Unit 52
Small challenges to go, part 3
Ch 8
H.H. Goldstine macht in seinem Vorwort zu dem Buch von O.I. Franksen „Mr. Babbage's Secret. The Tale of a Cipher – and APL." [5,6,7] folgende Bemerkung zum **Nutzen der Beschäftigung mit der Kryptographie**:
„… During a subsequent visit in the British Library he [O.I. Franksen] procured a set of rather poor photocopies of Babbage's manuscript on ciphers and deciphering. In his spare time over the years since then he has tried to get some meaning out of this unpublished notes, guessing the approach Babbage might have taken, implementing it in APL and painstakingly trying to compare his results with Babbage's in order to discover the special cases which might explain how Babbage actually went about it. In his other historical studies he had accidentally come across other **great scientists who had cultivated an interest in cryptography**

[[1,2,3]], and he started to recognize a common pattern which reminded him of his early computer work.
It struck him that **these great men were primarily problem-solvers with uncanny intuitions, and that deciphering in some way or other had been a training ground for sharpening their insights, their senses of abstract pattern, and their innovative powers in their attempts to cast real life problems into computable mathematical forms.** This discovery intrigued him, and he started developing a cryptographic tool-kit in APL, which he tested by cracking enciphered advertisements from the “agony columns” of Victorians newspapers …”

Wie sicher ist dieses Kryptosystem?
Ein Klartext über dem lateinischen Alphabet (nur Kleinbuchstaben, ohne Wortabstände, Satzzeichen, Sonderzeichen und Zahlen) soll von einem Sender zu einem Empfänger über einen offenen Kanal kryptographisch gesichert (d.h. durch einen nicht autorisierten

Außenstehenden nicht dekodierbar) übertragen werden.
Das Kryptosystem soll vorzugsweise für
** computerfreien (aber auch computergestützten)
** symmetrischen bidirektionalen kryptographisch gesicherten Nachrichtenaustausch (drei oder vier autorisierte Mitempfänger sind denkbar)
** mit kurzen Texten
konstruiert sein.

****

Auf der Senderseite wird der Klartext zunächst mittels nachstehender Kodetabelle (die auch beim Empfänger vorhanden sein muss)

Buchstabe	Zahlenkodewort	B	Z
e	5	u	71
t	1	p	87
r	3	m	70
i	9	y	88
n	2	g	75
o	6	w	79
a	0	v	85
s	4	b	74
d	78	x	77
l	84	k	81
c	89	q	83
h	73	j	72
f	86	z	82

linksbündig quasioptimal in einen (eindeutig und unverzögert dekodierbaren) zahlenkodierten Klartext
= Dezimalziffernfolge transformiert:
Zahlenkodierung.
****

Nun erfolgt von links beginnend eine **Segmentierung** dieses Textes in eine Folge von „Zehnergruppen“ = zehnstellige Dezimalziffernfolgen

$X_i = x_{i0}\ x_{i1}\ x_{i2}\ x_{i3}\ x_{i4}\ x_{i5}\ x_{i6}\ x_{i7}\ x_{i8}\ x_{i9}$

$x_{ik} \in \{0,1,2,3,4,5,6,7,8,9\};\ i=1,2,3,..,n$

==========

Beispiel 1.1

Text:

Wohin willst du Schnecke bei diesem Regen?

Klartext:

wohinwillstduschneckebeidiesemregen

zahlenkodierter Klartext:

79673927998484417871489732589815745978954570357552

Zehnergruppen X_i:

X_1=7967392799

X_2=8484417871

X_3=4897325898

X_4=1574597895

X_5=4570357552

==========

****

Jetzt startet der **erste Schritt der**

Kryptokodierung mit der Generierung der kryptographischen Schlüssel.
** Dazu wird für jede Zehnergruppe X_i
ein anderer krytographischer Schlüssel S_i
benutzt. Dieser ist ebenfalls eine Zehnergruppe
= zehnstellige Dezimalziffernfolge

$S_i = s_{i0}\ s_{i1}\ s_{i2}\ s_{i3}\ s_{i4}\ s_{i5}\ s_{i6}\ s_{i7}\ s_{i8}\ s_{i9}$

