

- Die Entdeckung der Häufigkeitsanalyse machte monoalphabetische Verschlüsselungsverfahren unbrauchbar
 - Im Geheimtext spiegeln sich direkt die Buchstabenhäufigkeiten des Klartexts wider
- Bessere Verfahren wurden nötig

Vigenère-Verschlüsselung

- Erfunden im 16. Jahrhundert (nach Christus) von Blaise de Vigenère
- **Polyalphabetische** Verschlüsselung
 - Es gibt mehr als ein Geheimtextalphabet
- War rund 300 Jahre lang sicher (“le chiffre indéchiffrable”)
 - Spoiler: Heute nicht mehr ;-)

- Verwende einen Schlüssel aus mehreren Buchstaben
- Lege den Schlüssel zeichenweise über den Klartext
 - Wiederhole den Schlüssel, falls nötig
- Der jeweilige Schlüsselbuchstabe legt fest, wie der “darunter” liegende Klartextbuchstabe zu verschlüsseln ist
- Mit dem **Vigenère-Quadrat** lassen sich Texte schnell ver- und entschlüsseln

- Schlüssel: ADE
- Klartext: topsecret

Schlüssel:	A	D	E	A	D	E	A	D	E
Klartext:	t	o	p	s	e	c	r	e	t
Geheimtext:	T	R	T	S	H	G	R	H	X

Vigenère-Quadrat

A	B	C	D	E	F	G	H	...
B	C	D	E	F	G	H	I	...
C	D	E	F	G	H	I	J	...
D	E	F	G	H	I	J	K	...
E	F	G	H	I	J	K	L	...
F	G	H	I	J	K	L	M	...
G	H	I	J	K	L	M	N	...
H	I	J	K	L	M	N	O	...
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	

- Suche in Spalte 1 diejenige Zeile i, in der das aktuelle Zeichen des Schlüssels steht
- Suche in Zeile 1 diejenige Spalte j, in der das aktuelle Zeichen des Klartexts steht
- Das Zeichen des Geheimtexts ist dann das Element am Kreuzungspunkt von Zeile i und Spalte j

- Mit einfacher Häufigkeitsanalyse ist Vigenère nicht zu knacken
 - Wieso?
 - Ein bestimmter Buchstabe des Klartexts wird nicht mehr immer zum gleichen Buchstaben im Geheimtext
- Mitte des 19. (!) Jahrhunderts fanden Charles Babbage und Friedrich Kasiski (unabhängig voneinander) eine Möglichkeit zur Entzifferung

1. Suche im Geheimtext nach sich wiederholenden Buchstabenfolgen
 - Annahme: Diese Folgen entstanden durch das Verschlüsseln des selben Klartexts mit dem selben Teil des Schlüssels
 - Plausibel, denn:
 - Der Schlüssel wiederholt sich ständig
 - Es gibt sprachtypische Buchstabenfolgen, die häufig auftreten (bspw. "sch", "ck", "ei")
2. Bestimme die Abstände der sich wiederholenden Folgen
 - Sind die Folgen wie in Punkt 1. beschrieben entstanden, so muss deren Abstand ein Vielfaches der Schlüssellänge sein
 - Mögliche Schlüssellängen sind also alle gemeinsamen Teiler der gefundenen Abstände

3. Für jede in Frage kommenden Schlüssellänge n wird der Geheimtext in n Teiltex te zerlegt:
- Teiltex t 0: Buchstaben an Position $0, n, 2n, \dots$
 - Teiltex t 1: Buchstaben an Position $1, n + 1, 2n + 1, \dots$
 - Und so weiter...

Feststellung: Jeder der n Teiltex te ist monoalphabetisch verschlüsselt! (Die Buchstaben eines jeden Teils wurden jeweils durch das gleiche Zeichen des Schlüssels verschlüsselt)

4. Wende die Häufigkeitsanalyse auf jeden Teiltex t separat an

- Entziffere den Geheimtext in der Datei `vigenere_geheim.txt` mit Hilfe von JCrypytool
 - <https://www.cryptool.org/de/>