Mehr Sicherheit mit 2FA

- Wer hat 2FA (Second Factor Authentication) eingeschaltet?
  - Wo?
  - Wer wieder ausgeschaltet?

Mehr Sicherheit mit 2FA

- Wieso machen wir das schon wieder?
  - Genau: Passwörter sind unsicher!
  - Weshalb schon wieder? Was ist das Hauptproblem?

- Wiederverwendung von Passwörtern
  - Benötigt nur eine unsichere Website, um alle anderen Konten zu kompromittieren.
  - Angriff ist einfach zu skalieren.

Wie wird eine Website gehackt?

- Wenn Sie ein Konto anlegen, werden Ihre Zugangsdaten abgespeichert.
    - Datenbank / Datei

```
hof@ksr.ch:just4now
sca@ksr.ch:password
gra@ksr.ch:12345678
```

- Erhält jemand Zugriff auf die Datei, sind die Zugangsdaten weg.
- Gibt es eine sicherere Speicherart?

Verschlüsselung

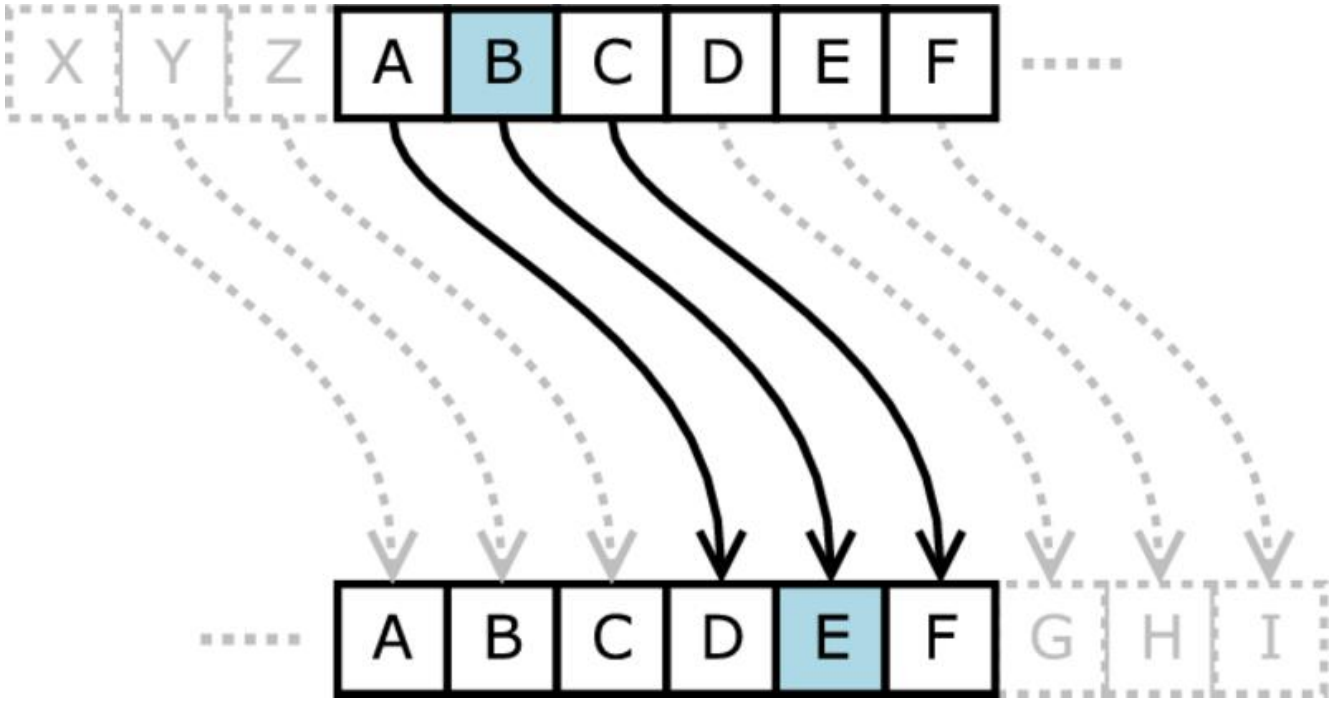
- Ziel: Text so abspeichern, dass niemand ihn lesen kann.
  - ausser wir, weil wir den Schlüssel kennen!

- Wer kann den folgenden Text entschlüsseln?

TVHVT JTU HVU

Caesar-Verschlüsselung

- Wir verschieben alle Buchstaben um eine fixe Anzahl:



Cäsar-Verschlüsselung

- Aufgabe 1: Schreiben Sie Cäsar-Verschlüsselung in Python.
  - im Wiki hat es Tipps...

Kryptologie-Begriffe

- Kryptologie: Die Lehre des Verborgenen
  - Kryptographie: Geheimschriften / Verschlüsselung
  - Kryptoanalyse: Verschlüsselungen analysieren / knacken

- Klartext – cleartext
- Chiffrat – ciphertext
- Schlüssel – key

Kryptologie-Begriffe

- Verschlüsselungsverfahren:
  - Wandelt den Klartext in das Chiffrat um, und umgekehrt.

