Security

- LV 4120 und 7240 -

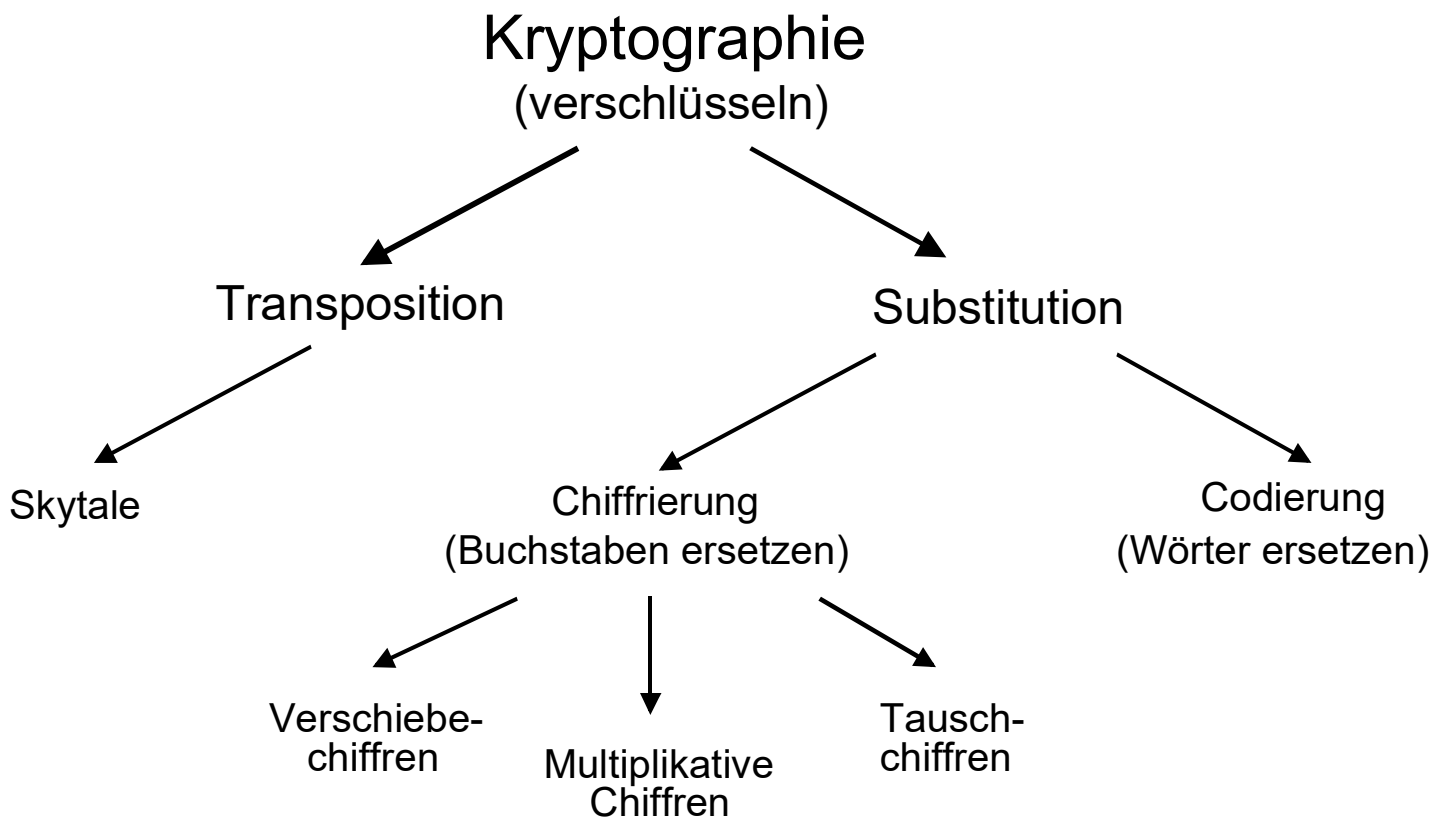
Monoalphabetische Chiffren und deren Analyse

