

Aufgabenblatt 13

Abgabe: 06.03.2017

Am 20. und 27. Februar findet jeweils kein Zirkel statt! Der nächste Termin ist also dementsprechend der 6. März.

Aufgabe 1.

Ist die folgende Aussage richtig: „Es ist entscheidend, dass an jeder Stelle des Kryptogramms der Schlüssel eindeutig den Klartextbuchstaben zu jedem Geheimtextbuchstaben festlegt“?

Aufgabe 2.

Der folgende Text wurde mit dem Vigenère-Algorithmus verschlüsselt. Bestimme mit dem Kasiski-Test die Schlüsselwortlänge, bestimme das Schlüsselwort und entschlüssele den Text!

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

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

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

Aufgabe 3.

Man kann das Verfahren von Vigenère auch dann anwenden, wenn man die Buchstaben durch die Zahlen 0, 1, ..., 25 darstellt. Beschreibe diese „modulo 26-Variante“ des Vigenere-Algorithmus.

Aufgabe 4.

- a) Schreibe ein Programm, das
- die Länge n eines Textes bestimmt,
 - die Häufigkeiten n_1, \dots, n_{26} der Buchstaben dieses Textes bestimmt, und
 - den Koinzidenzindex des Textes berechnet.
- b) Entwerfe ein Programm zur Vigenère-Chiffrierung, sowie eines, das Vigenère-chiffrierte Texte knackt.