$s_{ik} \in \{0,1,2,3,4,5,6,7,8,9\}$; i=1,2,3,..,n

** Die nacheinander zu benutzenden S_i ;
i=1(1)n entstehen durch 10-Segmentierung
einer von links nach rechts aufgebauten
dezimalen Pseudozufallsziffernfolge (dP).
** Diese dP soll im vorliegenden Falle den
„Statistischen Jahrbüchern “ des Statistischen
Bundesamtes der Jahre 19ΔΔ bis 2013
entnommen werden. Sie müssen bei Sender
und Empfänger vorhanden sein.[1)2)]
** Die dP ist eindeutig bestimmt durch die
Schlüsselinformation (geheimer Schlüssel) =
zehnstellige Dezimalziffernfolge

$S = s_0 s_1 s_2 s_3 s_4 s_5 s_6 s_7 s_8 s_9$; $s_k \in \{0,1,2,\ldots,9\}$.

Hierbei sind

s_2 dritte Ziffer der Jahrgangszahl des vom Sender ausgewählten Jahrbuches

s_5 vierte Ziffer der Jahrgangszahl

$s_0s_4s_6$ Seitenzahl (Seite 9 = Seite 009) in diesem Jahrbuch

s_1s_8 Zeilennummer (von oben gezählt) im Zahlenteil auf Seite $s_0s_4s_6$

s_7 Spaltennummer (von links gezählt) im Zahlenteil auf Seite $s_0s_4s_6$.

s_3, s_8 und **s_9** sind Navigationsanweisungen:

** Starte das Auslesen der dP auf Seite $s_0s_4s_6$ im Zahlenteil, Zeile s_1s_8, Spalte s_7 mit der (**s_3**-ten Ziffer vom rechten s_7-Rand gezählt) nach links bis zum linken Rand der Zeile s_1s_8 fortschreitend, dabei werden Nichtziffern und jede **s_8**-te Ziffer übergangen.

Ist (**s_9** + letzte so aus Zeile s_1s_8 ausgelesene Ziffer) $\begin{cases}\text{gerade}\\\text{ungerade}\end{cases}$, wird das Auslesen der dP aus der nächstoberen Zeile $\begin{cases}\text{von links nach rechts}\\\text{von rechts nach links}\end{cases}$ bis zum $\begin{cases}\text{rechten}\\\text{linken}\end{cases}$ Zeilenende fortgesetzt. Auch dabei werden Nichtziffern, space und jede **s_8**-te

Ziffer übergangen. Am jeweiligen Zeilenende wird das Auslesen der dP wie zuvor beschrieben fortgesetzt.
Das „so Auslesen der letzten Ziffer einer Zeile“ erfolgt unabhängig vom Auslesen des dP-Anteiles aus dieser Zeile.
Usf. bis zum Ende der benötigten dP.

Beispiel 1.2 S $\rightarrow$ dP $\rightarrow$ S_i

Basis:
Statistisches Jahrbuch Deutschland und Internationales 2012
ISBN 978-3-8246-0989-5
https://www.destatis.de/DE/Publikationen/StatistischesJahrbuch/StatistischesJahrbuch2012.pdf?__blob=publicationFile
oooooooooooooooooooooooooooooooooooooooooooooo

Jahrgang 2012, Seite 271,
im Zahlenteil Zeile 12, Spalte 5,

s_3=2, s_8=2, s_9=5$\rightarrow$

Schlüsselinformation
$S = s_0s_1s_2s_3s_4s_5s_6s_7s_8s_9 = 2112721525$
oooooooooooooooooooooooooooooooooooooooooooooo

Im Zahlenteil Zeile 12, dP-Auslesen nach links

58911#2459 259#41745#38194#2231459#58424

Spalte 5, s_3 =2, s_9 =5 $\rightarrow$

dP = **5**1241341925218#

Ist ($\mathbf{s_9}$ =5 + letzte aus Zeile s_1s_8 =12 ausgelesene Ziffer=5) $\begin{cases} =10^{\text{gerade}} \\ \end{cases}$, wird das Auslesen der dP aus der nächstoberen Zeile 11

$\begin{cases} \text{von links nach rechts} \\ \end{cases}$ bis zum $\begin{cases} \text{rechten} \\ \end{cases}$

Zeilenende fortgesetzt. Auch dabei werden Nichtziffern, space und jede $\mathbf{s_8}$ =2-te Ziffer übergangen.

oooooooooooooooooooooooooooooooooooooooooooo

Zeile 11

405353022724745713315829523568903<u>9</u>

dP = **5**1241341925218#4550227513525369З#

Am jeweiligen Zeilenende wird das Auslesen der dP wie zuvor beschrieben fortgesetzt.