- Terminologie und Grundsätze der Kryptographie
- Transpositions- und Substitutionsschiffren
- Verschiebechiffre (Caesar-Verschlüsselung)
- Multiplikative Chiffre
- Tauschchiffre (Affine Chiffre)
- Häufigkeitsanalyse
- Realisierung

Kap. 3: Monoalphabetische Chiffren und deren Analyse

Teil 1: Einteilung der kryptographischen Chiffrierverfahren

- Transpositionschiffren
- Substitutionschiffren


Kryptographie
(verschlüsseln)
Transposition
Substitution
Skytale
Chiffrierung
(Buchstaben ersetzen)
Codierung
(Wörter ersetzen)
Verschiebe-
chiffren
Multiplikative
Chiffren
Tausch-
chiffren

- Bei einer **Transpositionschiffre** wird der Geheimtext durch eine Permutation der Klartextzeichen erzeugt.

  ⇒ Die Zeichen bleiben gleich, tauschen aber ihre Plätze.

- Bei einer **Substitutionschiffre** wird jedes Zeichen des Klartextes durch ein anderes ersetzt.

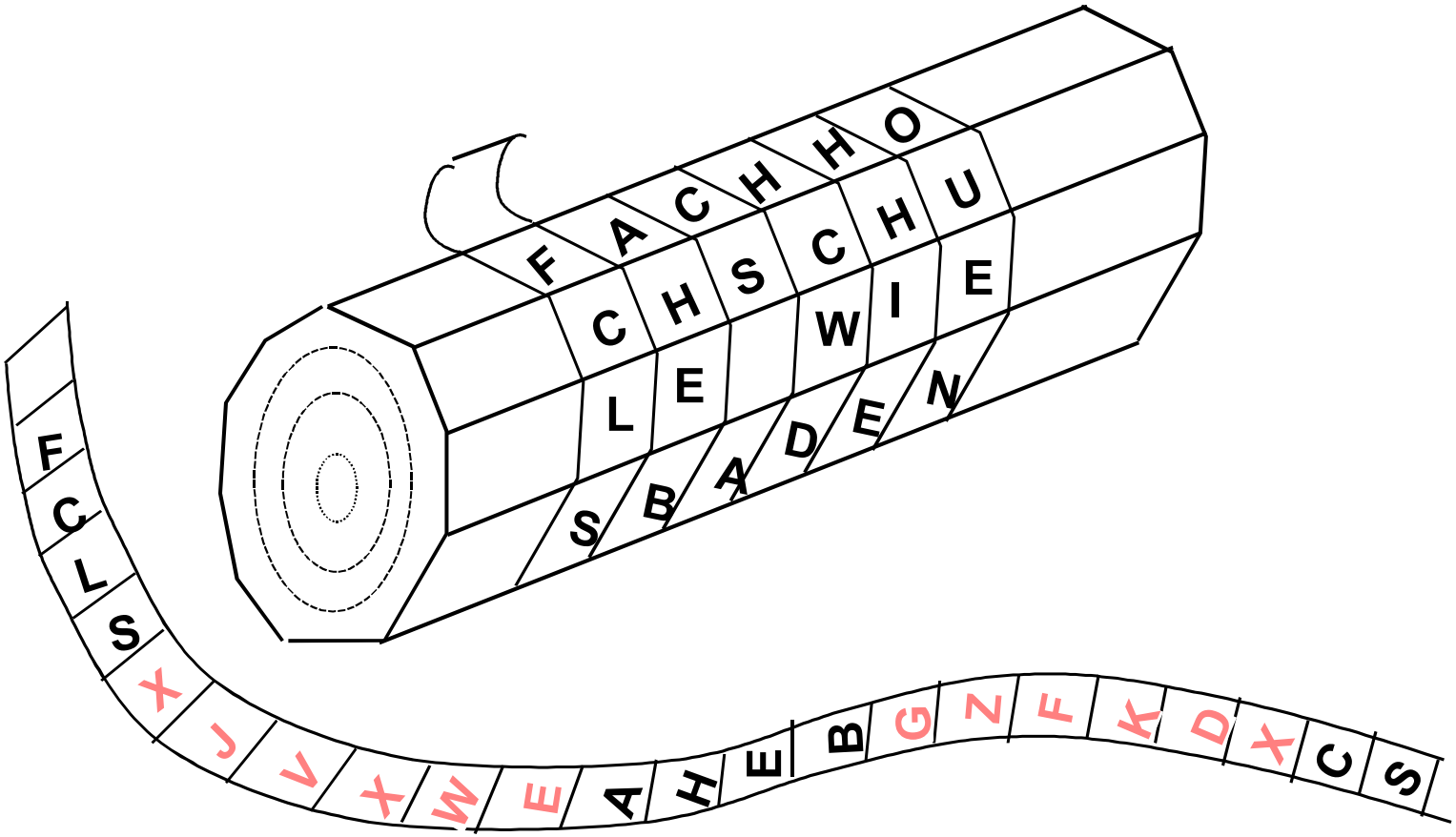
  ⇒ Die Position bleibt jedoch erhalten.

