar. Wir sehen, dass

$$(\overline{g}^B)^{\varphi(239)/17} = \overline{237}^{14}$$

in $\mathbb{Z}_{239}$, und wir müssen ein Element B_3 aus $\{0, \ldots, 16\}$ derart finden, dass $\overline{237}^{14} = (\overline{7}^{14})^{B_3}$ erfüllt ist. Mit etwas einfachem Rechnen (und ohne Taschenrechner) erhalten wir $B_3 = 15$. B ist also kongruent zu 15 modulo 17.

Aufgabe 4a: *Bestimme B_1 und B_2. Du kannst dabei $\overline{2}^{119} = \overline{1}$ verwenden.*

Aufgabe 4b: *Bestimme mit Hilfe von B_1, B_2 und B_3 den geheimen Schlüssel des Zodiac.*

Aufgabe 5

Der Zodiac hat bemerkt, dass seine Kommunikation, die er mit Hilfe des Diffie-Hellman Protokolls verschlüsselt, abgehört wird. Er geht daher zu einer Verschlüsselung mit Vigenère über, wobei er das Codewort via RSA austauscht.

Der öffentliche Schlüssel (n, e) seines Komplizen ist

$$n = 115,$$
$$e = 59.$$

Der Zodiac benutzt im Vigenèresystem ein Codewort, welches aus zwei Buchstaben des Alphabets besteht, die auf die übliche Weise in Zahlen umgesetzt werden: $A = 00$, $B = 01$, ..., $Z = 25$.

Jeder der beiden Buchstaben wird als Zahl $\overline{x}$ in $\mathbb{Z}_n$ betrachtet. Diese werden durch den Zodiac mit Hilfe von RSA mit dem oben genannten öffentlichen Schlüssel (n, e) codiert, und an den Komplizen geschickt. Wenn beispielweise das Codewort im Vigenèresystem `VS` wäre, mit den Buchstabenwerten $\overline{x}_1 = \overline{21}$ und $\overline{x}_2 = \overline{18}$, dann würde der Zodiac seinem Komplizen die beiden Zahlen $\overline{y}_1 = (\overline{x}_1)^e = (\overline{21})^{59} = \overline{76}$ und $\overline{y}_2 = (\overline{x}_2)^e = (\overline{18})^{59} = \overline{27}$ schicken. In Wirklichkeit schickt er:

$$\overline{y}_1 = \overline{38},$$
$$\overline{y}_2 = \overline{80}.$$

Der Komplize war jedoch etwas naiv bei der Wahl des öffentlichen Schlüssels, denn die Priemfaktorzerlegung von $n = 115$ ist leicht zu bestimmen: $115 = 5 \cdot 23$.

Hiermit kannst du nun die ursprünglichen Zahlen $\overline{x}_1$ und $\overline{x}_2$ berechnen, und daraus das aus zwei Buchstaben bestehende Codewort für das Vigenèresystem bestimmen.

Der Zodiac hat seinen Aufenthaltsort mit Hilfe des Vigenèresystems mit dem aus zwei Buchstaben bestehende Codewort verschlüsselt und schickt diesen an seinen Komplizen:

`SIJNFH`

Aufgabe 5: *Wie lautet der Aufenthaltsort des Zodiac?*

Antwortblatt

Schule: _____

Teamnummer: _____

Antwort auf Frage 1a: _____

Antwort auf Frage 1b: _____

Antwort auf Frage 2a: _____

Antwort auf Frage 2b: _____

Antwort auf Frage 3: _____

Antwort auf Frage 4a: _____

Antwort auf Frage 4b: _____

Antwort auf Frage 5: _____

Lösungen Sum of Us 2011

Antwort auf Frage 1a: **3**

Antwort auf Frage 1b: **KNL**

Antwort auf Frage 2a: **300-9072402-94**

Antwort auf Frage 2b: **0209**

Antwort auf Frage 3: **26**

Antwort auf Frage 4a: $B_1 = 1$ **und** $B_2 = 3$

Antwort auf Frage 4b: $B = 185$

Antwort auf Frage 5: **BOSTON**

Lösungen zu den Nachmittagsaufgaben 2011 zur Kryptographie

Aufgabe 1

Für die Buchstaben des Alphabets benutzen wir folgende Zahlenwerte:

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

Im Text markiert sind die ersten Wiederholungen zweier Wörter, die aus 3 Buchstaben bestehen, nämlich NRC und NVP.

SA OOA GOEPSATQGPX FEKNEOA SKG OKF QLV AEMKVRC LRT NRC VBPCHYQ
RTXRD WBCNRD EZ SSYQO TPLREOA. PC TPRG OKOPS HX OVYOA QKYW, NRC
WVEDYPBJPSYP JJZOYQ TNSBR LVG TCG. MOV PSAPW YPSPSXNX GHCNRY OVYSTP
WRCUJFOEOSTP XBESMPX, BQPRYCVNRGWSPS OVY MBOO, TPPHYNRY. NVP OKAOEEOA
OOF QLV VYAYDRY SUY CRWLFE XVNRG WYRDOA FXQ DEPSDRY NVP RVWPR OOE

Zwischen den beiden NRC's stehen 54 Buchstaben, zwischen den beiden NVP's 51 Buchstaben. Es ist $54 = 2\cdot 3^3$, $51 = 3\cdot 17$, ggT(54,51) = 3. Somit ist die **Länge des Codewortes 3**, da sie höchstens 5 sein sollte.

