Ludwig-Maximilans-
Universität München
Dr. Pascal Reisert

Wintersemester 2018/2019
Übungsblatt 1
19. Oktober 2018

Übungen zur Kryptographie
Lösung

Aufgabe 1

`CEODY XSECL OCMRB SOLNS OFYXM KOCKB LOXED JDOQO ROSWC MRBSP D`

Wir bestimmen die Häufigkeit der einzelnen Buchstaben und erhalten `O` 9-fach, `C` und `S` je 5-fach. Wir vermuten, dass `O` dem im deutschen häufisten Buchstaben `e` entspricht. Somit wäre $t = 10$ in $\sigma_t : x \mapsto x + t$. Mittels der Rücktransformation $\sigma_t^{-1} : x \mapsto x - t$ erhalten wir den Klartext

`Suetonius beschrieb die von Caesar benutze Geheimschrift`

Aufgabe 2

`WQVBD XHLAI NRGCN YEDZU PNKVI WQVST MFONJ`

Wie versuchen möglichst lange Buchstabenfolgen zu identifizieren und erkennen, dass

`WQV`BD XHLAI NRGCN YEDZU PNKVI `WQV`ST MFONJ

Die häufigste Dreibuchstabenkombination im Englischen ist `THE`. Mit `E` $= 4$, `H` $= 7$, `Q` $= 16$, `T` $= 19$, `V` $= 21$, `W` $= 22$ erhalten wir

$$\varphi_{a,b}(19) = 19a + b = 22, \varphi_{a,b}(7) = 7a + b = 16, \varphi_{a,b}(4) = 4a + b = 21$$
$$\Rightarrow 15a = 1 \Rightarrow 49 + b = 16 \Rightarrow a = 7, b = 19.$$

Wir erhalten die Umkehrfunktion $\varphi_{7,19}^{-1}(x) = 15x + 1$ und damit den Klartext

`The quick brown fox jumps over the lazy dog`

Bemerkung. Das Inverse modulo 26 lässt sich mit dem euklidischen Algorithmus berechnen - für 15

$$26 = 15 + 11 \Rightarrow 15 = 11 + 4 \Rightarrow 11 = 2 \cdot 4 + 3 \Rightarrow 4 = 3 + 1$$
$$1 = 4 - 3 = 3 \cdot 4 - 11 = 3 \cdot 15 - 4 \cdot 11 = -4 \cdot 26 + 7 \cdot 15.$$

Aufgabe 3

VWDDP WFEWA ZPXFW XPAAV WEHWD ERZJG BVWBW BSUGD BPAIE FWBSP MPATZ PEZUY YI

Den ersten drei Buchstaben DER entspricht VWD. Da die ersten beiden Buchstaben VW aufeinanderfolgend sind, vermuten wir, dass sie nicht mit dem Kennwortteil verschlüsselt wurden. Mit der üblichen Assoziierung erhalten wir $x \mapsto x + 17$ und

deLLX eNMeI HXFNe FXIId eMPeL MZHRO JDeJe JACOL JXIQM NeJAX UXIBH XMHCG GQ

Ersetzen wir noch D durch r (anstatt L) erhalten wir

derrX eNMeI HXFNe FXIId eMPer MZHRO JdeJe JACOr JXIQM NeJAX UXIBH XMHCG GQ

Die häufigsten verbleibenden Buchstaben sind X (7), I, J, M (je 5); die häufigsten verbleibenden Buchstaben im Deutschen sind n, i, s, a, t. Wir betrachten die Kombination JdeJeJ. Hier ist J wahrscheinlich kein Vokal. Von den häufigsten Trigrammen ein, ich, nde, die, und, der kommt nur nde infrage. Wir versuchen also J = n.