Ist ($\mathbf{s_9}$ =5 + letzte aus Zeile 11 ausgelesene Ziffer=9) $\left\{ \right.$ =14 $\left\{ \right.$ gerade , wird das Auslesen der dP aus der nächstoberen Zeile 10 $\left\{ \right.$ von links nach rechts $\left\{ \right.$ bis zum $\left\{ \right.$ rechten Zeilenende fortgesetzt. Auch dabei werden Nichtziffern, space und jede $\mathbf{s_8}$ =2-te Ziffer übergangen.

Zeile 10
4022365358839298228317661 5
dP = **5**1241341925218#4550227513525 3693#
423558992816 1#

Am jeweiligen Zeilenende wird das Auslesen der dP wie zuvor beschrieben fortgesetzt.

Ist ($\mathbf{s_9}$ =5 + letzte aus Zeile 10 ausgelesene Ziffer=5) $\left\{ \right.$ =10 $^{\text{gerade}}$, wird das Auslesen der dP aus der nächstoberen Zeile 9 $\left\{ \right.$ von links nach rechts bis zum $\left\{ \right.$ rechten Zeilenende fortgesetzt. Auch dabei werden Nichtziffern, space und jede $\mathbf{s_8}$ =2-te Ziffer übergangen.

Zeile 9
230616019369 4681537149772974 4
dP = **5**1241341925218#45502275135253693#
423558992816 1#201096485747274#

Am jeweiligen Zeilenende wird das Auslesen der dP wie zuvor beschrieben fortgesetzt.

Ist ($\mathbf{s_9}$ =5 + letzte aus Zeile 9 ausgelesene Ziffer=$\underline{4}$) $\left\{ \begin{array}{l} =9 \\ \text{ungerade} \end{array} \right.$, wird das Auslesen der dP aus der nächstoberen Zeile 8

$\left\{ \begin{array}{l} \text{von rechts nach links} \end{array} \right.$ bis zum $\left\{ \begin{array}{l} \text{linken} \end{array} \right.$ Zeilenende fortgesetzt. Auch dabei werden Nichtziffern, space und jede $\mathbf{s_8}$ =2-te Ziffer übergangen.

Zeile 8
27081838466789018351726039 4062
dP = **5**12413419252 18#45502275135253693#
423558992816 1#201096485747274#
209021319768887#
Stop.

Die nacheinander zu benutzenden S_i (i=1,2,3,..) entstehen durch 10-Segmentierung der so erhaltenen dP (das Trennzeichen # wird dabei ignoriert):

S_1=5124134192
S_2=5218455022
S_3=7513525369
S_4=3423558992

S_5=8161201096

==========

****

Nun der zweite Schritt, die Generierung des Ciphertexts auf der Senderseite aus dem zahlenkodierten Klartext und den kryptographischen Schlüsseln. Dabei ist der Ciphertext ebenfalls eine Folge von Zehnergruppen = zehnstellige Dezimalziffernfolgen

$Y_i = y_{i0}\ y_{i1}\ y_{i2}\ y_{i3}\ y_{i4}\ y_{i5}\ y_{i6}\ y_{i7}\ y_{i8}\ y_{i9}$

$y_{ik} \in \{0,1,2,3,4,5,6,7,8,9\}$; i=0,1,2,3,..,n

Diese werden aus den X_i, den S_i und S durch „positionsweise Addition modulo 10“ [3] gebildet:

Im Kopf des Ciphertextes steht die Zehnergruppe

$Y_0 = S \boxplus Y_k \boxplus Y_{n-m}$,

die kontextabhängig kodierte Schlüsselinformation.

Dabei sind k und m zwischen Sender und Empfänger vereinbart, z.B. k=m=2.

Ihr folgen die die zu übermittelnde kodierte Information enthaltenden Zehnergruppen

$Y_1, Y_2, \ldots, Y_n$ mit

$Y_i = X_i \boxplus S_i;\ i=1(1)n$.

Der Ciphertext $Y_0Y_1Y_2\ldots Y_n$ [4)] ist damit (wie der zahlenkodierte Klartext $X_1X_2\ldots X_n$) eine Dezimalziffernfolge.