  - Substitutionschiffren sind demnach invertierbare Abbildungen eines endlichen Alphabets A auf ein (evtl. anderes) endliches Alphabet.
  - Eine Substitutionschiffre heißt **monoalphabetisch**, wenn jedes Klartextzeichen immer auf das gleiche Geheimtextzeichen abgebildet wird.
  - Ansonsten heißt die Substitutionschiffre **polyalphabetisch**.

Kap. 3: Monoalphabetische Chiffren und deren Analyse

Teil 2: Einfache Chiffriermaschinen

- Skytale
- Alberti-Scheibe


F A C H H O
C H S C H U
L E W I E
S B A D E N
F C L S X J V X W E A H E B G Z F K D X C S

Arithmetik

- Für die rechnergestützte Realisierung einer Substitutionschiffre benötigen wir Rechenregeln für das Addieren und Multiplizieren von Zahlen in {0, 1, 2, ..., n-1}, deren Resultat ebenfalls in {0, 1, 2, ..., n-1} liegt.
- Ferner müssen für das erzielte Resultat die zuvor aufgestellten Rechenregeln weiterhin gelten.
- Wir erreichen dies, indem wir Resultate größer als n-1 durch n dividieren und den Divisionsrest als neues Ergebnis benutzen.
- Zum Rechnen mit Resten benötigen wir des weiteren einige grundlegende Sätze aus der elementaren Zahlentheorie (vgl. Kap. II), insbesondere zum Rechnen mit Zahlen **modulo** n.

- Julius Caesar (100 bis 44 v. Chr.)
- Jedes Klartextzeichen wird um **drei** Positionen verschoben.

