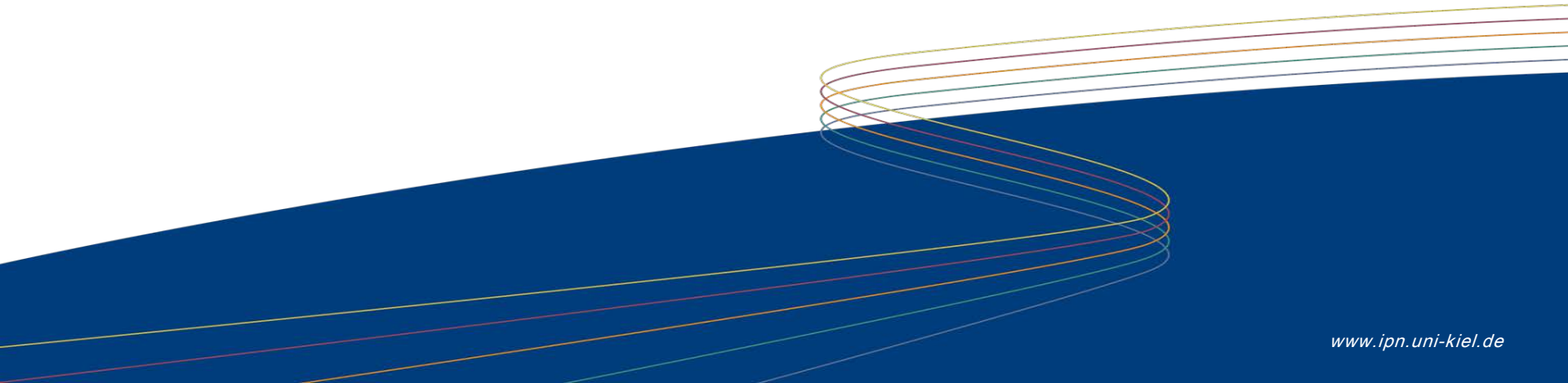
Leibniz Gemeinschaft

IPN
Leibniz-Institut für die Pädagogik der Naturwissenschaften und Mathematik

Die Vigenère-Verschlüsselung

Krypto-Camp 2019



Historisches

- Namensgeber: Blaise de **Vigenère** (1523 –1596)
- Verbesserung der Cäsar-Verschlüsselung
- Vergrößerung des Schlüsselraums
- Konnte erstmals um 1850 systematisch geknackt werden.

Die Vigenère-Verschlüsselung

Voraussetzung:

- Buchstaben aus dem lateinischen Alphabet
- Sender und Empfänger haben gleichen Schlüssel

Vorgehen:

- Ein Buchstabe wird wie bei der Cäsar-Verschlüsselung verschoben.
- **Aber** nicht jeder Buchstabe um den gleichen Wert.

Der Schlüssel im Vigenère-Verfahren

- Buchstaben werden um verschiedene Werte verschoben
- Schlüssel besteht nicht aus einer Zahl, sondern aus mehreren, oder:
- Um sich den Schlüssel besser merken zu können: **Schlüsselwort**

Beispiel für ein Schlüsselwort

- **Schlüsselwort:** „baum“
- In Zahlen: 1 0 20 12

- **Cäsar-Scheibe:** Stelle innen Buchstaben statt Zahl ein.
- **„am PC“:** `finde_position()`

Vigenère-Verschlüsselung

- Nachricht: „bewegungerwartet“
- Schlüssel: „hallo“

Nachricht:	b	e	w	e	g	u	n	g	e	r	w	a	r	t	e	t
Schlüssel:																

Vigenère-Verschlüsselung

- Nachricht: „bewegungerwartet“
- Schlüssel: „hallo“

Nachricht:	b	e	w	e	g	u	n	g	e	r	w	a	r	t	e	t
Schlüssel:	h	a	l	l	o											

Vigenère-Verschlüsselung

- Nachricht: „bewegungerwartet“
- Schlüssel: „hallo“

Nachricht:	b	e	w	e	g	u	n	g	e	r	w	a	r	t	e	t
Schlüssel:	h	a	l	l	o	h	a	l	l	o						

Vigenère-Verschlüsselung

- Nachricht: „bewegungerwartet“
- Schlüssel: „hallo“

Nachricht:	b	e	w	e	g	u	n	g	e	r	w	a	r	t	e	t
Schlüssel:	h	a	l	l	o	h	a	l	l	o	h	a	l	l	o	

Vigenère-Verschlüsselung

- Nachricht: „bewegungerwartet“
- Schlüssel: „hallo“

Nachricht:	b	e	w	e	g	u	n	g	e	r	w	a	r	t	e	t
Schlüssel:	h	a	l	l	o	h	a	l	l	o	h	a	l	l	o	h

Vigenère-Verschlüsselung

Der Nachrichten-Buchstabe wird um den Schlüsselbuchstaben „verschoben“.