Die Stellung von NRC und NVP im Text – u.a. nach einem Komma bzw. am Satzanfang- wie auch der gleiche 1.Buchstabe ‚N' lässt vermuten, dass es sich um die bestimmten Artikel *DER, DIE* oder *DAS* handelt. Die Zuordnung DER → NRC liefert wegen

3 + **10** ≡ 13 , 4 + **13** ≡ 17, 17 + **11** ≡ 2 mod 26 das **Codewort KNL** .

Die Codierung von DIE ist dann gerade NVP. Diese Codierung ergibt einen sinnvollen Text: *IN DEN VEREINIGTEN STAATEN.....*

Aufgabe 2

a) Wegen MOD(3009032402, 97) = 58 kann man die Prüfziffer durch Änderung **einer** Ziffer nicht zu 58 machen. Da 94-58 = 36 muss man durch Ändern einer der Ziffern von 3009072402 zusätzlich 36 erhalten. Dies kann naheliegend keine Einer- oder Zehnerziffer sein. Nun ist

MOD(100, 97) = 3 , MOD(1000, 97) = 30 , MOD(10000, 97) = 9 und 4·9 = 36.

Erhöht man also die 5. Stelle von rechts um 4, so erhält man die korrekte Kontonummer mit

MOD(300907**7**2402, 97) = 94.

b) Das Produkt P = A·B kann nicht aus genau zwei Primfaktoren bestehen (wegen Aussage 1), da in diesem Fall die Summe A+B bekannt wäre. Aber auch in keiner der Zerlegungen der Summe S = A + B dürfen A und B beide Primzahlen sein, da sonst Komplize S nicht in jedem Fall wissen könnte, dass Komplize P die Summe nicht kennt (Aussage 2, 1.Teil). Somit entfallen von den Summen kleiner als 14 :

13 = 2 + 11 = ….; 12 = 5 + 7 = …; 10 = 3 + 7 = …; 9 = 2 + 7 = …; 8 = 3 + 5 = …;
7 = 2 + 5 = …; 6 = 3 + 3 = …; 5 = 2 +3; 4 = 2 + 2.

Somit kommt nur die Summe 11 in Frage.

Nun hat 11 die additiven Zerlegungen: 11 = 2 + 9 = 3 + 8 = 4 + 7 = 5 + 6 .

Dies ergibt die Produkte 18, 24, 28, 30. Wegen Aussage 3 darf keiner dieser Produkte P=A·B eine additive Zerlegung S=A+B zulassen, die größer als 13 ist.
Wegen 24 = 2·12 und 2+12>13, 28=2·14und 2+14>13, 30=2·15 und 2+15>13 , 18=2·9=3·6 und 2+9=11, 3+6=9 ist also nur A=2 und B=9 möglich, was den Code 0209 ergibt.

Aufgabe 3

Gegeben sind p = 239, $\overline{g}=\overline{7}$ *und* $\overline{7}^{B}=\overline{237}=\overline{(-2)}$. Wähle z.B. A = 16, da es aufgrund der Potenzierungen häufig günstig ist, eine Zweierpotenz zu wählen. Natürlich würde auch jede andere Zahl aus der betrachteten Menge möglich sein.

Bestimme als nächstes 7^{16} mod 239, also $\overline{7}^{16}$.

Wegen $7^4 = 49^2 = 2401 = 2390 + 11$ ist $7^4 \equiv 11$ mod 239, damit

$7^8 = (7^4)^2 \equiv 11^2 = 121$ und somit $7^{16} \equiv 121^2 = 14641 = 6\cdot239 + 62$. Es ist also $\overline{7}^{16}=\overline{62}$.

Dies liefert nach Tabelle y = 105. Zu lösen bleibt also die Kongruenz:

$\overline{105}=\overline{x}\cdot\overline{7}^{16B}=\overline{x}\cdot(\overline{7}^{B})^{16}=\overline{x}\cdot(\overline{-2})^{16}$

Nun ist $2^8 = 256 = 239 + 17$, also $\overline{2}^{8}=\overline{17}$ und damit $(\overline{-2})^{16}=\overline{2}^{16}=(\overline{2}^{8})^{2}=\overline{17}^{2}=\overline{289}=\overline{50}$.

Zu lösen bleibt also $\overline{105}=\overline{50}\,\overline{x}$ oder in der ‚mod'-Schreibweise 50x ≡ 105 mod 239.

Da ggT(105,50) = 5 teilerfremd zu 239 ist, kann man kürzen und erhält 10x ≡ 21 mod 239.

