

# Cybersecurity Workshop

*Paul Hoerenz*

**Kryptologie**

Caesar, Viginere

**Web**

Einfache Exploits

**OSINT**

Informationsbeschaffung

# Caesar Cipher

---

A	0
B	1
C	2
D	3
...	...

Schlüssel: **B** ( $A \rightarrow B$ )

Plaintext: **H A L L O**

Ciphertext:

# Caesar Cipher

---

A	0
B	1
C	2
D	3
...	...

Schlüssel: **B** ( $A \rightarrow B$ )

Plaintext: **HALLO**

Ciphertext: **I B M M P**

# **Caesar Cipher**

---

## **Aufgabe 1**

Entschlüssle folgenden Text:

**Jwxyj Mjfzxktwijwzsl ljhmfkky**

# Automatisierte Angriffe

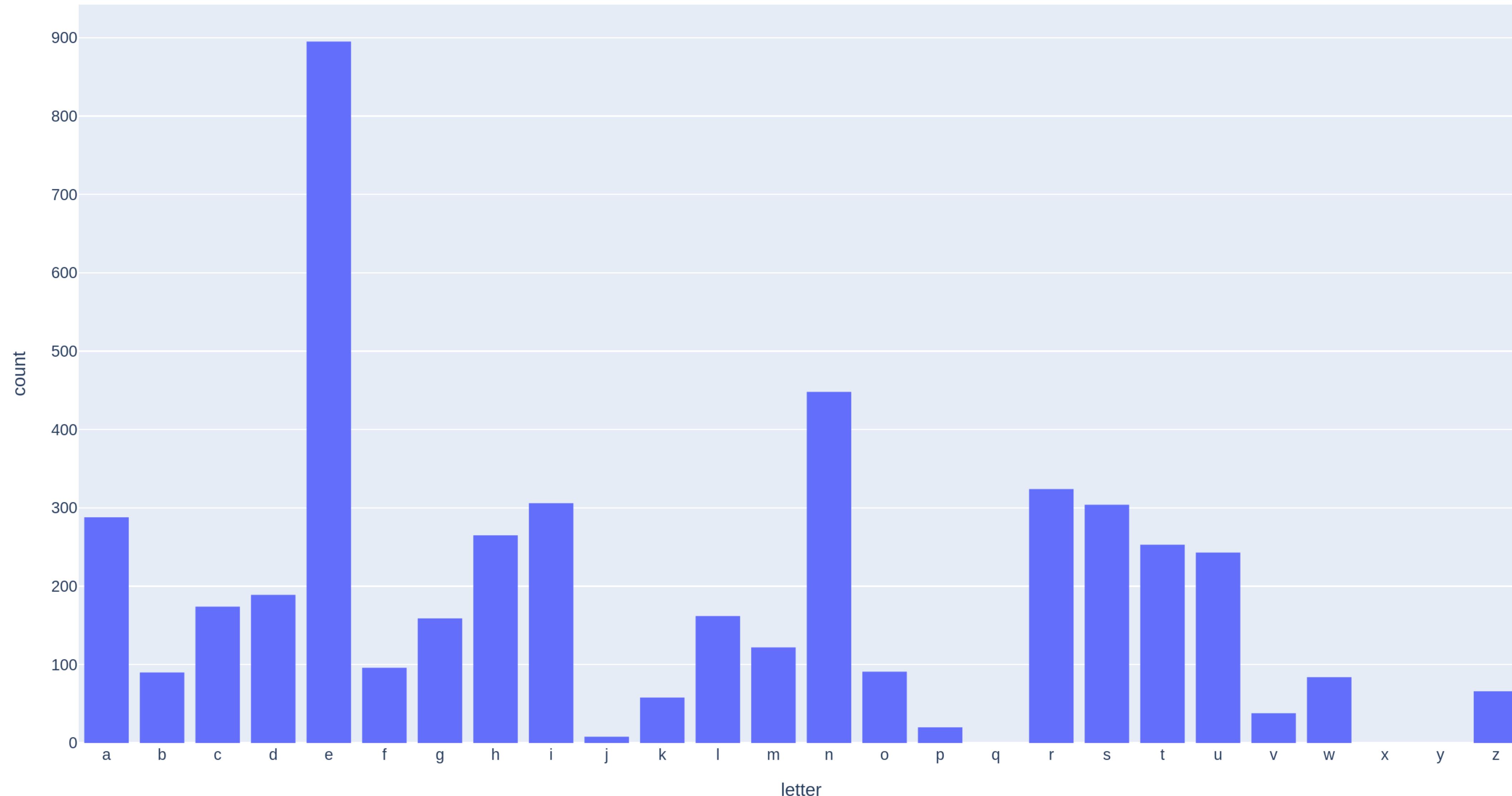
---

Als Gregor Samsa eines Morgens aus unruhigen Träumen erwachte, fand er sich in seinem Bett zu einem ungeheueren Ungeziefer verwandelt. Er lag auf seinem panzerartig harten Rücken und sah, wenn er den Kopf ein wenig hob, seinen gewölbten, braunen, von bogenförmigen Versteifungen geteilten Bauch, auf