Fachdidaktik I, HS 2023 Martin Pfister

Kryptosystem nach Vorbild von Vigenère unter Einbezug natürlicher Alphabete

1. Vorwissen und Zielsetzungen

Die Einheit ist eine Vertiefung und Ergänzung nach dem Kapitel 2 „Geheimschriften und Datensicherheit“ von 2-4 Lektionen inkl. Vorbereitungsauftrag und Hausaufgaben.

Inhaltlich ist die Einheit interdisziplinär angelegt und öffnet den Schülerinnen und Schülern Zugang zu dem, was die Sprachwissenschaft über Schriften und ihre Eigenschaften weiss. Dieses Wissen soll wiederum genutzt werden, um ein eigenes Kryptosystem nach dem Vorbild von Vigenère zu entwickeln.

In einer vorgelagerten Vorbereitungsaufgabe soll der Klasse bewusst werden, dank welcher Eigenschaften Alphabete sich als Grundlage für Geheimschriften eignen. Die Schüler sollen erkennen, dass der fixierten Reihenfolge der Buchstaben eine Schlüsselrolle zukommt. Nur sie erlaubt eine praktikable Matrix, auf welcher die Transpositionsalgorithmen von Caesar bis Vigenère angewandt werden.

Ein Vergleich mit anderen Schriftsystemen soll alternative Ordnungsprinzipien zeigen, die ebenfalls fest verfügbar sind und von kulturellen Faktoren abhängig sind.

Nun soll die Aufgabe sein, im polyalphabetischen Verfahren nach Vigenère positionsbedingt nicht nur den Schlüssel zu wechseln, sondern das ganze alphabetische Bezugssystem. Die indische, Inuit- und japanische Schrift soll dabei die Ordnung liefern.

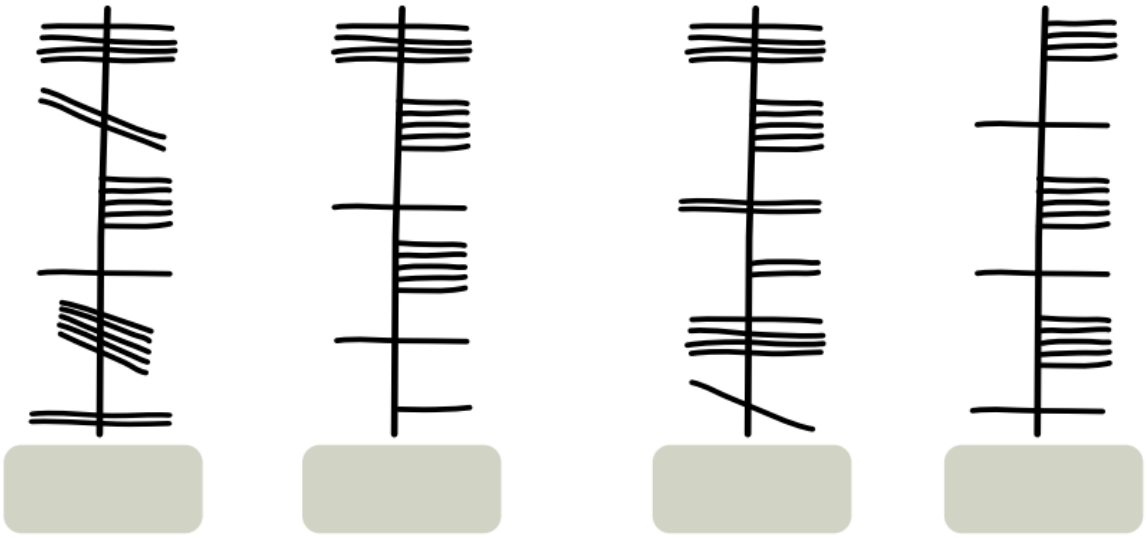
Anschliessend soll die Friedman’sche Charakteristik geprüft werden und beurteilt werden, ob ein Angriff mit stochastischen Methoden, selbst bei kürzestem Schlüssel, noch eine Chance hat.

