Kasiski und Friedmann gegen Vigenere

Kasiski-Test / Friedmann-Test

- (Entschlüsselung der Vigenere-Verschlüsselung durch Charles Babbage 1854)
- **Grundidee:** Ist die Länge des Schlüsselwortes *n* bekannt, kann man die Vigenere-Verschlüsselung auf *n* monoalphabetische Verschlüsselungen zurückführen und *n* Häufigkeitsanalysen durchführen und so auf das Schlüsselwort kommen

Warum?

- der *erste* Geheimtextbuchstabe, der *n+1*., der *2n+1*., der *3n+1*. .... stehen unter demselben Schlüsselbuchstaben und werden somit mit derselben Caesar-Verschiebung codiert. Dasselbe gilt für den *2*., den *n+2*., den *2n+2*. Geheimtextbuchstaben usw.
- Die Frage reduziert sich somit auf das Finden der Schlüsselwortlänge.

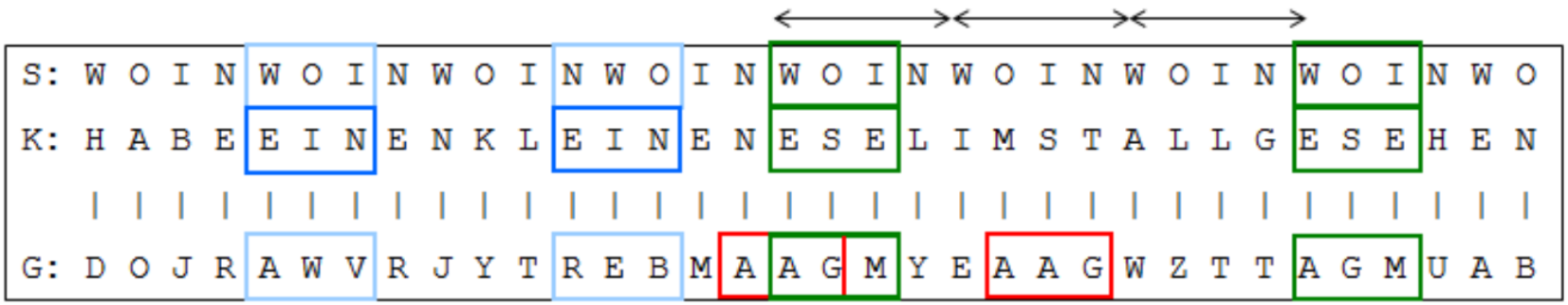
Vigenere „knacken“

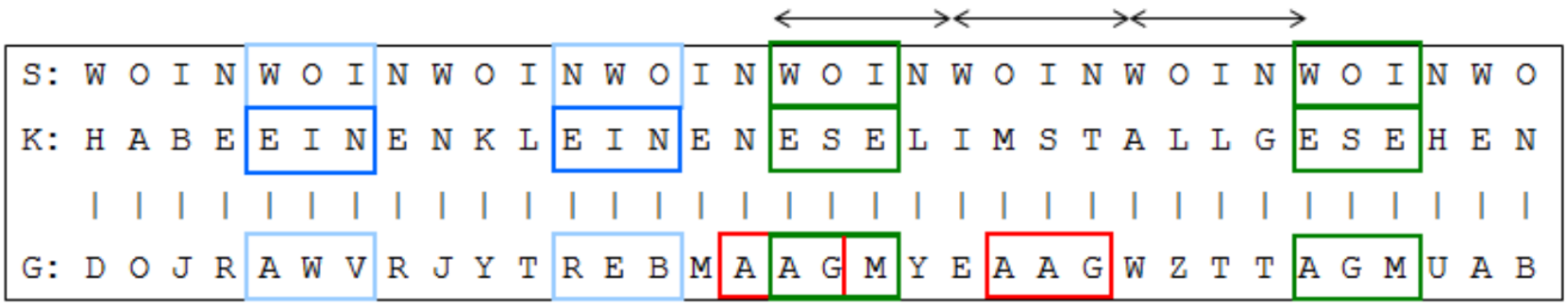
- Die *n* Caesar-Verschiebungen sind deshalb so leicht zu „knacken“, weil jeweils nur noch das Klartext-e per Häufigkeitsanalyse identifiziert werden muss

Kasiski-Test

- **Grundidee:** gleiche Geheimbuchstabenfolgen (mind. 3 Buchstaben) sind höchstwahrscheinlich gleiche Klartextfolgen, die an gleicher Stelle unter dem Schlüsselwort stehen.
- Zeichenabstand zwischen diesen Wiederholungen ist ein Vielfaches der Schlüssellänge

- Beispiel


S: W O I N W O I N W O I N W O I N W O I N W O I N W O I N W O I N W O I N W O
K: H A B E E I N E N K L E I N E N E S E L I M S T A L L G E S E H E N
G: D O J R A W V R J Y T R E B M A A G M Y E A A G W Z T T A G M U A B




```
Schlüssel:   . . . .
Klartext:    H A B E
             E I N E
             N K L E
             I N E N
             E S E L
             I M S T
             A L L G
             E S E H
             E N
Geheimtext:  D O J R
             A W V R
             J Y T R
             E B M A
             A G M Y
             E A A G
             W Z T T
             A G M U
             A B
```

Übung

FIQFIQIOUOELOTHFIQVN
HJNLHELOLDODMVCKIELE
AVFIQIOUOWXSDHHEIFIH
STIVEUEIHTEHJNLHUQHU
QEFLODHUSLDHKFUWFLHJ
DHSNLDHWNEKSLHCEQEIJ
TOQEEUOAOTWDQPHOTLFR
LODLFSHSELOMDMIJFNIM
AJHE

- Die nebenstehende Zeichenfolge enthält einen nach dem Vigenère-Verfahren codierten Text
- Beschreiben Sie, wie mithilfe des Kasiski-Tests solche Texte „geknackt“ werden können.
- Ermitteln Sie die Länge des Codewortes mithilfe des Kasiski-Tests.
- Bestimmen Sie das Codewort und entschlüsseln Sie die erste Zeile.