dessen Höhe sich die Bettdecke, zum gänzlichen Niedergleiten bereit, kaum noch erhalten konnte. Seine vielen, im Vergleich zu seinem sonstigen Umfang kläglich dünnen Beine flimmerten ihm hilflos vor den Augen.

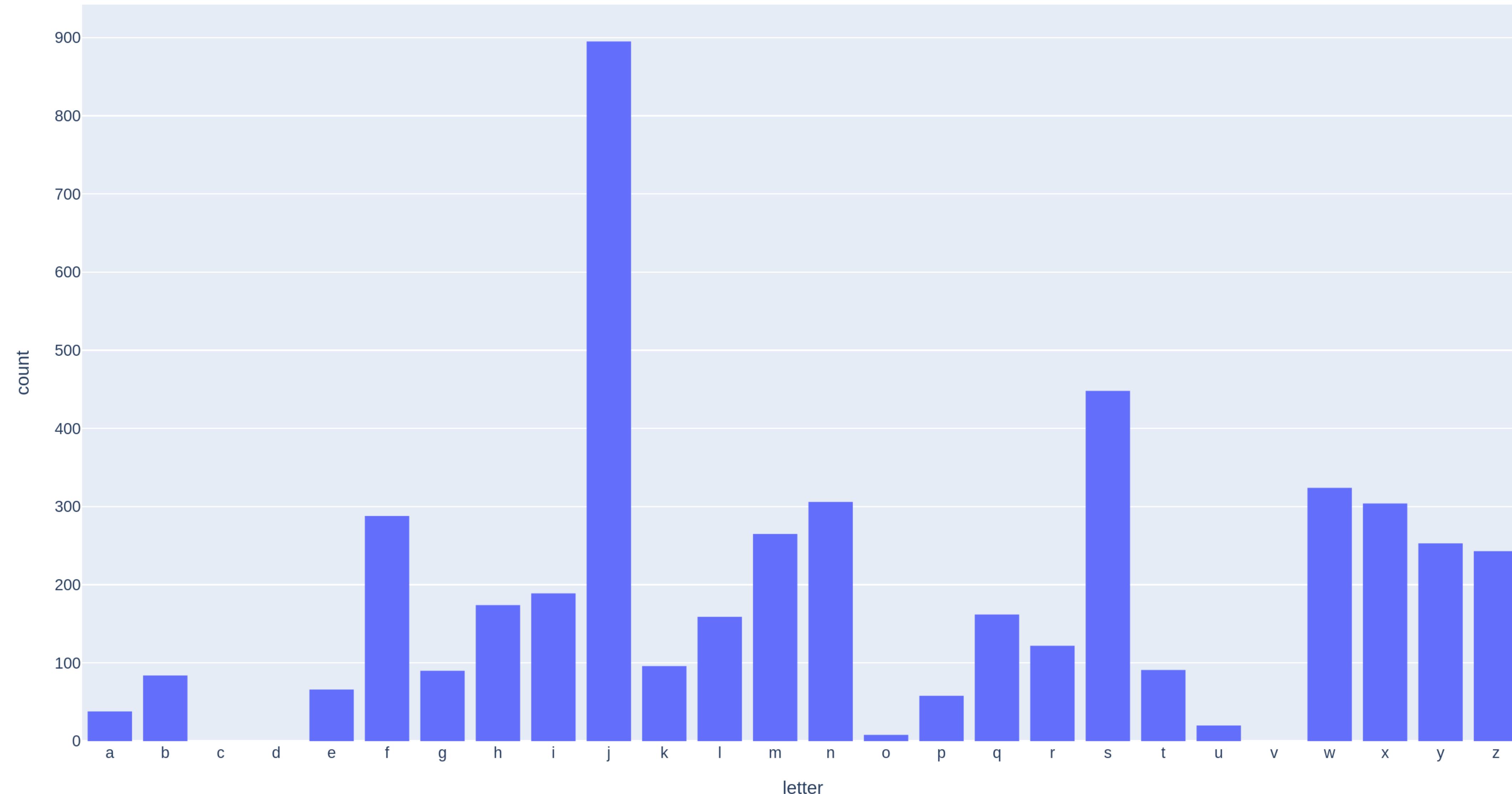
»Was ist mit mir geschehen?«, dachte er. Es war kein Traum. Sein Zimmer, ein richtiges, nur etwas zu kleines Menschenzimmer, lag ruhig zwischen den vier wohlbekannten Wänden. Über dem Tisch, auf dem eine auseinandergepackte Musterkollektion von Tuchwaren ausgebreitet war – Samsa war Reisender – hing das Bild, das er vor kurzem aus einer illustrierten Zeitschrift ausgeschnitten und in einem hübschen, vergoldeten Rahmen untergebracht hatte. Es stellte eine Dame dar, die mit einem Pelzhut und einer Pelzboa versehen, aufrecht dasaß und einen schweren Pelzmuff, in dem ihr ganzer Unterarm verschwunden war, dem Beschauer entgegenhob. [...]

