Projekt 1 - Klassische Kryptographie

Mit Hilfe eines Python Programmes sollen drei klassische kryptographische Verfahren umgesetzt werden.

- Die Skytale
- Der Caesar Chiffre
- Der Vigenère Chiffre

Alle Chiffre sollen mit Schlüssel entschlüsselbar sein, die beiden unteren auch ohne.

Die Skytale (https://de.wikipedia.org/wiki/Skytale (https://de.wikipedia.org/wiki/Skytale))

Umsetzung

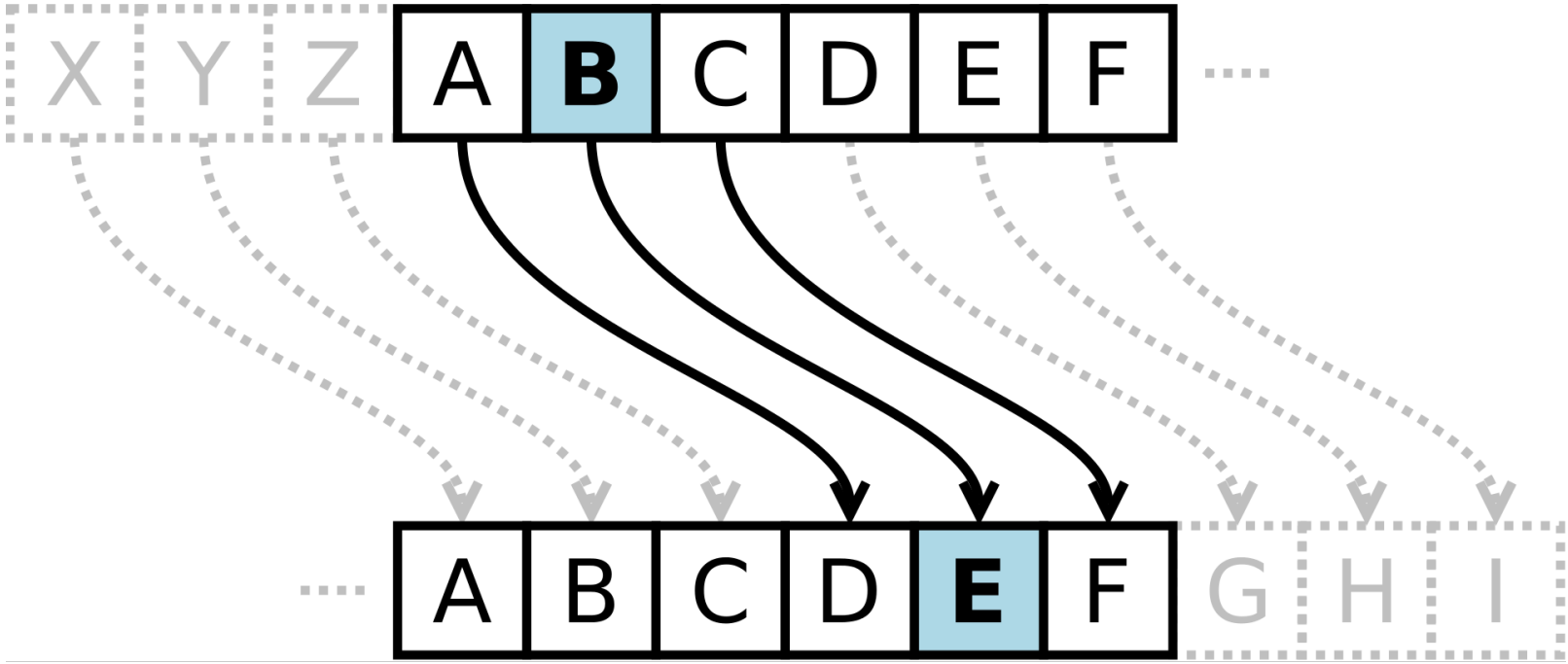
- Text "Mein erster verschlüsselter Text"
- Blocklänge = 5

