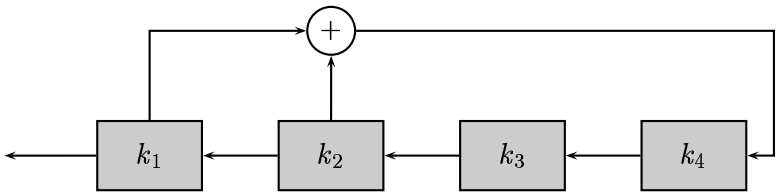
Übungen zur Kryptologie 1 Sommersemester 2002
Johannes Köbler/Olaf Beyersdorff

Übungsblatt 4

Aufgabe 15 (schriftlich, 10 Punkte)

Ein lineares Schieberegister (LSR) der Länge m ist eine Anordnung von m Speicherzellen $k_1, \ldots, k_m$, wobei jede Zelle k_i ein Bit Information speichern kann.



Seien $c_0, \ldots, c_{m-1} \in \{0,1\}$ Konstanten, wobei $c_0 = 1$. Ein Rechenschritt eines LSR besteht darin, zunächst das Bit $\ell = \bigoplus_{j=0}^{m-1} c_j \cdot k_{j+1}$ zu berechnen. Dann wird k_1 ausgegeben und der Inhalt der Speicherzellen um eine Position nach links verschoben, wobei k_m den Wert ℓ erhält. Auf diese Art entsteht eine Bitfolge z_i mit $z_i = k_i$, $1 \leq i \leq m$, und

$$z_{i+m} = \sum_{j=0}^{m-1} c_j z_{i+j} \bmod 2, \ i \geq 1.$$

Offensichtlich ist diese Folge nicht zufällig, sondern besteht aus einem sich ständig wiederholenden Muster, dessen Länge als Periode des LSR bezeichnet wird.

a) Konstruieren Sie ein LSR der Länge $m = 5$ mit Periode 31.

b) Zeigen Sie, daß die Periode höchstens $2^m - 1$ ist.

c) Überlegen Sie sich, wie die auf einem LSR basierende Stromchiffre bei Kenntnis von $2m$ aufeinanderfolgenden Klartext/Kryptotext-Bitpaaren gebrochen werden kann, falls $k = (k_1, \ldots, k_m, c_0, \ldots, c_{m-1})$ als Schlüssel benutzt wird.

Aufgabe 16

Entschlüsseln Sie durch eine Häufigkeitsanalyse (von Bigrammen) folgende Kryptotexte.

a) `hssit oient thehs aotre tsehf rteet`
(*Hinweis:* Der Klartext wurde durch eine Blocktransposition, mit der Blocklänge 5 verschlüsselt.)

b) `sihos tseet eetts eftin hrheh otatr`
(*Hinweis:* Der Klartext wurde durch eine Matrixtransposition mit einer 6×5 Matrix verschlüsselt.)

Aufgabe 17

a) Durch eine Häufigkeitsanalyse wurde festgestellt, dass eine affine Chiffre `E` auf `l` und `T` auf `g` abbildet. Bestimmen Sie den Schlüssel.

b) Wie Teilaufgabe a, nur wurde `J` auf `t` und `N` auf `v` abgebildet.

Tabelle 1: Einteilung von Buchstaben in Cliquen mit vergleichbaren Häufigkeitswerten.

	Deutsch	Englisch	Französisch
sehr häufig	E	E	E
häufig	N | I R S | A T	T | A O I N | S R H	N | A R S I T U
durchschnittlich	D H U | L G O | C M	L D | C U M F	L D | C M P
selten	B F W K Z | P V	P G W Y B | V K	V | F B G Q H X
sehr selten	J Y X Q	X J Q Z	J Y Z K W

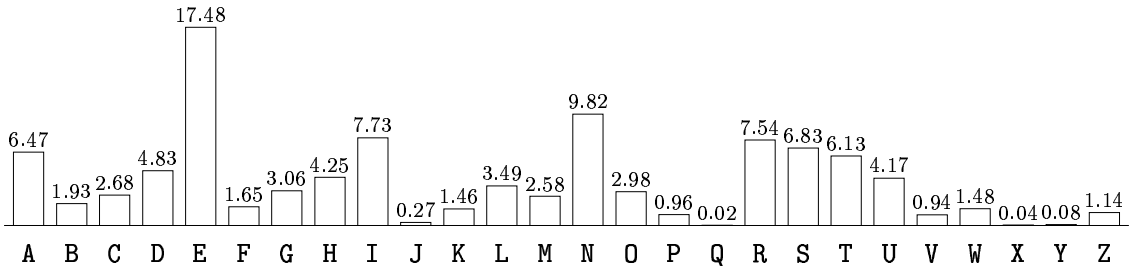


Abbildung 1: Häufigkeitsverteilung von Einzelbuchstaben im Deutschen (in %).

