Entschlüsselung geheimer Botschaften am Computer

Arbeitsblatt 3

Die Vigenère Verschlüsselung, eine polyalphabetische Substitution:

Vigenère-Quadrat:

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
s	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
c	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
h	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
l	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
u	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
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	e
s	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
s	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
e	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
l	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	i
w	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j
o	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	k	k
r	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l
t	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m
↓	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n
	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	l	l	m	n	o
	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p
	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q
	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r
	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s
	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t
	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u
	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v
	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w
	y	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
	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

Verschlüsselung von „HEUTE IST ES SEHR HEISS“ mit dem Schlüsselwort „primzahl“:

Klartext:	H	E	U	T	E	I	S	T	E	S	S	E	H	R	H	E	I	S	S
	p	r	i	m	z	a	h	l	p	r	i	m	z	a	h	l	p	r	i
Chiffretext:			c	f	d	i	z	e	t	j	a	q	g	r	o	p	x	j	a

Aufgabe 5 (gemeinsam/schriftlich): Entschlüssle mit dem Schlüsselwort „handy“ den Text

a e k w c l n g v a o l h h q z e y q k h c u w q w a f v

Aufgabe 6 (gemeinsam): Entschlüssle den Text aus der Datei `text5-Vigenere.txt` mit Hilfe des Vigenere-Breakers.

Aufgabe 7 (schriftlich): Entschlüssle den Text aus der Datei `text6-Vigenere.txt` mit Hilfe des Vigenere-Breakers.
Hinweis: Die Schlüssellänge ist 10.

Anmerkungen:

Vorteil: Die Buchstabenhäufigkeit ist versteckt. Gleiche Buchstaben werden verschieden verschlüsselt

Nachteil: Nach l Buchstaben (l =Länge des Schlüsselwortes) wiederholt sich die Verschlüsselung, jeder Block aus l Buchstaben wird nach dem gleichen Prinzip verschlüsselt

Vigenère-Verschlüsselung knacken:

- Finde die Länge l des Schlüsselwortes
- Schreibe den verschlüsselten Text in l Spalten
- In jeder Spalte Häufigkeitsanalyse liefert die Codierung von „E“

Dann ist das Schlüsselwort bekannt, der Text kann entschlüsselt werden.

Hinweise zu CrypTool: Die vermutete Länge des Schlüsselwortes (Abstand der höchsten Balken) eingeben (bei unserem Text 10). Das Schlüsselwort wird zu AAAAAAAAAA gesetzt. Dann auf den ersten Buchstaben des Schlüsselwortes klicken. Das Programm unterteilt den Geheimtext in Blöcke, die gleich lang wie das Schlüsselwort sind. Die grünen Balken stellen eine Häufigkeitsanalyse der Buchstaben dar, die in den Blöcken an erster Stelle stehen. Den höchsten grünen Balken durch klicken auf `Links` oder `Rechts` auf `E` schieben. Dann ist der erste Buchstabe des Schlüsselwortes bestimmt. Nun auf den zweiten Buchstaben des Schlüsselwortes klicken. Nun stellen die grünen Balken eine Häufigkeitsanalyse der Buchstaben dar, die in den Blöcken an zweiter Stelle stehen. Wieder den höchsten Balken auf `E` schieben. Entsprechend so lange weitermachen, bis alle Buchstaben des Schlüsselwortes bestimmt sind.
Unterhalb der Balkengraphik steht nun der entschlüsselte Text.