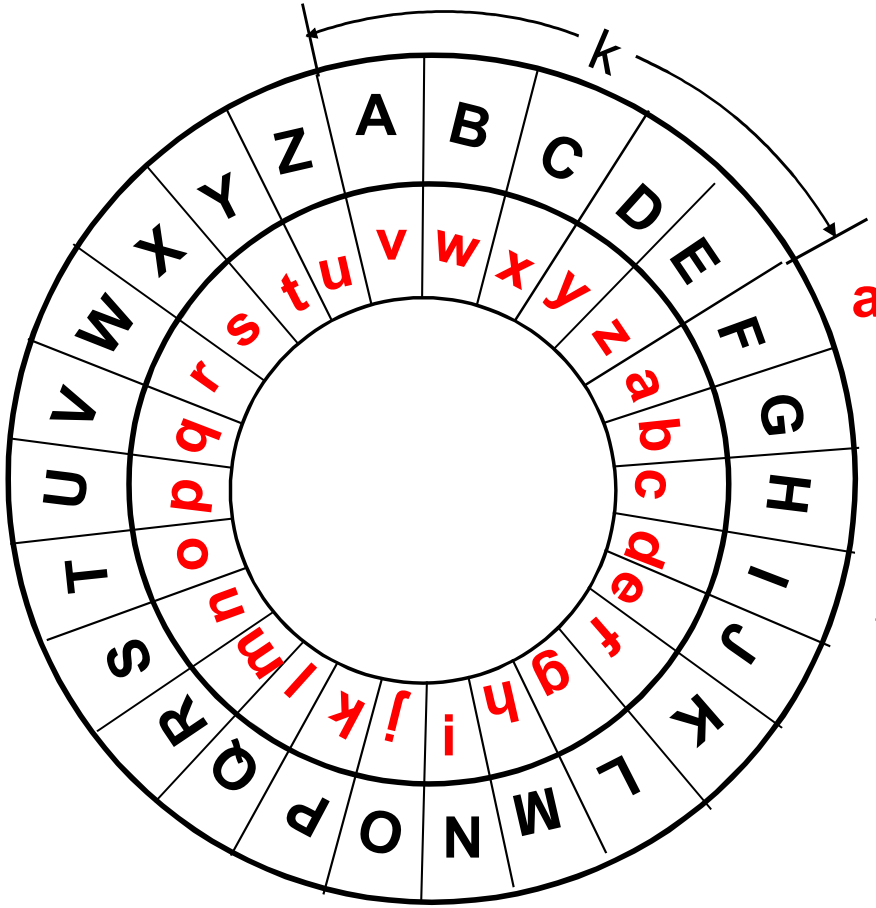
Klartext:	a	b	c	d	e	f	g	...	z
Chiffretext:	D	E	F	G	H	I	J	...	C

- Verallgemeinerung: Bei einer Verschiebechiffre wird jedes Klartextzeichen **z** durch ein um **k** Zeichen im Alphabet verschobenes Zeichen ersetzt.

  Es sei A ein Alphabet mit n Zeichen, die von 0 bis n-1 durchnumeriert sind. Dann gilt für eine Verschiebechiffre allgemein: $\mathbf{E: z \rightarrow (z + k) \bmod n}$
- Eigenschaften:
  - Durch Probieren leicht zu knacken
  - Durchführung von Häufigkeitsanalysen möglich

Die 26 möglichen Verschiebechiffren:

Klartext:		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
Chiffretexte:	**0**	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
	1	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	A
Schlüssel	**2**	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
k	**3**	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
	4	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
	5	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
	6	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
	7	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
	8	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
	...																										
	25	Z	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



a b c ... z = Klartextzeichen

A B C ... Z = Chiffretextzeichen

Schlüssel

hier: k = 5

Kap. 3: Monoalphabetische Chiffren und deren Analyse

Teil 3: Komplexe Verschiebechiffren

- Multiplikative Chiffren
- Affine Tauschchiffren

- Bei einer multiplikativen Chiffre über dem Alphabet A wird jedes Klartextzeichen z mit einer Zahl $t \in \{0, 1, ..., n\}$ multipliziert.
- t und n = |A| (Mächtigkeit) müssen teilerfremd sein, d. h. es muss gelten: ggT(t, n) = 1
- Die Chiffrevorschrift lautet:

$$\mathbf{E: \ z \rightarrow (z \cdot t) \bmod n} \ \text{ mit } \ \mathbf{t \in Z_n \setminus \{0\} = \{1, ..., n-1\}}$$

- Zu jeder multiplikativen Chiffre E mit ggT(t, n) = 1 gibt es eine multiplikative Dechiffrierfunktion D mit D(E(z)) = z für $\forall \ z \in A$.
- Es gilt:

$$\mathbf{D: \ z' \rightarrow (b \cdot z') \bmod n} \ ,$$

wobei $b \in \mathbf{Z_n}$ mit $t \cdot b \equiv 1 \bmod n$ ist.

- Sei ggT(t, n) = 1. Dann wird jede Chiffre

  $$\mathbf{E: z \rightarrow (z \cdot t + k) \bmod n \text{ mit } t \in Z_n \setminus \{0\} = \{1, ..., n-1\}}$$

  eine ***affine Chiffre*** oder Tauschchiffre genannt.