Nachricht:	b	e	w	e	g	u	n	g	e	r	w	a	r	t	e	t
Schlüssel:	h	a	l	l	o	h	a	l	l	o	h	a	l	l	o	h

Auftrag Nr. 1:

- Verschlüssele die Nachricht mit dem Vigenère-Verfahren.

Nachricht:	b	e	w	e	g	u	n	g	e	r	w	a	r	t	e	t
Schlüssel:	h	a	l	l	o	h	a	l	l	o	h	a	l	l	o	h

Auftrag Nr. 1:

- Verschlüssele die Nachricht mit dem Vigenère-Verfahren.

Nachricht:	b	e	w	e	g	u	n	g	e	r	w	a	r	t	e	t
Schlüssel:	h	a	l	l	o	h	a	l	l	o	h	a	l	l	o	h
Chiffre:	i	e	h	p	u	b	n	r	p	f	d	a	c	e	s	a

Verschlüsseln mit der Vigenère-Tabelle

- Nachrichten-Buchstaben in der obersten Zeile finden.
- Schlüssel-Buchstaben in der Spalte ganz links finden.
- Schnittpunkt von Zeile und Spalte ist die Chiffre.

Auftrag Nr. 2:

- Verschlüssele die Nachricht mit dem Vigenère-Verfahren.

Nachricht:	v	o	r	z	e	i	t	i	g	a	b	b	r	e	c	h	e	n
Schlüssel:	v	i	g	e	n	e	r	e	v	i	g	e	n	e	r	e	v	i
Chiffre:																		

Auftrag Nr. 2:

- Verschlüssele die Nachricht mit dem Vigenère-Verfahren.

Nachricht:	v	o	r	z	e	i	t	i	g	a	b	b	r	e	c	h	e	n
Schlüssel:	v	i	g	e	n	e	r	e	v	i	g	e	n	e	r	e	v	i
Chiffre:	q	w	x	d	r	m	k	m	b	i	h	f	e	i	t	l	z	v

Entschlüsseln mit der Vigenère-Tabelle

- Schlüssel-Buchstaben in der Spalte ganz links finden.
- In der gleichen Zeile nach rechts, bis zum Chiffre-Buchstaben gehen.
- Der Klartext-Buchtstabe steht in der gleichen Spalte, wie der, oben gefundene, Chiffre-Buchstabe.

Auftrag Nr. 3

- Entschlüssele die Nachricht mit dem Vigenère-Verfahren.

Chiffre:	p	s	u	n	q	l	a	y	g	f	e	a	j	s	c	w	o	h	g	h	h
Schlüssel:	k	o	m	a	n	d	o	k	o	m	a	n	d	o	k	o	m	a	n	d	o
Nachricht:																					

Auftrag Nr. 3

- Entschlüssele die Nachricht mit dem Vigenère-Verfahren.

Chiffre:	p	s	u	n	q	l	a	y	g	f	e	a	j	s	c	w	o	h	g	h	h
Schlüssel:	k	o	m	a	n	d	o	k	o	m	a	n	d	o	k	o	m	a	n	d	o
Nachricht:	f	e	i	n	d	i	m	o	s	t	e	n	g	e	s	i	c	h	t	e	t

Sicherheit des Vigenère-Verfahrens

Wie kann ein Angreifer aus einer Chiffre den Klartext erhalten, ohne den Schlüssel zu kennen?

- Alle Schlüssel ausprobieren
- Häufigkeitsanalyse

Alle Schlüssel ausprobieren

- Der Schlüssel aus Nr. 3 hat 7 Stellen.
- Alle möglichen 7-stelligen Schlüsselwörter:
  $26 \cdot 26 \cdot 26 \cdot 26 \cdot 26 \cdot 26 \cdot 26 = 8.031.810.176$

- Dauert bei langen Schlüsseln zu lange.

Auftrag Nr. 4

- Nachricht: ‚hund‘
- Finde den richtigen Schlüssel, sodass die Chiffre ‚haus‘ ergibt.
- Finde den richtigen Schlüssel, sodass die Chiffre ‚baum‘ ergibt.

- 1. Schlüssel: ‚aghp‘, 2. Schlüssel: ‚ughj‘

Alle Schlüssel ausprobieren

- Führt nicht mehr unbedingt zum Ziel!
- Was passiert wenn die Nachricht länger wird?

Alle Schlüssel ausprobieren

- Führt nicht mehr unbedingt zum Ziel!
- Was passiert, wenn die Nachricht länger wird?
  - Unwahrscheinlich, dass es mehrere ‚sinnvolle' Entschlüsselungen gibt.
- Was passiert, wenn der Schlüssel länger wird?

Alle Schlüssel ausprobieren

- Führt nicht mehr unbedingt zum Ziel!
- Was passiert, wenn die Nachricht länger wird?
  - Unwahrscheinlich, dass es mehrere ‚sinnvolle' Entschlüsselungen gibt.
- Was passiert, wenn der Schlüssel länger wird?
  - Wahrscheinlicher, dass es mehrere ‚sinnvolle' Entschlüsselungen gibt.