Nun ist 10·24 = 240 ≡ 1 mod 239. Da 24 und 239 teilerfremd sind, kann man obige Kongruenz mit 24 multiplizieren und erhält die äquivalente Gleichung:

10·24·x ≡ 21·24 oder 240x ≡ 1·x ≡ (10 + 10 + 1)·24 = 240 + 240 + 24 ≡ 1 + 1 +24 = 26.

Somit ist $\overline{x}=\overline{26}$.

Aufgabe 4

a) Es ist φ(239) = 238 = 2·7·17 mit $p_1 = 2$, $p_2 = 7$, $p_3 = 17$.

Um B_1 zu bestimmen, ist die Kongruenz $\overline{237}^{\frac{\varphi(239)}{2}}=(\overline{7}^{\frac{\varphi(239)}{2}})^{B_1}$ *also* $\overline{237}^{119}=(\overline{7}^{119})^{B_1}$ zu lösen.

Nun ist, s. Aufg. 3, $\overline{237}=\overline{(-2)}$ und somit $\overline{237}^{119}=\overline{(-2)}^{119}=-\overline{2}^{119}=-\overline{1}$ (s. Hinweis). Da B_1 nur 0 oder 1 sein kann, kommt nur $B_1 = 1$ in Frage, was man auch durch Nachrechnen bestätigen kann.

Um B_2 zu bestimmen, ist die Kongruenz $\overline{237}^{\frac{\varphi(239)}{7}}=(\overline{7}^{\frac{\varphi(239)}{7}})^{B_2}$ *also* $\overline{237}^{34}=(\overline{7}^{34})^{B_2}$ zu lösen mit $B_2 \in \{0,1,2,3,4,5,6\}$. Durch Nachrechnen erhält man $\overline{(-2)}^{34}=\overline{2}^{34}=\overline{201}$ wie auch, s. Aufg.3, $\overline{7}^{32}=(\overline{7}^{16})^{2}=\overline{62}^{2}=\overline{20}$ *und damit* $\overline{7}^{34}=\overline{7}^{32}\cdot\overline{7}^{2}=\overline{20}\cdot\overline{49}=\overline{24}$. Nun ist $\overline{24}^{2}=\overline{98}$ *und* $\overline{24}^{3}=\overline{201}$, sodass $B_2 = 3$ ist.

b) Zu lösen ist jetzt das folgende System von Kongruenzen:

$B \equiv 1 \bmod 2$

$B \equiv 3 \bmod 7$

$B \equiv 15 \bmod 17$

Um den Chinesischen Restsatz anzuwenden, haben wir zu lösen:

$a_1 \cdot 2 + b_1 \cdot 119 = 1$; eine Lösung ist z.B. (-59,1).

$a_2 \cdot 7 + b_2 \cdot 34 = 1$; eine Lösung ist z.B. (5,-1).

$a_3 \cdot 17 + b_3 \cdot 14 = 1$; eine Lösung ist z.B. (5,-6).

Dann ist $3 \cdot (-1) = -3 \equiv 4 \bmod 7$ wie auch $15 \cdot (-6) = -90 \equiv 12 \bmod 17$ und es ergibt sich

$B = 1 \cdot 1 \cdot 119 + 4 \cdot 34 + 12 \cdot 14 = 423 \equiv 185 \bmod 239$.

Also B = 185.

Aufgabe 5

Es ist $115 = 5 \cdot 23$ die Primfaktorzerlegung von n = 115. Damit ist $\varphi(n) = 4 \cdot 22 = 88$.

Den geheimen Schlüssel d erhalten wir durch Lösen der Kongruenz $e \cdot d \equiv 1 \bmod \varphi(n)$, also hier $59 \cdot d \equiv 1 \bmod 88$. Falls man nicht die Lösung d = 3 schnell sieht, wandelt man das um in die diophantische Gleichung $59d + 88y = 1$. Der Euklidische Algorithmus

$88 = 1 \cdot 59 + 29$

$59 = 2 \cdot 29 + 1$

liefert $1 = 59 - 2 \cdot 29 = 59 - 2 \cdot (88 - 1 \cdot 59) = 3 \cdot 59 - 2 \cdot 88$, also d = 3.

Um den Klartext des Codewortes zu erhalten, berechnen wir

$\overline{x_1} = \overline{y_1}^3 = \overline{38}^3$ *wie auch* $\overline{x_2} = \overline{y_2}^3 = \overline{80}^3$ mit dem Modul 115.

Nun ist $38^3 = 38^2 \cdot 38 \equiv 64 \cdot 38 \equiv 17 \rightarrow$ R, $80^3 = 80^2 \cdot 80 \equiv 75 \cdot 80 \equiv 20 \rightarrow$ U. (s.Aufg.1)

Das Codewort für das Vigenèresystem lautet also: RU.

Mod 26 erhalten wir also

S	I	J	N	F	H
18	8	9	13	5	7
-17	-20	-17	-20	-17	-20
1	14	18	19	14	13
B	O	S	T	O	N

Der Aufenthaltsort ist also BOSTON.