0	1	2	3	4
M	e	i	n	
e	r	s	t	e
r		v	e	r
s	c	h	l	ü
s	s	e	l	t
e	r		T	e
x	t			

- Verschlüsselt "Merssexer csrtisvhe ntellT erüte"

Caesar Chiffre (https://de.wikipedia.org/wiki/Caesar-Verschl%C3%BCsselung (https://de.wikipedia.org/wiki/Caesar-Verschl%C3%BCsselung))

Bild: Von Cepheus - Eigenes Werk, Gemeinfrei, https://commons.wikimedia.org/w/index.php?curid=1235339 (https://commons.wikimedia.org/w/index.php?curid=1235339)

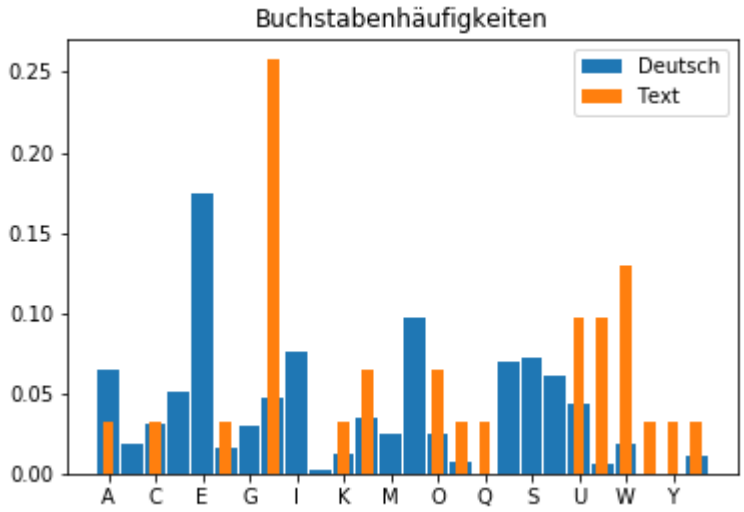


Umsetzung

- Text "Mein zweiter verschluesselter Text"
- Schlüsselbuchstabe = "D"
- Verschlüsselt: "Phlq czhlwhu yhuvfkoxhvvhowhu Whaw"
- Sicherer wenn Leer- und Satzzeichen, Groß- und Kleinschreibung entfernt

Kryptanalyse - Caesar

Buchstabenhäufigkeitsanalyse



Vigenère Chiffre (https://de.wikipedia.org/wiki/Polyalphabetische_Substitution#Vigen.C3.A8re-Verschl.C3.BCsselung (https://de.wikipedia.org/wiki/Polyalphabetische_Substitution#Vigen.C3.A8re-Verschl.C3.BCsselung))

Umsetzung

- Caesar Chiffre mit Schlüsselwort statt -buchstabe
- Text: "meindritterverschluesseltertext"
- Schlüsselwort: "hallo"

h	a	l	l	o	h	a	l	l	o	h	a	l	l	o	h	a	l	l	o	h	a	l	l	o	h
m	e	i	n	d	r	i	t	t	e	r	v	e	r	s	c	h	l	u	e	s	s	e	l	t	e	r	t	e	x	t
t	e	t	y	r	y	i	e	e	s	y	v	p	c	g	j	h	w	f	s	z	s	p	w	h	l	r	e	p	l	a

- Verschlüssel: "tetyryieesyvpcgjhwfszspwhlrepla"

Kryptanalyse - Vigenère

- Für Schlüssellänge *N* ist jeder *N*te Buchstabe gleich verschlüsselt.
- Die Nachricht lässt sich unterteilen in *N* Blöcke.
- Schlüssellänge errechnen
  - Berechne den **Koinzidenzindex** https://de.wikipedia.org/wiki/Koinzidenzindex (https://de.wikipedia.org/wiki/Koinzidenzindex) für jede Schlüssellänge