derrX eNMeI HXFNe FXIId eMPer MZHRO ndene nACOr nXIQM NenAX UXIBH XMHCG GQ

Wir betrachten den Anfang derr*e. Wörter die mit r und Konsonant beginnen sind sehr selten, Rhein, wir vermuten also, dass es sich bei dem fehlenden Buchstaben um einen Artikel handelt. Der häufigste Artikel nach dem e ist das i, dann das a.
Mit X=i ergibt sich

derri eNMeI HiFNe FiIId eMPer MZHRO ndene nACOr niIQM NenAi UiIBH iMHCG GQ

Mit X=a ergibt sich

derra eNMeI HaFNe FaIId eMPer MZHRO ndene nACOr naIQM NenAa UaIBH aMHCG GQ

Wir ersetzen noch das häufige M durch s und bekommen für X=i

derri eNseI HiFNe FiIId esPer sZHRO ndene nACOr niIQs NenAi UiIBH isHCG GQ

Mit dem a ergibt sich

derra eNseI HaFNe FaIId esPer sZHRO ndene nACOr naIQs NenAa UaIBH asHCG GQ

Man erkennt raetselhafte im Fall X=a. Insbesondere entspricht F=f der ersten Substiution (f als Nachbarbuchstabe von d und e) und N=t (N Nachbarbuchstabe von M, t Nachbarbuchstabe von s).

derra etsel hafte Falld esPer sZHRO ndene nACOr nalQs tenAa UalBH asHCG GQ

rnalQsten könnte rnalisten und damit Journalisten sein.

derra etsel hafte Falld esPer sZHRu ndene njour nalis tenja UalBH asHoG Gi

Aus aktuellem Anlaß kann man HasHoGGi zu Kashoggi auflösen.

derra etsel hafte Falld esPer sZhRu ndene njour nalis tenja UalBk ashog gi

Es ergibt sich

Der raetselhafte Fall des verschwundenen Journalisten Jamal Kashoggi

Es ist

abcdefghijklmnopqrstuvwxyz
PQRVWXYZISTANBULCDEFGHJKMO

Das Passwort ist also Istanbul.

Aufgabe 4

MNDCGAMQZCGKAGQNGOCDAAUDE
PSNDXCDHMAPAMGOUPHMNDZUTD
HMKXDGQMNDUZHEPHLCDHWNPEN
PHTGOTDAZEPSNDXEGHAPAMPHL
GQAMPEICDHDZENSGADXDSXDAD
HMPHLZUPAMPHEMODMMDX

Wir bestimmen zunächst die Häufigkeit der verschiedenen Buchstaben und erhalten:

Buchstabe	Anzahl	Buchstabe	Anzahl	Buchstabe	Anzahl
D	20	X	6	I	1
M	14	U	5	W	1
A	13	S	4	B	0
H	13	O	4	F	0
P	13	Q	4	J	0
G	10	L	3	V	0
N	9	T	3	R	0
E	8	K	2	Y	0
C	6	Z	6		

Als nächstes bestimmen wir alle Abfolgen von mehr als drei Buchstaben die sich wiederholen:

- 2fach EPSNDX,
- 2fach APAMPH + 1fach APAM+ 1fach AMP + 1fach MPH,
- 3fach MND,
- 3fach CDH,
- 3fach DHM,
- 3fach PHL.

MNDCGAMQZCGKAGQNGOCDAAUDE
PSNDXCDHMAPAMGOUPHMNDZUTD
HMKXDGQMNDUZHEPHLCDHWNPEN
PHTGOTDAZEPSNDXEGHAPAMPHL
GQAMPEICDHDZENSGADXDSXDAD
HMPHLZUPAMPHEMODMMDX

Wir erhoffen uns, dass zumindest eines der Trigramme den englischen Artikel the darstellt. Überprüfen wir für welche der Kombinationen auch holmes möglich ist. Für die Kombinationen P***S, S***N, N***D, D***X, P***A, A***M, M***P, P***H, D***H, H***M, H***L ergeben sich die folgenden vorkommenden verschlüsselten Worte für holmes

- NGOCDA, NDXCDH, NSGADX,
- DXDSXD, DMMDX.,
- MGOUPH,

- DXCDHM, DXEGHA, DHMPHL,

- PENPHT, PAMPHL, PAMPHE,

- HAPAMP, HEPHLC, HMPHLZ.

Davon haben nur NGOCDA, NSGADX , MGOUPH , DXEGHA die richtige Form. Die zugehörigen Triagramme sind SND, MND, AMP, CDO, wovon SND und AMP in längeren Kombinationen auftreten. Da wir das Wortende jedoch nicht kennen könnten sie natürlich auch the darstellen. Von den Triagrammen AMP und CDO ist AMP wahrscheinlicher, da der Buchstabe M mit einer Häufigkeit von 9,66% auftritt, wohingegen C nur 4,14 % der Buchstaben ausmacht. Die für den Buchstaben T erwartete Häufigkeit ist jedoch 9,25 %. Man beachte A hat eine Häufigkeit von 8,97 % und S nur eine Häufigkeit von 2,76 %.
Um eine möglichst gute Wahl treffen zu können vergleichen wir weitere Buchstaben von NGOCDA, NSGADX und MGOUPH auf Häufigkeit.