Nach diesem Zwischenerfolg sollen die Schülerinnen und Schüler Stärken und Schwächen des bisher entwickelten Kryptosystems beurteilen. Es werden Ideen gesucht, um den Wechsel der Alphabete nicht zyklisch zu iterieren, sondern deren Abfolge besser zu verschleiern. Mit der Idee der Fibonacci-Folge, deren Glieder jeweils modulo 4 gerechnet werden, haben wir zudem einen Ansatz, der auch für das Programmieren eine wertvolle Zusatzübung darstellt.

Je nach Zeitbudget können die Programme in Python vorgegeben oder als Programmieraufgabe gelöst werden.

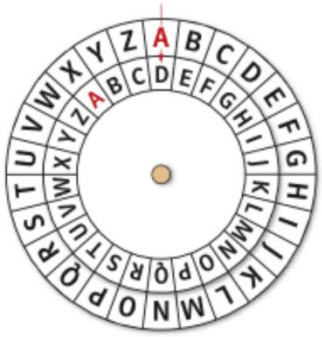
2. Unterlagen für Schülerinnen und Schüler

Vorbereitungsaufgabe 1: Versuchen sie die Wörter in lateinischer Schrift den Wörtern in der altirischen Ogham-Schrift zuzuordnen[1]. Überlegen Sie dabei, welche Eigenschaften Alphabete haben müssen, damit dies überhaupt gelingen kann.



ANANAS BANANE MELONE ORANGE

Vorbereitungsaufgabe 2: Gehen sie die Beispiele und Übungen des Kapitels 2 nochmals im geistigen Auge durch. Welches Element bleibt in allen Verfahren unverändert?

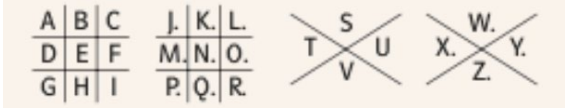


Beispiel 2.3, S. 58

Beispiel 2.2, Seite 53

	1	2	3	4	5	6	7	8	9
○	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	

Geschichtlicher Kontext, Seite 55



[1] Biber-Wettbewerb 2023, SVIA

***Wir halten fest**: ……*

……..

……..

……

(siehe Lösungen)

Andere Schriftsysteme der Menschheit

Arbeiten sie in 3 Gruppen an je einer der folgenden Schriften. Lesen sie den linguistischen Exkurs in den Lösungen. Arbeiten sie die Unterschiede zum Lateinischen heraus.

A Das Indische Devanagari

अ	आ	इ	ई	उ	ऊ
a	ā	i	ī	u	ū
ऋ	ॠ	ऌ			
ṛ	ṝ	ḷ			
ए	ऐ	ओ	औ		
e	ai	o	au		
◌ं	◌ः				
(ṃ)	(ḥ)				
क	ख	ग	घ	ङ	
ka	kha	ga	gha	ṅa	
च	छ	ज	झ	ञ	
ca	cha	ja	jha	ña	
ट	ठ	ड	ढ	ण	
ṭa	ṭha	ḍa	ḍha	ṇa	
त	थ	द	ध	न	
ta	tha	da	dha	na	
प	फ	ब	भ	म	
pa	pha	ba	bha	ma	
य	र	ल	व	स	
ya	ra	la	va	sa	

B Das Abugida Inuktitut Syllabar (Inuit)