Sicherheit des Vigenère-Verfahrens

Wie kann ein Angreifer aus einer Chiffre den Klartext erhalten, ohne den Schlüssel zu kennen?

- Alle Schlüssel ausprobieren
- Häufigkeitsanalyse

Häufigkeitsanalyse

- Warum hat die Häufigkeitsanalyse beim Cäsar-Verfahren funktioniert?

Häufigkeitsanalyse

- Warum hat die Häufigkeitsanalyse beim Cäsar-Verfahren funktioniert?
  - Jeder Buchstabe wurde um den gleichen Wert verschoben.

Auftrag Nr. 5

- Klartext: ‚ein Esel‘
- Finde einen Schlüssel, sodass der Klartext, mit dem Vigènere-Verfahren zur Chiffre: ‚xxx xxxx‘ verschlüsselt wird.

- Schlüssel: , tpkxtftm‘

Häufigkeitsanalyse

- Warum hat die Häufigkeitsanalyse beim Cäsar-Verfahren funktioniert?

  Jeder Buchstabe wurde um den gleichen Wert verschoben.

- Wann funktioniert die Häufigkeitsanalyse beim Vigenère-Verfahren?

Häufigkeitsanalyse

- Warum hat die Häufigkeitsanalyse beim Cäsar-Verfahren funktioniert?

  Jeder Buchstabe wurde im den gleichen Wert verschoben.

- Wann funktioniert die Häufigkeitsanalyse beim Vigenère-Verfahren?

  Wenn genügend Klartext-Buchstaben mit dem gleichen Schlüssel-Buchstaben verschlüsselt werden.

Häufigkeitsanalyse

Funktioniert nur, wenn wir die Länge des Schlüssels kennen!

Sonst wissen wir nicht, welcher Buchstabe mit dem wievielten Schlüsselbuchstaben verschlüsselt wurde.

Häufigkeitsanalyse

- Länge des Schlüssels: 7

Chiffre:	p	s	u	n	q	l	a	y	g	f	e	a	j	s	c	w	o	h	g	h	h
Schlüssel:	?	?	?	?	?	?	?	?	?	?	?	?	?	?	?	?	?	?	?	?	?

Häufigkeitsanalyse

- Länge des Schlüssels: 7

Chiffre:	p	s	u	n	q	l	a	y	g	f	e	a	j	s	c	w	o	h	g	h	h
Schlüssel:	?							?							?						

- ‚p‘,‘y‘ und ‚c‘ wurden mit dem gleichen Schlüssel verschlüsselt

Häufigkeitsanalyse

- Länge des Schlüssels: 7

Chiffre:	p	s	u	n	q	l	a	y	g	f	e	a	j	s	c	w	o	h	g	h	h
Schlüssel:		?							?							?					

- ‚s‘,‘g‘ und ‚w‘ wurden mit dem gleichen Schlüssel verschlüsselt

Häufigkeitsanalyse

- Warum hat die Häufigkeitsanalyse beim Cäsar-Verfahren funktioniert?

  Jeder Buchstabe wurde im den gleichen Wert verschoben.

- Wann funktioniert die Häufigkeitsanalyse beim Vigenère-Verfahren?

  Wenn genügend Klartext-Buchstaben mit dem gleichen Schlüssel-Buchstaben verschlüsselt werden.

Auftrag Nr. 6

- Chiffre: ‚zku wthhigq xpv qäfjvvh zqfjh pkwvzqfj cq jnhkfjht uwgonh. dukqih nqihht olv. vgl eguglv.‘
- Knacke die Verschlüsselung, der Schlüssel hat 2 Stellen.
- Schlüssel: ‚dc‘
- Klartext: ‚wir treffen uns nächste woche mittwoch an gleicher stelle. bringe koffer mit. sei bereit.'

Vergleich zu Cäsar

- Sehr viel größerer Schlüsselraum
- Brute-Force liefert nichtmehr eindeutig die Nachricht
- Nichtmehr sinnvoll von Hand zu knacken!
- Angreifbar durch Häufigkeitsanalyse, wenn Länge des Schlüssels bekannt

Auftrag Nr. 7

- Stelle deinem Partner eine Aufgabe zum Vigenère-Verfahren.
- Du kannst:
  - Nachricht & Schlüssel vorgeben und verschlüsseln lassen,
  - Chiffre & Schlüssel vorgeben und entschlüsseln lassen,
  - Nachricht & Chiffre vorgeben und den Schlüssel finden lassen.

Auftrag Nr. *

- Entschlüssele die Nachricht mit dem Vigenère-Verfahren.

- Witz: ‚jiu brn orcer hvf zdbd dwbgu lgu vuvq? lvbgscliowrrn‘
- Schlüssel: ‚nichtzuknacken‘