Buchstabe	NGOCDA	NSGADX	MGOUPH
e (12,75 %)	D (13,79 %)	D (13,79 %)	P (8,97 %)
o (7,5 %)	G (6,90 %)	S (2,76 %)	G (6,90 %)
s (6,0 %)	A (8,97 %)	X (4,14 %)	H (8,97 %).

Wir erhalten die Abweichungen von (e,o,s) als

NGOCDA	$\sqrt{0,5 \cdot ((12,75-13,79)^2+(7,5-6,9)^2+(6,0-8,97)^2)} = 2,26$
NSGADX	$\sqrt{0,5 \cdot ((12,75-13,79)^2+(7,5-2,76)^2+(6,0-4,14)^2)} = 3,67$
MGOUPH	$\sqrt{0,5 \cdot ((12,75-8,97)^2+(7,5-6,9)^2+(6,0-8,97)^2)} = 3,43.$

Nach diesen Beobachtungen vermuten wir, dass holmes gerade durch NGOCDA dargestellt wird und MND folglich the ist. Unser Alphabeth nimmt damit die folgende Form an

```
ABCDEFGHIJKLMNOPQRSTUMWXYZ
s  me     o            h l              t
```

Setzen wir alle bereits bekannten Buchstaben ein, dann ergibt sich

```
MNDCGAMQZCGKAGQNGOCDAAUDE
themost  mo so holmess e
PSNDXCDHMAPAMGOUPHMNDZUTD
  he me ts stol   the   e
HMKXDGQMNDUZHEPHLCDHWNPEN
 t  eo the       me  h  h
PHTGOTDAZEPSNDXEGHAPAMPHL
   ol es    he  o s st
GQAMPEICDHDZENSGADXDSXDAD
o st   me e  h ose e  ese
HMPHLZUPAMPHEMODMMDX.
 t      st   tlette .
```

Betrachten wir unseren Lückentext genau, so lässt sich am Ende des Textes das Wort letter erkennen. Wir erhalten

```
MNDCGAMQZCGKAGQNGOCDAAUDE
themost  mo so holmess e
PSNDXCDHMAPAMGOUPHMNDZUTD
  herme ts stol   the   e
HMKXDGQMNDUZHEPHLCDHWNPEN
 t reo the       me  h  h
PHTGOTDAZEPSNDXEGHAPAMPHL
   ol es    her o s st
GQAMPEICDHDZENSGADXDSXDAD
o st   me e  h osere rese
HMPHLZUPAMPHEMODMMDX.
 t      st   tletter.
```

Wir betrachten wiederum die Häufigkeiten der verbleibenden Buchstaben. In unserem Text treten `H`, `P` häufig auf, in der englischen Sprache sind die noch nicht verwendeten häufigsten Buchstaben `n`,`i`,`a`. Die Kombination `CDHC=me*e` in der fünften Zeile unseres Textes lässt vermuten, dass `H` kein Vokal ist, also versuchen wir `H=n`.

```
MNDCGAMQZCGKAGQNGOCDAAUDE
themost  mo so holmess e
PSNDXCDHMAPAMGOUPHMNDZUTD
  herments stol  nthe   e
HMKXDGQMNDUZHEPHLCDHWNPEN
nt reo the  n  n men h  h
PHTGOTDAZEPSNDXEGHAPAMPHL
 n ol es    her ons st n
GQAMPEICDHDZENSGADXDSXDAD
o st   mene  h osere rese
HMPHLZUPAMPHEMODMMDX
nt n    st n tletter.
```

Für `P` betrachten wir die beiden Möglichkeiten

`P=a`

```
MNDCGAMQZCGKAGQNGOCDAAUDE
themost  mo so holmess e
PSNDXCDHMAPAMGOUPHMNDZUTD
a hermentsastol anthe   e
HMKXDGQMNDUZHEPHLCDHWNPEN
nt reo the  n an men ha h
PHTGOTDAZEPSNDXEGHAPAMPHL
an ol es  a her onsastan
GQAMPEICDHDZENSGADXDSXDAD
o sta  mene  h osere rese
HMPHLZUPAMPHEMODMMDX.
ntan   astan tletter.
```