- Um aus Chiffrezeichen z‘ wieder Klartextzeichen berechnen zu können, wendet man die Dechiffrierfunktion D wie folgt an:

  $$\mathbf{D: z' \rightarrow (b \cdot z' + l) \bmod n},$$

  wobei $b, l \in \mathbf{Z_n}$ mit $t \cdot b \equiv 1 \bmod n$ und $l \cdot t \equiv (n - k) \bmod n$ gilt.
  Ferner besteht der Zusammenhang: $l = b\,(n - k) \bmod n$

- Beispiel: $t = 5; k = 7; n = 26$

  $\Rightarrow$ $E: z' = (5 \cdot z + 7) \bmod 26$ mit der Dechiffrierfunktion

  $D: z = (21 \cdot z' + 9) \bmod 26$, um aus z‘ wieder z berechnen zu können $\rightarrow b = 21; l = 9$ und $t \cdot b = 105 \equiv 1 \bmod 26$.

z	z‘ = (5·z + 7) mod 26	z = (21·z‘ + 9) mod 26
1	12	(21·12 + 9) mod 26 = 1
2	17	(21·17 + 9) mod 26 = 2
3	22	(21·22 + 9) mod 26 = 3
4	1	(21·1 + 9) mod 26 = 4
...	...	...
12	15	(21·15 + 9) mod 26 = 12

Kap. 3: Monoalphabetische Chiffren und deren Analyse

Teil 4: Häufigkeitsanalyse

- Buchstabenverteilungen
- Bi- und Trigramme

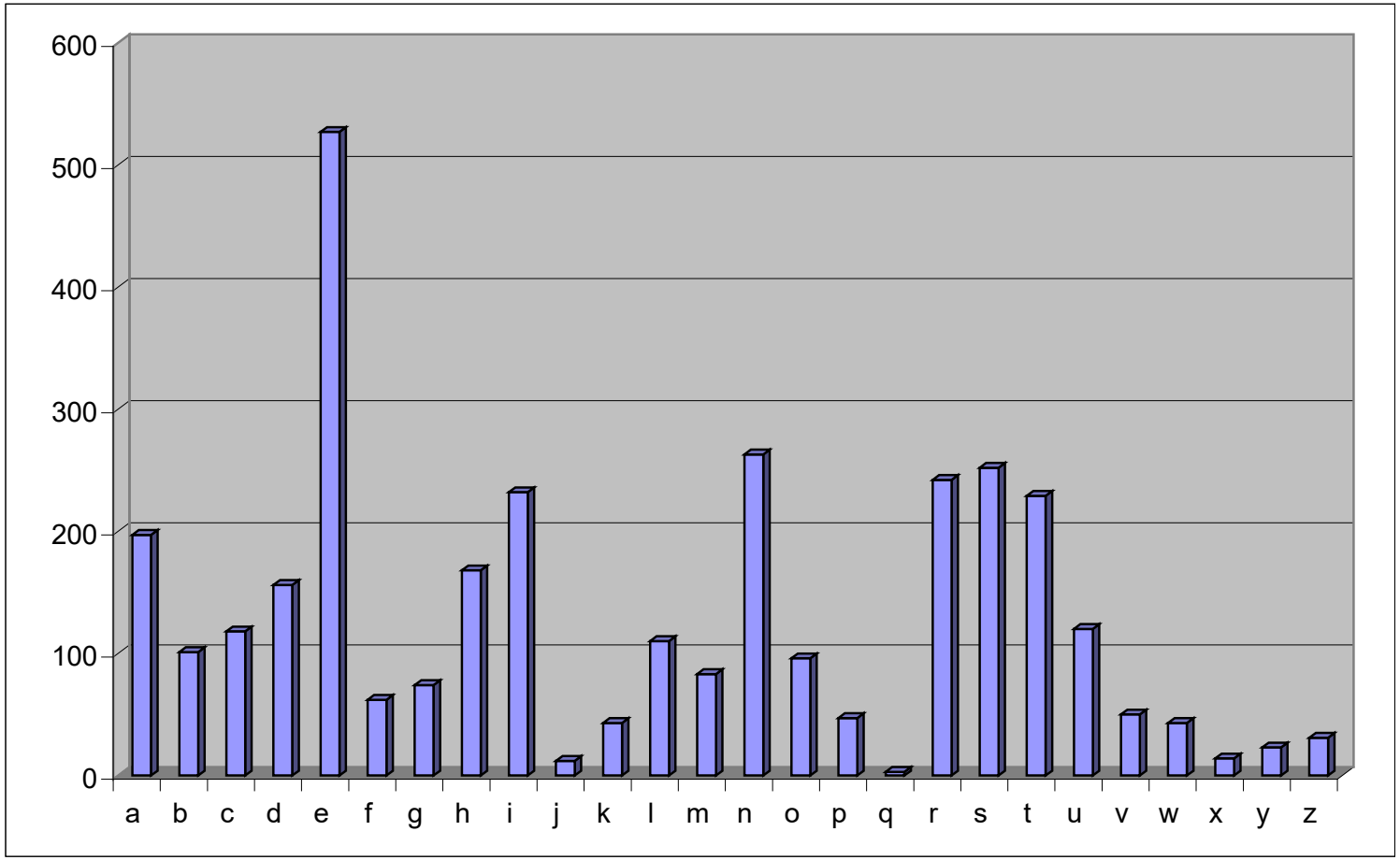
Buchstabe	Häufigkeit [%]	Buchstabe	Häufigkeit [%]
a	6,51	n	9,78
b	1,89	o	2,51
c	3,06	p	0,79
d	5,08	q	0,02
e	17,40	r	7,00
f	1,66	s	7,27
g	3,01	t	6,15
h	4,76	u	4,35
i	7,55	v	0,67
j	0,27	w	1,89
k	1,21	x	0,03
l	3,44	y	0,04
m	2,53	z	1,13