# Plaintext

---



# Ciphertext



# Viginere Cipher

---

Schlüssel: **T T O**

Plaintext: **S T R E N G   G E H E I M E   N A C H R I C H T**

Keystream:

Ciphertext:

# Viginere Cipher

---

Schlüssel: **T T O**

Plaintext: **S T R E N G   G E H E I M E   N A C H R I C H T**

Keystream: **T T O**

Ciphertext:

# Viginere Cipher

---

Schlüssel: **T T O**

Plaintext: **S T R E N G   G E H E I M E   N A C H R I C H T**

Keystream: **T T O T T O**

Ciphertext:

# Viginere Cipher

---

Schlüssel:      **T T O**

Plaintext:      **S T R E N G    G E H E I M E    N A C H R I C H T**

Keystream:      **T T O T T O    T T O T T O T    T O T T O T T O T**

Ciphertext:

# Viginere Cipher

---

Schlüssel: **TTO**

Plaintext: **STRENG GEHEIME NACHRICHT**

Keystream: **TTOTTO TTOTTOT TOTTOTTOT**

Ciphertext: **LMFXGU ZXVXBAX GOVAFBVVM**

## Viginere Cipher

---

Wir kennen die **Länge des Schlüssels**  
nicht, aber wir können sie herausfinden!

# Viginere Cipher

---

## Aufgabe 2

Starte „Key to My Heart“ und  
ermittle die Schlüssellänge.

# Viginere Cipher

---

Mithilfe der Länge können wir den Schlüssel  
wie beim **Caesar Cipher** ermitteln!