`P=i`

```
MNDCGAMQZCGKAGQNGOCDAAUDE
themost  mo so holmess e
PSNDXCDHMAPAMGOUPHMNDZUTD
i hermentsistol inthe   e
HMKXDGQMNDUZHEPHLCDHWNPEN
nt reo the  n in men hi h
PHTGOTDAZEPSNDXEGHAPAMPHL
in ol es  i her onsistin
GQAMPEICDHDZENSGADXDSXDAD
o sti  mene  h osere rese
HMPHLZUPAMPHEMODMMDX.
ntin   istin tletter.
```

Wir erkennen auf der rechten Seite das Wort `consisting`. Wir versuchen deshalb mit `H=i` weiter aufzulösen.

```
MNDCGAMQZCGKAGQNGOCDAAUDE
themost  mo so holmess ec
PSNDXCDHMAPAMGOUPHMNDZUTD
i hermentsistol inthe   e
HMKXDGQMNDUZHEPHLCDHWNPEN
nt reo the  ncingmen hich
PHTGOTDAZEPSNDXEGHAPAMPHL
in ol es ci herconsisting
GQAMPEICDHDZENSGADXDSXDAD
o stic mene ch osere rese
HMPHLZUPAMPHEMODMMDX.
nting  istinctletter.
```

In der zweiten Zeile erkennen wir das Satzfragment `is told in the`. In der vierten Zeile könnte es `consisting of` heißen.

```
MNDCGAMQZCGKAGQNGOCDAAUDE
themostf mo sofholmessdec
PSNDXCDHMAPAMGOUPHMNDZUTD
i hermentsistoldinthe d e
HMKXDGQMNDUZHEPHLCDHWNPEN
nt reofthed ncingmen hich
PHTGOTDAZEPSNDXEGHAPAMPHL
in ol es ci herconsisting
GQAMPEICDHDZENSGADXDSXDAD
ofstic mene ch osere rese
HMPHLZUPAMPHEMODMMDX.
nting distinctletter.
```

Sowohl `decipherment` in Zeile 1f sowie auch `cipher` in Zeile vier, deuten auf `S=p` hin.

```
MNDCGAMQZCGKAGQNGOCDAAUDE
themostf mo sofholmessdec
PSNDXCDHMAPAMGOUPHMNDZUTD
iphermentsistoldinthe d e
HMKXDGQMNDUZHEPHLCDHWNPEN
nt reofthed ncingmen hich
PHTGOTDAZEPSNDXEGHAPAMPHL
in ol es cipherconsisting
GQAMPEICDHDZENSGADXDSXDAD
ofstic mene chposereprese
HMPHLZUPAMPHEMODMMDX.
nting distinctletter.
```

Wir schließen weiter mit `of the d*ncing men` auf `Z=a`

```
MNDCGAMQZCGKAGQNGOCDAAUDE
themostfamo sofholmessdec
PSNDXCDHMAPAMGOUPHMNDZUTD
iphermentsistoldinthead e
```

```
HMKXDGQMNDUZHEPHLCDHWNPEN
nt reofthedancingmen hich
PHTGOTDAZEPSNDXEGHAPAMPHL
in ol esacipherconsisting
GQAMPEICDHDZENSGADXDSXDAD
ofstic meneachposereprese
HMPHLZUPAMPHEMODMMDX.
ntingadistinctletter.
```

Schließlich ergeben sich die verbleibenden Buchstaben leicht zu:

```
ABCDEFGHIJKLMNOPQRSTUMWXYZ
tsga v ikdrnl oucfehm wp
```

```
MNDCGAMQZCGKAGQNGOCDAAUDE
themostfamousofholmessdec
PSNDXCDHMAPAMGOUPHMNDZUTD
iphermentsistoldintheadve
HMKXDGQMNDUZHEPHLCDHWNPEN
ntureofthedancingmenwhich
PHTGOTDAZEPSNDXEGHAPAMPHL
involvesacipherconsisting
GQAMPEICDHDZENSGADXDSXDAD
ofstickmeneachposereprese
HMPHLZUPAMPHEMODMMDX.
ntingadistinctletter.
```

The most famous of Holmes's decipherments is told in "the adventure of the dancing men", which involves a cipher consisting of stickmen, each pose representing a distinct letter.