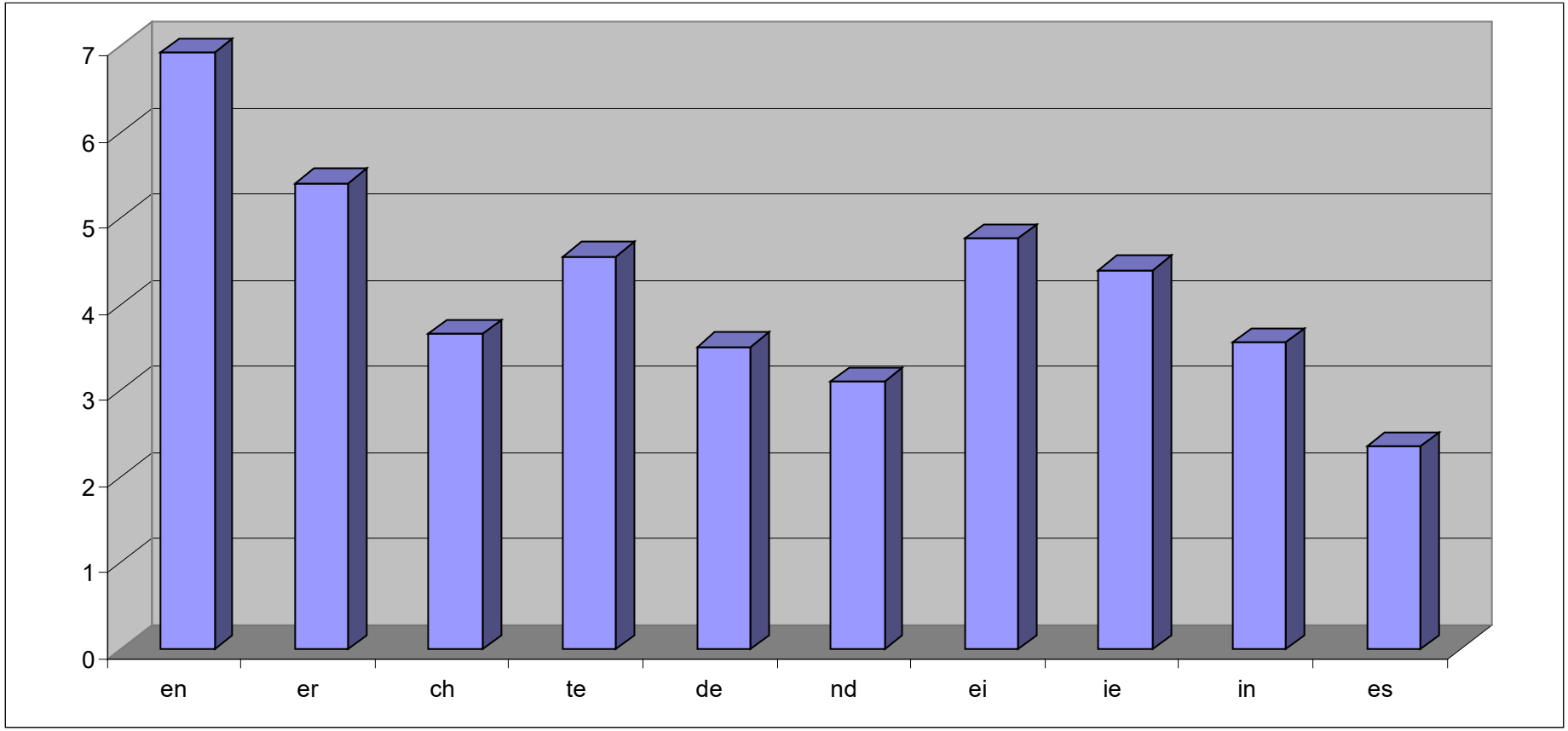
Gruppenhäufigkeiten und Bigramme der deutschen Sprache:

