Systemsicherheit

Übungsblatt 3

Vorgehen bei Kyptoanalyse

- Histogramm der Zeichen

  $\Rightarrow$ Substitution oder nicht

  $\Rightarrow$ Ungefähre Anzahl der Alphabete

- Polyalphabetisch: Hist. von Perioden

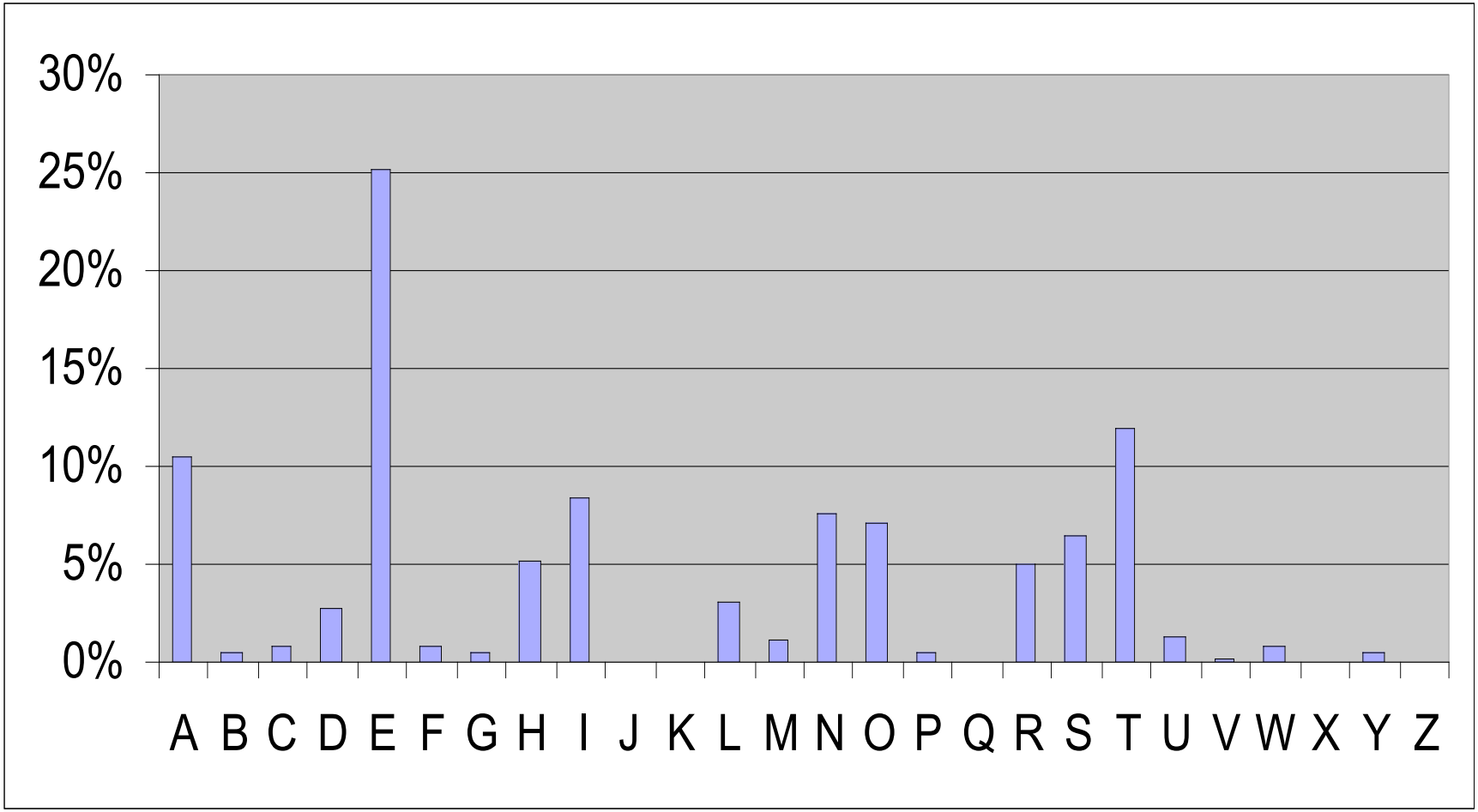
  $\Rightarrow$ Normalverteilung bei tatsächlicher Periode