# Viginere Cipher

---

Schlüssel:      **T T O**

Plaintext:      **S T R E N G    G E H E I M E    N A C H R I C H T**

Keystream:      **T T O T T O    T T O T T O T    T O T T O T T O T**

Ciphertext:      **L M F X G U    Z X V X B A X    G O V A F B V V M**

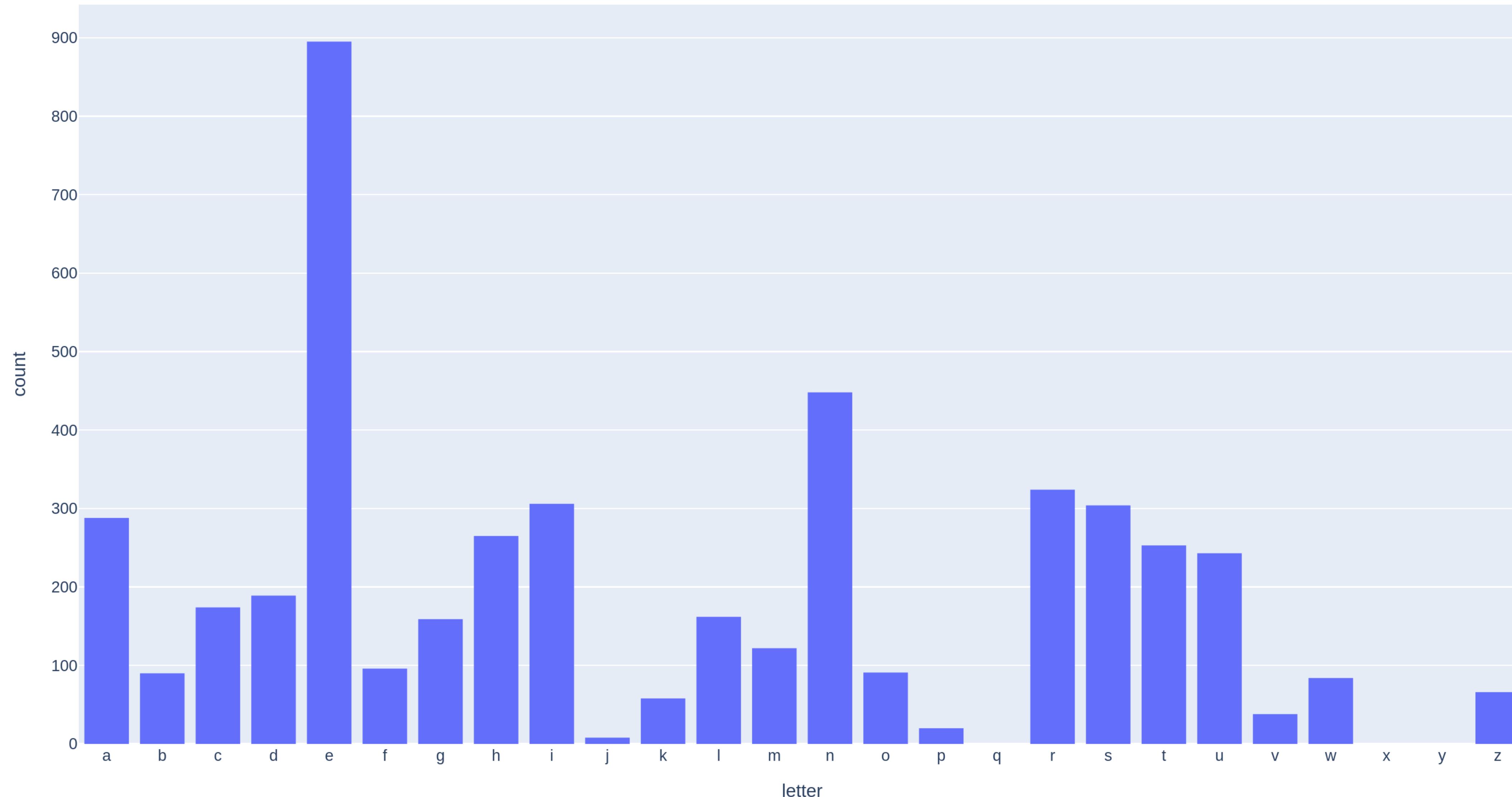
# Viginere Cipher

---

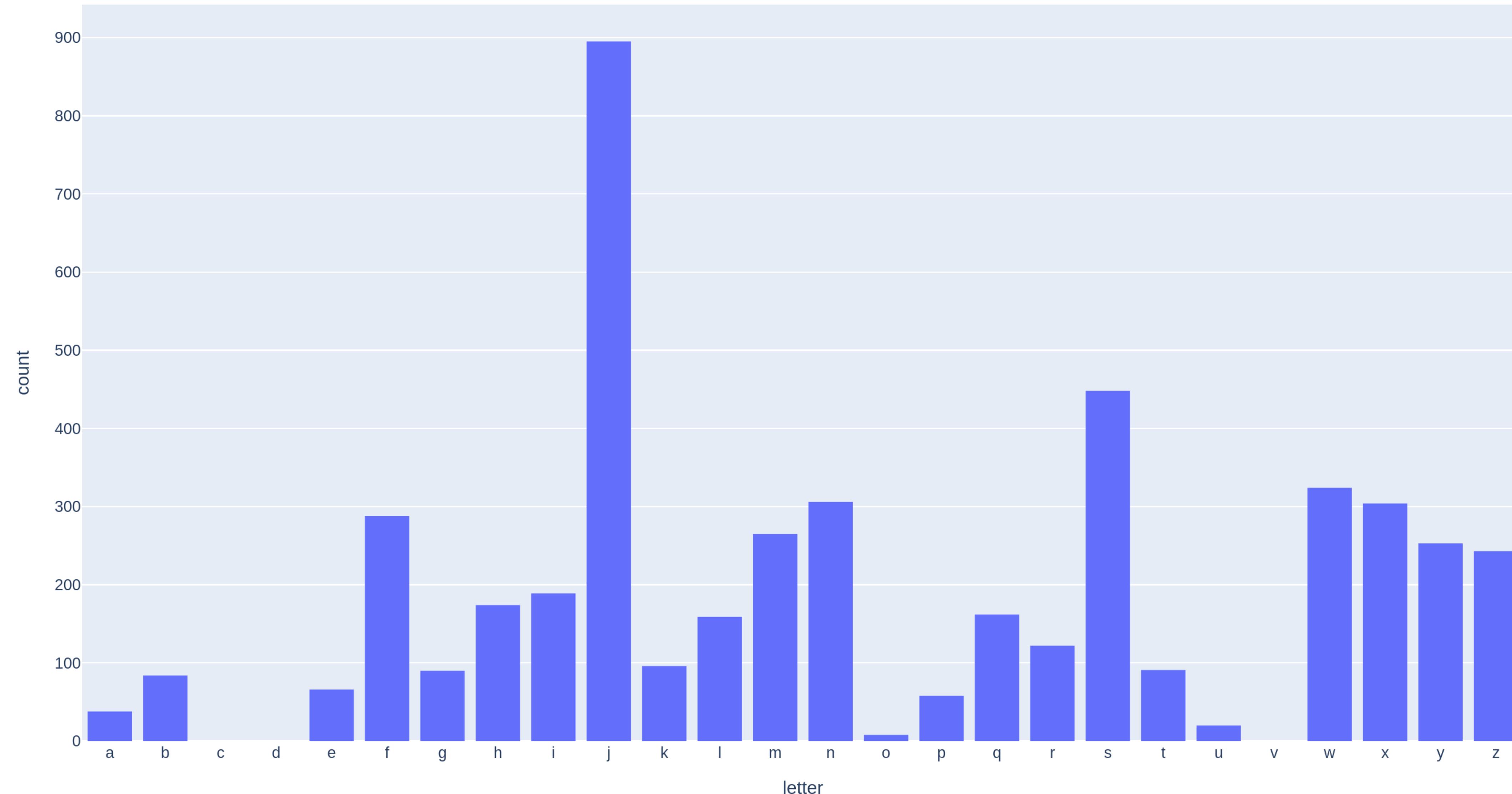
Häufigster Buchstabe:  
**E (4)**

# Plaintext

---



# Ciphertext



# Viginere Cipher

---

Formel:  $x - 4 \bmod 26$

„Histogram verschieben“

# **Viginere Cipher**

---

## **Aufgabe 2**

Starte „Key to My Heart“ und entschlüssle die geheime Nachricht.

*(In Großbuchstaben in zeroday eintragen!)*

# One-Time-Pad



# Schlüssel:

1. (echt) zufällig
  2. nur einmal verwenden
  3. gleich lang wie Nachricht

Mit einer **einfachen Änderung** wird aus  
einem unsicheren Verfahren ein  
**unbrechbarer Cipher!**

*(In der Praxis aber kaum einsetzbar)*

# Cybersecurity Workshop

*Paul Hoerenz*

Kryptologie

Caesar, Viginere

Web

Einfache Exploits

OSINT

Informationsbeschaffung

# **IT-Sicherheitswettbewerbe (für Teams)**

---

## **Capture The Flag**

Flags finden und Punkte sammeln,  