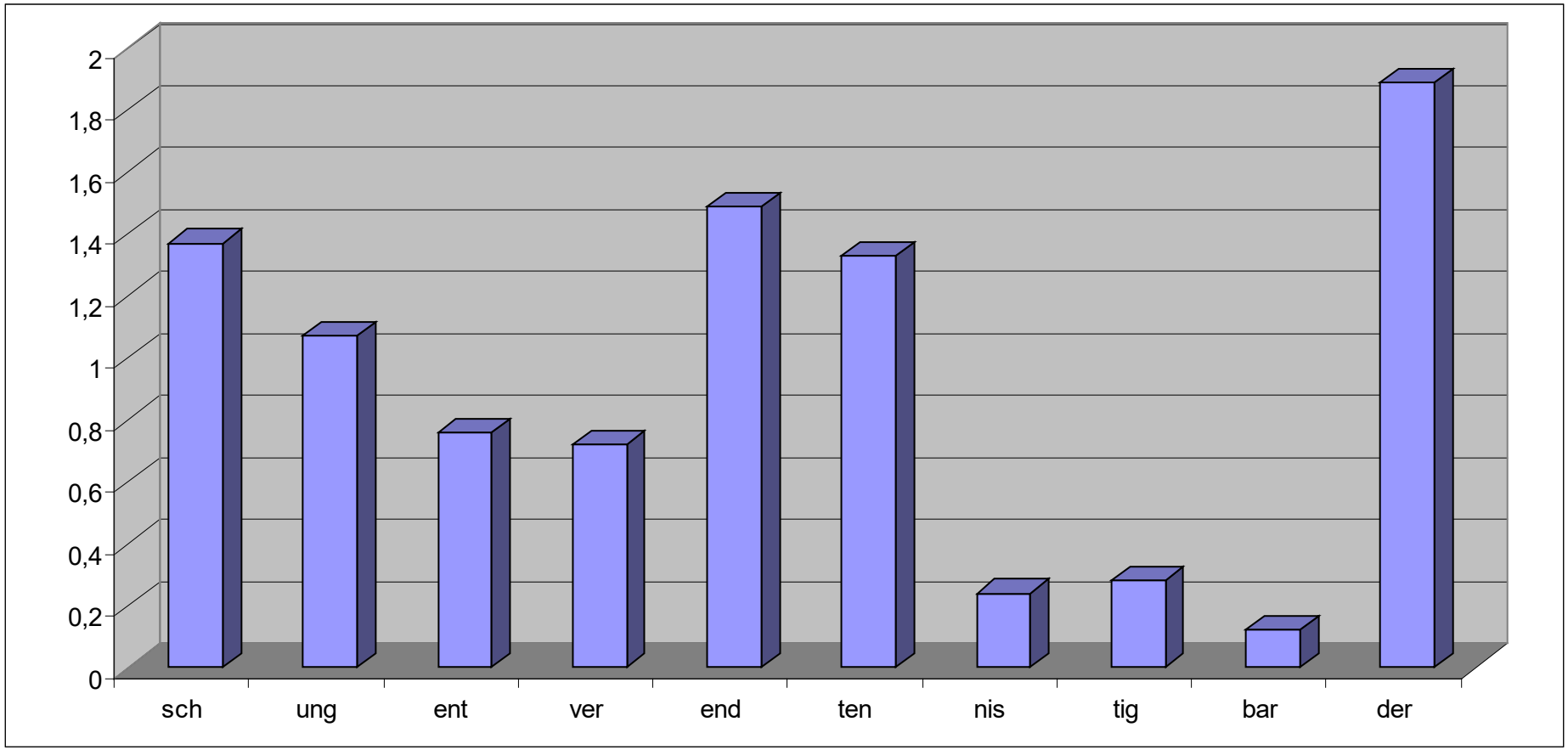
Gruppe	Anteil der Buchstaben dieser Gruppe an einem Text in [%]
e, n	27,18
i, s, r, a, t	34,48
d, h, u, l, c, g, m, o, b, w, f, k, z	36,52
p, v, j, y, x, q	1,82