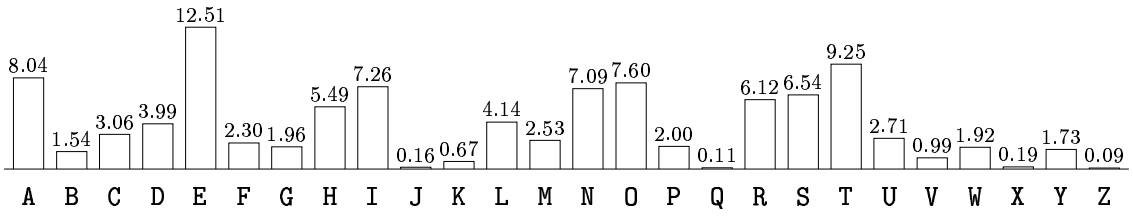


Abbildung 2: Häufigkeitsverteilung von Einzelbuchstaben im Englischen (in %).

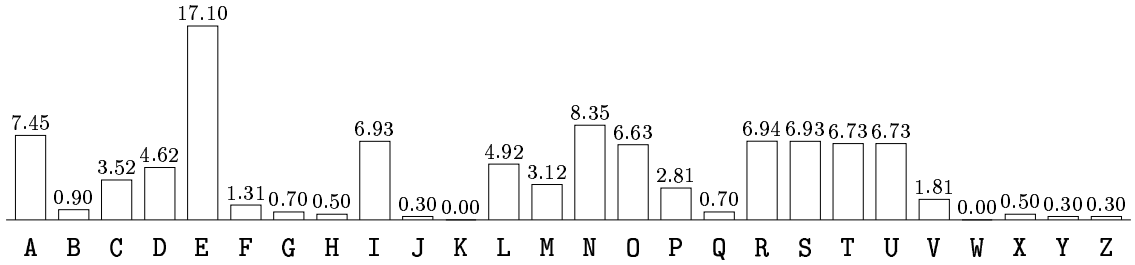


Abbildung 3: Häufigkeitsverteilung von Einzelbuchstaben im Französischen (in %).

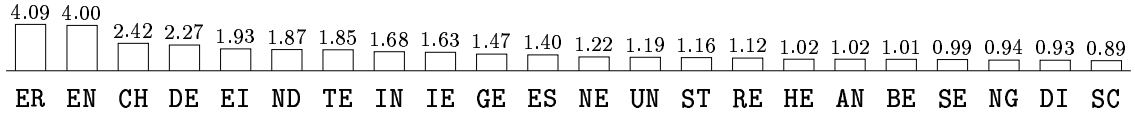


Abbildung 4: Die häufigsten Bigramme im Deutschen (Angaben in %).

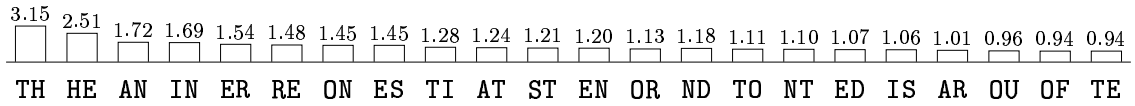


Abbildung 5: Die häufigsten Bigramme im Englischen (in %).

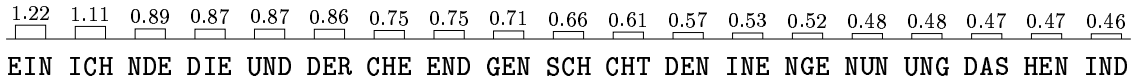


Abbildung 6: Die häufigsten Trigramme im Deutschen (in %).

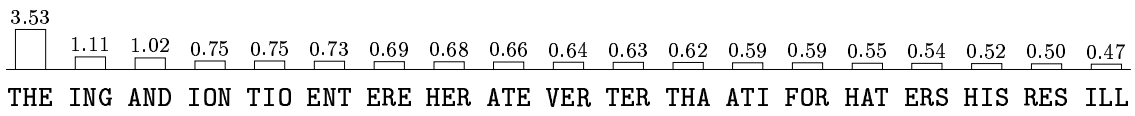


Abbildung 7: Die häufigsten Trigramme im Englischen (in %).