Lösen praxisnaher Aufgaben

CTF-Aufgaben sind **herausfordernd**.

Es ist **normal**, dass:

- du nicht sofort die Lösung siehst
- du dich festfährst
- du mehrfach neu ansetzen musst

### Was hilft?

- Denk in kleinen Schritten
- Lies Aufgabenstellungen genau
- Im Team kommunizieren
- Nicht entmutigen lassen!

## **Aufgabe 3**

Starte „payvault“ und  
finde die Flag.

## **Aufgabe 4**

Starte „Ticket to Hackville“  
und finde die Flag.

# Cybersecurity Workshop

*Paul Hoerenz*

Kryptologie

Caesar, Viginere

Web

Einfache Exploits

OSINT

Informationsbeschaffung

## Informationsbeschaffung

- Nutzung frei zugänglicher Datenquellen
- versteckte Informationen finden
- Kombination aus Technik, Recherche und Kreativität



## **Aufgabe 5**

Finde Folgendes:

1. Stadtnamen
2. Höhe des höchsten Gebäudes auf dem Foto

Translated from Arabic by Google

In the morning, the cities display their beauty and present themselves to the newcomers.. The beautiful city of Kiffa has shown its virtues this morning!!



1:45 PM · Feb 20, 2013

## **Aufgabe 6**

Finde die Koordinaten des Ortes, an dem das Foto aufgenommen wurde.