- Schlüsselraum:
  - Anzahl verschiedene Schlüssel eines Verfahrens, als 2er Logarithmus in bit
    - 2 Schlüssel: 1 bit
    - 1024 Schlüssel: 10 bit
  - Wieviele Schlüssel gibt es bei der Cäsar-Verschlüsselung?

Monoalphabetische Substitution

- Jeder Buchstabe wird mit einem anderen vertauscht.
  - Komplexer als Cäsar
  - Wie gross ist der Schlüsselraum?

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

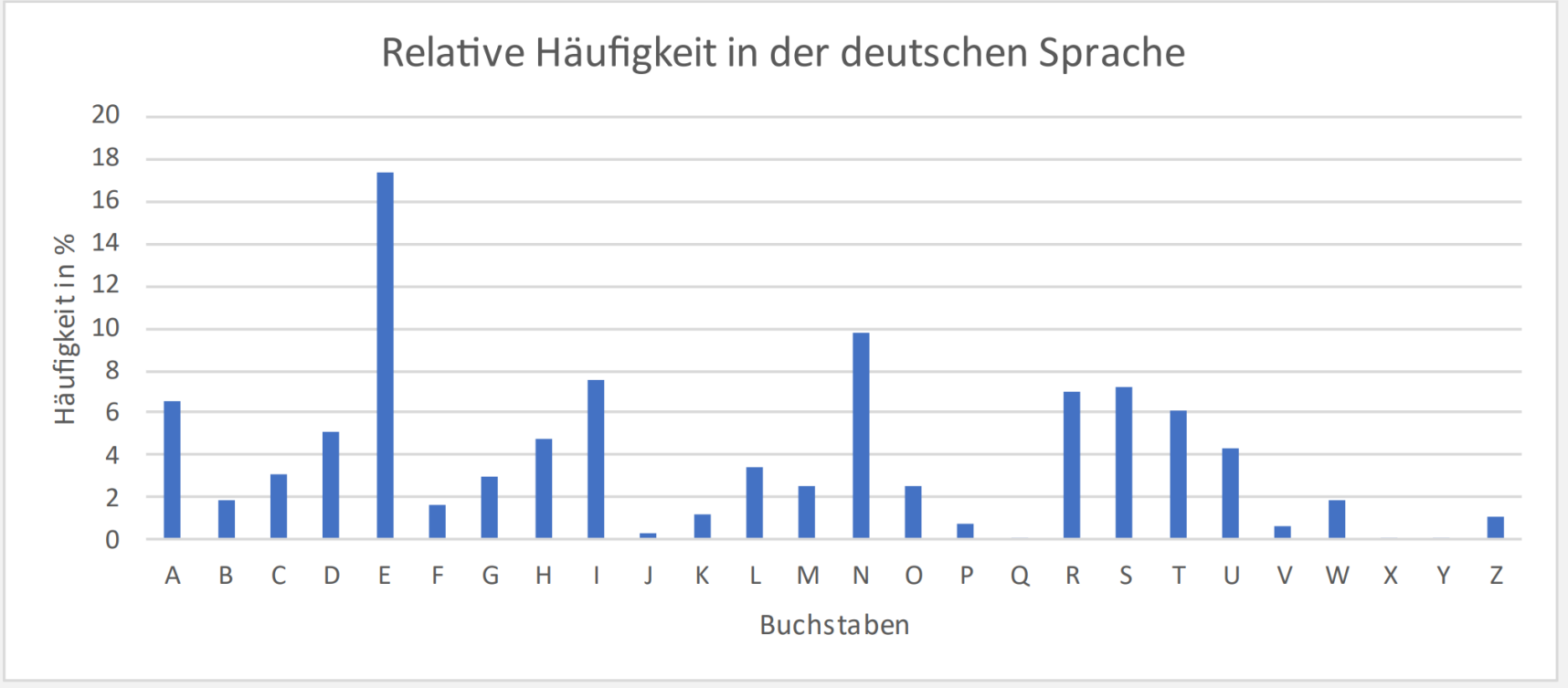
Monoalphabetische Substitution

- Schlüsselraum:
  - $26 \cdot 25 \cdot \cdots \cdot 3 \cdot 2 = 26! \cong 4 \cdot 10^{26} \cong 2^{88} = 88\ bit$
  - fast unmöglich zu knacken mit *Brute Force* (alles durchprobieren)

- Gibt es trotzdem eine Möglichkeit?

Häufigkeitsanalyse

- Nicht alle Buchstaben kommen gleich häufig vor
  - Deutsch: E, S, R, A sind häufiger als Y, Q, X, J



Häufigkeitsanalyse

- Wie können wir das ausnützen, um eine Verschlüsselung zu brechen?
  - https://studio.code.org/s/frequency_analysis/lessons/1/levels/1