ᐃ	i	ᐅ	u	ᐊ	a	ᐦ	h
ᐱ	pi	ᐳ	pu	ᐸ	pa	ᐨ	p
ᑎ	ti	ᑐ	tu	ᑕ	ta	ᑦ	t
ᑭ	ki	ᑯ	ku	ᑲ	ka	ᑲ	k
ᒋ	gi	ᒍ	gu	ᒐ	ga	ᒐ	g
ᒥ	mi	ᒧ	mu	ᒪ	ma	ᒪ	m
ᓂ	ni	ᓄ	nu	ᓇ	ᓐ	n	
ᓯ	si	ᓯ	su	ᓴ	sa	ᓴ	s
ᓪ	li	ᓫ	lu	ᓬ	la	ᓬ	l
ᔨ	ji	ᔪ	ju	ᔭ	ja	ᔭ	j
ᕀ	vi	ᕁ	vu	ᕃ	va	ᕃ	v
ᕆ	ri	ᕇ	ru	ᕋ	ra	ᕋ	r
ᖁ	qi	ᖃᓄ	qu	ᖃᓇ	qa	ᖃᓇ	q
ᖽᐊ	ngi	ᖽᐊᓄ	ngu	ᖽᐊᓇ	nga	ᖽᐊᓇ	ng
ᒃ	cłi	ᒃᓄ	cłu	ᒃᓇ	cła	ᒃᓇ	cł

C Das Japanische Katakana

ア	a	イ	i	ウ	u	エ	e	オ	o		
カ	ka	キ	ki	ク	ku	ケ	ke	コ	ko	キャ	kya
サ	sa	シ	si	ス	su	セ	se	ソ	so	シャ	sha
タ	ta	チ	ti	ツ	tu	テ	te	ト	to	チャ	cha
ナ	na	ニ	ni	ヌ	nu	ネ	ne	ノ	no	ニャ	nya
ハ	ha	ヒ	hi	フ	fu	ヘ	he	ホ	ho	ヒャ	hya
マ	ma	ミ	mi	ム	mu	メ	me	モ	mo	ミャ	mya
ヤ	ya	†	yi	ユ	yu	†	ye	ヨ	yo		
ラ	ra	リ	ri	ル	ru	レ	re	ロ	ro	リャ	rya
ワ	wa	ヰ	wi	†	wu	ヱ	we	ヲ	wo		
ガ	ga	ギ	gi	グ	gu	ゲ	ge	ゴ	go		
ザ	za	ヅ	zi	ズ	zu	ゼ	ze	ゾ	zo		
ダ	da	ヂ	di	ヅ	du	デ	de	ド	do		
バ	ba	ビ	bi	ブ	bu	ベ	be	ボ	bo		
パ	pa	ピ	pi	プ	pu	ペ	pa	ポ	Po		

Diskussion der präsentierten Vergleiche:

……..

……..

……

……

(siehe Lösungen)

Nutzung für kryptologische Zwecke

Wir versuchen, unserem lateinischen Alphabet 3 neue alternative Anordnungen zu geben. Dabei folgen wir den 3 untersuchten Schriften und tragen die Buchstaben der Reihe nach so in die Tabelle ein, wie sie in der jeweiligen Schrift angeordnet sind. Bei uns nicht vorkommende Laute lassen wir aus. Am Schluss tragen wir alle Buchstaben, die im Alphabet nicht vorkommen, nach und füllen die Tabelle bis zum Platz 26 alphabetisch auf.

Latein	A	B	C	D	E	F	G	H	I	J	K	L	M
Indisch													
Inuit													
Katakana													

Latein	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Indisch													
Inuit													
Katakana													

(Siehe Lösungen)

Wir nehmen nun das Beispiel 2.7, Seite 67 als Vorlage (Kryptosystem nach Vigenère)

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

Im Beispiel 2.8, Seite 69 haben wir einen Angriff bei bekannter Schlüssellänge kennengelernt. Dabei ergeben alle Positionen auf einem Vielfachen der Schlüssellänge eine Menge, die sich stochastisch untersuchen lässt. Aber eben auch nur, weil an dieser Position wieder gleich chiffriert wird. Was wäre, wenn nicht? Was wäre, wenn wir, bei gleichem Schlüssel, nach jedem Buchstaben das zugrunde liegende Alphabet wechseln?

Wir verschlüsseln nach Vigenère mit dem kurzen Schlüssel „**key**“, wechseln aber nach jedem Buchstaben das Alphabet.

- Überlegen sie, unter welchen Umständen der Kasiski-Test noch funktionieren wird.