- bei ~ Gleichverteilung: Kasiski-Test

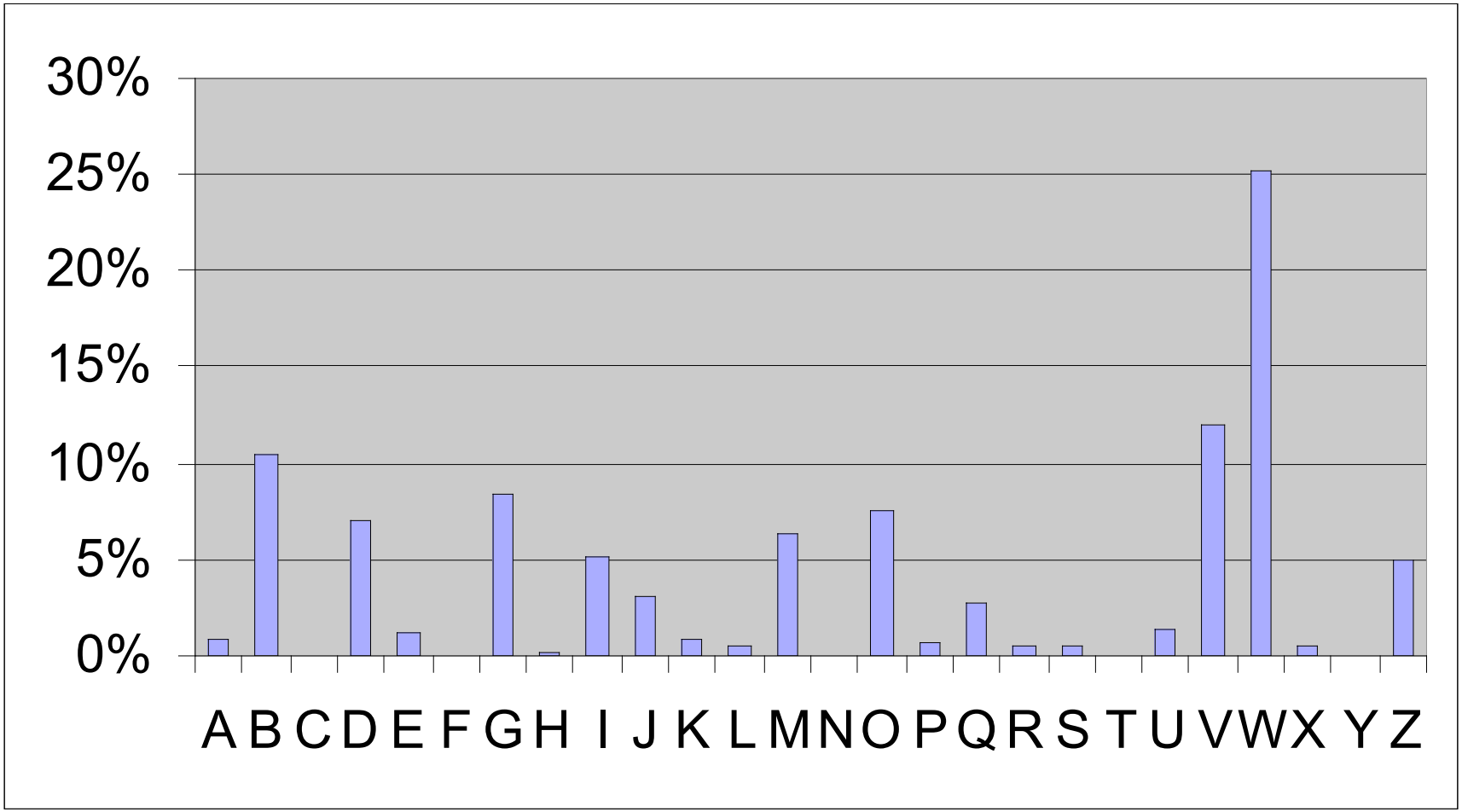
  $\Rightarrow$ Schlüssellänge

  $\Rightarrow$ Normalverteilung bei Schlüssel-Periode

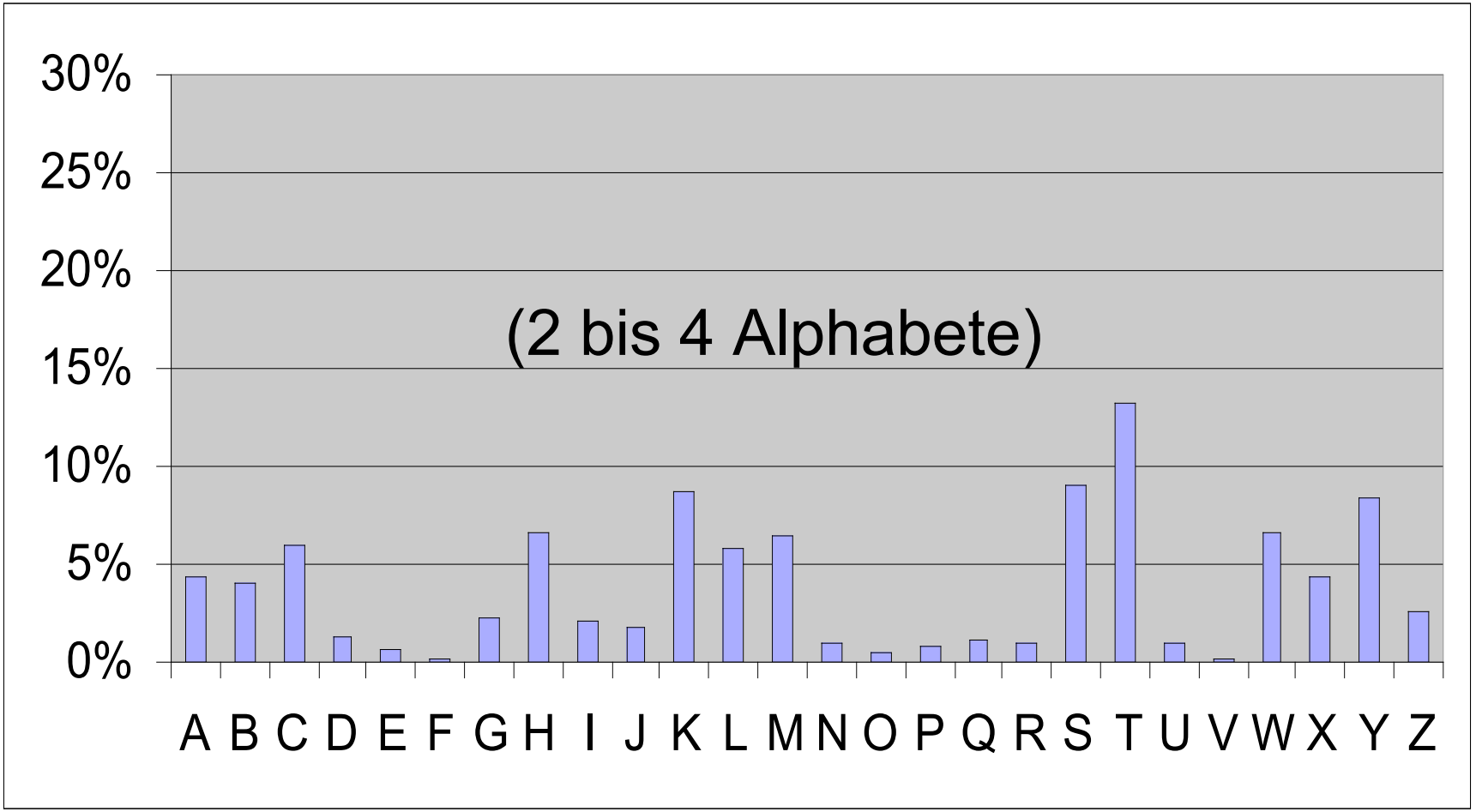