==========

Beispiel 1.3

n=5, k=m=2

X_1=7967392799

X_2=8484417871

X_3=4897325898

X_4=1574597895

X_5=4570357552

S =2112721525

S_1=5124134192

S_2=5218455022

S_3=7513525369
S_4=3423558992

S_5=8161201096 $\rightarrow$

$Y_1=X_1 \boxplus S_1$=2081426881

$Y_2=X_2 \boxplus S_2$=3692862893

$Y_3=X_3 \boxplus S_3$=1300840157

$Y_4=X_4 \boxplus S_4$=4997045787

$Y_5=X_5 \boxplus S_5$=2631558548

$Y_0=S \boxplus Y_2 \boxplus Y_3$=6004323465

Ciphertext $Y_0Y_1Y_2\ldots Y_n$ =
6004323465208142688136928628931300840
157499704578726315585 48
==========

Diese kann nun direkt oder nach weiterer zwischen Sender und Empfänger vereinbarter Transportkodierung

binäre Optimal- + Kanalkodierung,

Z→B mittels der bei der Zahlenkodierung benutzten Codetabelle, …

über einen offenen Kanal

geschriebener Text auf Datenträger,
email, Skype,

Handy,
QR, …
zum Empfänger übertragen werden.
****

Nach entsprechender Transportdekodierung liegt dem autorisierten Empfänger der Ciphertext vor. Damit ist n bestimmt:

$$n = \frac{\text{length(Ciphertext)}}{10} - 1 .$$

Der Ciphertext wird nun in die Zehnergruppen $Y_0, Y_1, Y_2, \ldots, Y_n$ segmentiert.

==========

Beispiel 1.4

Empfangener Ciphertext=
600432346520814268813692862893130084015749970457872631558548 $\rightarrow$

n=5

Y_0=6004323465
Y_1 =2081426881
Y_2 =3692862893
Y_3 =1300840157
Y_4 =4997045787
Y_5= 2631558548

==========

****

Der autorisierte Empfänger berechnet jetzt zuerst die Schlüsselinformation

$S = Y_0 \boxminus (Y_k \boxplus Y_{n-m})$

und bestimmt damit - wie auf der Senderseite beschrieben - die kryptographischen Schlüssel S_i ; i=1(1)n .

==========

Beispiel 1.5

n=5 ; k=m=2

$S = Y_0 \boxminus (Y_2 \boxplus Y_3)$

= 6004323465

$\boxminus$ (3692862893

$\boxplus$ 1300840157)

= 6004323465

$\boxminus$ 4992602940

= 2112721525 $\rightarrow$

$S_1 = 5124134192$

$S_2 = 5218455022$

$S_3 = 7513525369$

$S_4 = 3423558992$

$S_5 = 8161201096$

****

Mit diesen können die Segmente des zahlenkodierten Klartextes

$X_1 = Y_1 \boxminus S_1$

$X_2 = Y_2 \boxminus S_2$

$X_3 = Y_3 \boxminus S_3$

$X_4 = Y_4 \boxminus S_4$

$X_5 = Y_5 \boxminus S_5$

und damit der zahlenkodierte Klartext=
$X_1\ X_2\ X_3\ X_4\ X_5$
bestimmt werden.

==========

Beispiel 1.6

$X_1 = Y_1 \boxminus S_1 = 7967392799$

$X_2 = Y_2 \boxminus S_2 = 8484417871$

$X_3 = Y_3 \boxminus S_3 = 4897325898$

$X_4 = Y_4 \boxminus S_4 = 1574597895$

$X_5 = Y_5 \boxminus S_5 = 4570357552$

zahlenkodierter Klartext=
7967392799848441787148973258981574597895457035755 2

==========

****

Aus diesem ergibt sich schließlich mit der Kodetabelle Z→B der kryptographisch gesichert übertragene Klartext.