Angenommen, wir würden immer dieselbe Reihenfolge der Alphabete durchspielen: Latein, Indisch, Inuit, Japanisch und dann wieder von vorne:

- Wie sollte sich die Schlüssellänge (hier 3) zur Anzahl der rotierenden Alphabete idealerweise verhalten?

- Überlegen sie, ob es bessere Lösungen gibt als die gleichförmige Wiederholung derselben Alphabet-Abfolge.

Von den diskutierten Möglichkeiten nehmen wir uns die Fibonacci-Folge vor.

1, 1, 2, 3, 5, 8, 23, …

Wie sie aus der Mathematik wissen, ist ihre Bildungsregel:

$f_n = f_{n-1} + f_{n-2}$ für $n \geq 3$

Anfangswerte: $f_1 = f_2 = 1$

Wie sie aus dem Programmierunterricht schon wissen, lässt sich die Fibonacci-Folge rekursiv oder iterativ programmieren. Auf Rekursion sollten wir verzichten, da bei längeren Texten sonst die Gefahr eines Stack Overflows real ist.

Zur Erinnerung die iterative Programmierweise am Beispiel der ersten 10 Glieder:

```
def fibonacci(n):
    a, b = 0, 1
    for i in range(n+1):
        a, b = b, a + b

    return a


for i in range(10):
    print(fibonacci(i))
```

Es existiert aber auch die Möglichkeit, das n-te Glied direkt zu berechnen, mit Moivre-Binet:

$$f_n = \frac{1}{\sqrt{5}}\left(\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n\right)$$

- Aufwärmübung: Setzen sie die Formel in Python um und berechnen sie das 10-te Glied, zum Vergleich mit der bekannten iterativen Programmierweise.

Das wollen wir nun tun:

Verschlüsseln sie die Botschaft so, dass jedem Buchstaben der Reihe nach ein Glied der Fibonacci-Folge zugewiesen wird, dessen Wert aber modulo 4 gerechnet wird. Je nach Ergebnis wird bei 0 das lateinisch, bei 1 das indische, bei 2 das Inuit- und bei 3 das japanische Alphabet zugrunde gelegt.

Programmieren mit Python

Schreiben sie ein Programm, das Texte mit beliebig langen Schlüsseln und den 4 Alphabeten in oben beschriebener Weise verschlüsselt.

- Verschlüsseln sie mit dem Programm und dem Schlüssel ***key*** die ersten beiden Abschnitte der Zusammenfassung auf Seite 77:

Dasbeduerfnisdatenvorunbefugtenzuschuetzenistmindestenssoaltwiedieschriftenselbstdiekryptologi edielehredergeheimschriftenistmindestensjahrealtsiebestehtausdenteilenkryptographiediewissensch aftdesentwurfsvonkryptosystemenundkryptoanalysedieentwicklungvonmethodenzumbrechenvonkry ptosystemendieaeltestengeheimschriftenderantikebsiertenaufsubstitutionenundtranspositionendied atensicherheitbasiertedamalsaufdiegeheimhaltungderganzengeheimschriftweshalbdiegeheimschriftn ichtschriftlichaufbewahrtwerdendurfteundsomitauswendiggelerntwerdenmusste

- Ermitteln sie die Friedman'sche Charakteristik mithilfe des Programms aus 2.41
- Gehen sie auf einfachinformatik, unter Lernumgebungen auf **Geheimschriften und Datensicherheit**: *Offene Knobelaufgabe, Entschlüssele einen frei gewählten Geheimtext*. Visualisieren sie dort die relative Häufigkeit der Buchstaben im Geheimtext gegenüber jener des Deutschen.

Fazit:

- Was haben sie über die Art und Funktionsweise von natürlichen Schriften gelernt?
- Welcher Vorteil bietet die Orientierung der Alphabet-Reihenfolge nach existierenden Schriften?
- Welche Auswirkung hat die Verwendung von polyalphabetisch unterschiedlichen Alphabeten gezeigt?