Zeichenhäufigkeit im Klartext



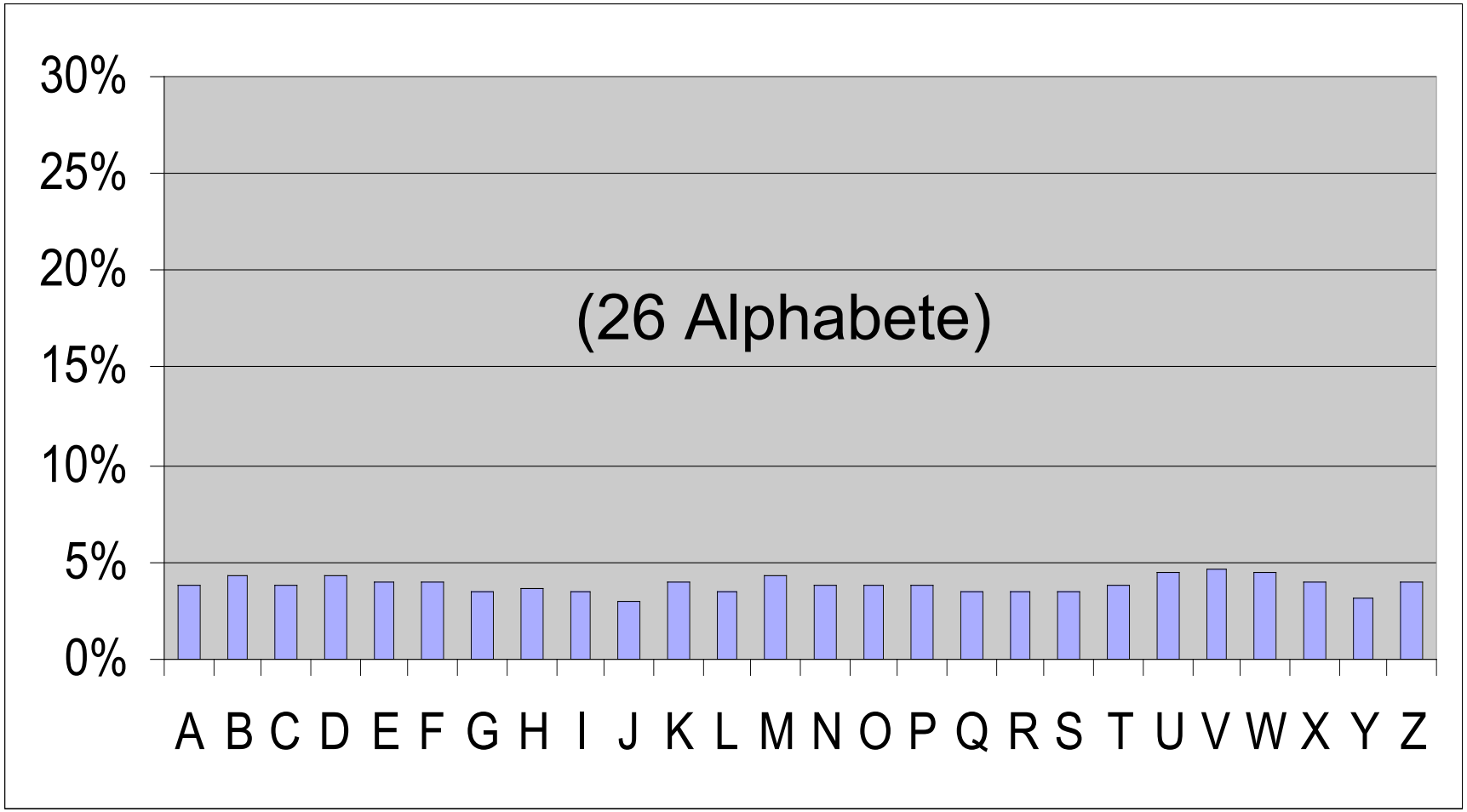
Monoalphabetisch



Polyalphabetisch



Maximal Polyalphabetisch



Verwendung der Werkzeuge

- Vertausche ABCD → BADC in file.txt

```
extract 2 0 < file.txt > f0.txt
extract 2 1 < file.txt > f1.txt
combine f1.txt f0.txt
```

- Histogramm der Trigramme

```
ngram 3 < file.txt
```

- Histogramm der Zeichen an Periode 5

```
extract 5 0 < file.txt | ngram 1
```