==========

Beispiel 1.7

79 6 73 9 2 79 9 84 84 41787148973

↓↓ ↓↓↓ ↓ ↓ ↓ ↓

w o h i n w i l l

25898157459789545703 5 75 5 2

↓↓ ↓↓↓

r e g e n

****

1) Vgl. [3,4,5].
2) Natürlich können dazu auch andere ähnliche ubiquitäre Zahlenwerke oder algorithmische Pseudozufallszahlengeneratoren [5] benutzt werden.
3)

$A = a_0a_1a_2a_3a_4a_5a_6a_7a_8a_9$

$B = b_0b_1b_2b_3b_4b_5b_6b_7b_8b_9$

$C = c_0c_1c_2c_3c_4c_5c_6c_7c_8c_9$

Positionsweise Addition und

Subtraktion modulo 10

$A \boxplus B = C \quad \text{mit} \quad \forall i \; c_i = (a_i + b_i) \bmod 10$

$A \boxminus B = C \quad \text{mit} \quad \forall i \; c_i = (a_i - b_i) \bmod 10$

Eigenschaften:

** $A \boxplus B = B \boxplus A$

** $A \boxplus (B \boxplus C) = (A \boxplus B) \boxplus C$

** Aus $C = A \boxplus B$ folgt $A = C \boxminus B$

und $B = C \boxminus A$.

** $A \boxplus B$ ist Gruppenoperation.

4) Die Positionierung der kontextabhängig kodierten Schlüsselinformation Y_0 kann natürlich auch anders vereinbart werden, z.B. zwischen Y_3 und Y_4 .

Fragen

** Wie sicher ist dieses Kryptosystem?

** Wo liegen seine Schwachstellen?

** Wie könnte man es sicherer machen?

** Was geschieht, wenn der Sender zweimal hintereinander das gleiche S zum Kryptokodieren von zwei verschiedenen Klartexten benutzt?

** Was geschieht, wenn senderseitig oder bei der Übertragung im Ciphertext in einer Position eine zufällige Verfälschung (z.B. 3→7) auftritt? Lässt sich dann empfängerseitig der Klartext wiederherstellen?
Wenn nicht, wie kann man eine Einfehlererkennung (vgl. [9])/ -lokalisierung/-korrektur in das beschriebene Kryptosystem einbauen (vgl. binäre Kanalkodierung [10])?
Genauer formuliert:
Wieviel Kontrollstellen muss man einem zehnstelligen dezimalen Zahlenwort Y_i mindestens anfügen, damit eine Verfälschung in einer Stelle mit Sicherheit erkannt/ lokalisiert/korrigiert werden kann?
Wie sind die Kontrollstellen zu berechnen?
Wie erfolgen Fehlererkennung/-lokalisierung/-korrektur? Gefragt ist die eleganteste Lösung (maybe matrix

representation over ($\mathbb{N}^n$, a⊞b)?)

** Diskutieren Sie andere Anwendungen der Operationen a⊞b und a⊟b.

References

[1] http://de.wikipedia.org/wiki/Kryptographie

[2] http://en.wikipedia.org/wiki/Cryptography

In [1] und [2] umfangreiches Literaturverzeichnis zur Kryptographie.

[3] D. Kahn. The Codebreakers: The Comprehensive History of Secret Communication from Ancient Times to the Internet. Scribner, New York 1996. ISBN 978-0-684-83130-5

[4] J. Mader. Dr.-Sorge-Report. Berlin 1984

[5] C. Pöppe. Kryptograpie. Freund liest mit. Spektrum der Wissenschaft Mai 2014, S. 20-22

[6] O.I. Franksen. Mr. Babbage's Secret. The Tale of a Cipher – and APL. Strandbergs Forlag, Birkerod 1984

[7] http://en.wikipedia.org/wiki/Charles_Babbage http://de.wikipedia.org/wiki/Charles_Babbage

[8] http://en.wikipedia.org/wiki/APL_(language)

http://de.wikipedia.org/wiki/APL_(Programmiersprache)
[9] http://en.wikipedia.org/wiki/Check_digit
http://de.wikipedia.org/wiki/Prüfziffer
[10] D. Schönfeld, H. Klimant, R. Piotraschke. Informations- und Kodierungstheorie. ISBN 978-3-8348-0647-5

Lateral

Well-known, publicly available and until now not yet decrypted ciphertexts, waiting for you.

[11] http://en.wikipedia.org/wiki/Kryptos
http://de.wikipedia.org/wiki/Kryptos_(Skulptur)
[12] http://en.wikipedia.org/wiki/Voynich_manuscript
http://de.wikipedia.org/wiki/Voynich-Manuskript
[13] http://www.welt.de/wissenschaft/article13746896/Diese-Geheimschrift-laesst-Kryptologen-verzweifeln.html
[14] http://www.golem.de/1110/87314.html