Übungen zu Substitutionsverfahren

1. Übungsaufgabe:

Entschlüsseln Sie den Schlüsseltext = LNLDLRQGYZLYPXKNTLPPLNTRA, der mit Hilfe einer monoalphabetischen Substitution mit der nachfolgenden Verschlüsselungsvorschrift verschlüsselt wurde:

```
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
Schlüsseltext: G W X V L O A K U B C N D R M F H Y P Q T Z E I J S
```

2. Übungsaufgabe:

Der Schlüsseltext = 34 75 61 47 80 01 93 78 41 51 93 25 04 29 72 64, der mit Hilfe einer homophonen Substitution verschlüsselt wurde, soll von Ihnen mit der folgenden Verschlüsselungsvorschrift entschlüsselt werden.

Klartext:	Schlüsseltext:
A	(10,21,52,59,71)
B	(20,34)
C	(28,06,80)
D	(19,58,70,81,87)
E	(09,18,29,33,38,40,42,54,55,60,66,75,85,86,92,93,99)
F	(00,41)
G	(08,12,97)
H	(01,07,24)
I	(14,39,50,65,76,88,94)
J	(57)
K	(23)
L	(02,05,82)
M	(27,11,49)
N	(30,35,43,62,67,68,72,77,79)
O	(26,53)
P	(31)
Q	(25)
R	(17,36,51,69,74,78,83)
S	(15,16,45,56,61,73,96)
T	(13,32,90,91,95,98)
U	(03,04,47)
V	(37)
W	(22)
X	(44)
Y	(48)
Z	(64)

3. Übungsaufgabe

Der Schlüsseltext = S Y U H X D U T H K I Z J E wurde mit Hilfe einer polyalphabetischen Substitution unter Verwendung des Schlüssels = GEHEIM verschlüsselt.

a) Wie lautet der dazugehörige Klartext?

b) Sie kennen den Klartext = IF UNMODIFIED SINCE, den

Schlüsseltext = MS WBPWQOJVGR VQAII sowie die

Verschlüsselungsvorschrift (siehe unten). Wie lautet der verwendete Schlüssel?

c) Schicken Sie Ihrem Nachbarn eine verschlüsselte Nachricht. Die Nachricht soll mit der polyalphabitischen Substitution und der dazu notwendige Schlüssel mit der homophonen Substitution (siehe Übung 2) verschlüsselt werden. Viel Spaß.

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**
Schlüsseltext:	**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**
	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**
	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**
	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**
	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**
	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**
	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**
	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**
	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**
	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**
	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**
	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**
	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**
	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**	**K**	**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**

Übung zu Tranpositionsverfahren

1. Übungsaufgabe:
Der Schlüsseltest = SACBUHNWEAEESLI soll nach dem Zick-Zack-Verfahren von Ihnen entschlüsselt werden. Wie heißt der Klartext und der Schlüssel (Tiefe des Verfahrens)?

Übungsaufgabe zur Kryptoanalysis
Der folgende Schlüsseltext ist mit Hilfe einer monoalphabetischen Substitution verschlüsselt worden.
Ihre Aufgabe soll sein, den Text zu entschlüsseln bzw. die Verschlüsselungsvorschrift mit Hilfe einer statistischen Analyse (siehe Häufigkeit der Buchstaben) des Schlüsseltextes oder durch ausprobieren zu erhalten. Der Originaltext (Klartext) ist in deutscher Sprache.

Schlüsseltext:

Rq efy Gaseysrtl tiun yftys Wfypjinp wat

Wyszunpryzzyprtlzwysginsyt

ysgryppyt jr oayttyt oitt qit efyzy Iplasfdnqyt jrziydjpfun wat

yftyq Visiqydys ikniytlfl qiunyt eys eyt Ikpirg eys

Dsitzgasqidfat za zdiso kyyftgprzzd eizz anty zyfty Oyttdtfz

oyfty Ytdzunpryzzyprtl qaylpfun fzd