Buchstabenpaar	Häufigkeit [%]	Buchstabenpaar	Häufigkeit [%]
en	3,88	nd	1,99
er	3,75	ei	1,88
ch	2,75	ie	1,79
te	2,26	in	1,67
de	2,00	es	1,52

Buchstabe	Häufigkeit [%]	Buchstabe	Häufigkeit [%]
a	8,2	n	6,7
b	1,5	o	7,5
c	2,8	p	1,9
d	4,3	q	0,1
e	12,7	r	6,0
f	2,2	s	6,3
g	2,0	t	9,1
h	6,1	u	2,8
i	7,0	v	1,0
j	0,2	w	2,4
k	0,8	x	0,2
l	4,0	y	2,0
m	2,4	z	0,1


600
500
400
300
200
100
0
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


7
6
5
4
3
2
1
0
en
er
ch
te
de
nd
ei
ie
in
es


2
1,8
1,6
1,4
1,2
1
0,8
0,6
0,4
0,2
0
sch
ung
ent
ver
end
ten
nis
tig
bar
der

```
/* Datum: 19.07.2002                                                    */
/* Autor: Bernhard Geib                                                 */
/* Funktion: Verschluesselung mit einer affinen Tauschchiffre           */

#include <stdio.h>

int main (void)
{  int c;

   c = getchar();
   while (c != EOF)
   {
      if (c != '\n')
      {
         c = (17 * c + 4) % 256;
      }
      printf ("%c", c);
      c = getchar();          }
   return 0;                  }
```

```
/* Datum: 19.07.2002                                                    */
/* Autor: Bernhard Geib                                                 */
/* Funktion: Entschluesselung mit einer affinen Tauschchiffre           */

#include <stdio.h>

int main (void)
{  int c;

   c = getchar();
   while (c != EOF)
   {
      if (c != '\n')
      {
         c = (241 * c + 60) % 256;
      }
      printf ("%c", c);
      c = getchar();          }
   return 0;                  }
```