Prüfung B: Bedingungen, Schleifen, Chiffrierung, 4AB

Donnerstag, 31. März 2022

Zeit: 40 Minuten max. Punktezahl: 15.5

Hilfsmittel: keine, ohne Laptop

Name: Lösung Total Punkte: Note:

Aufgabe 1 (3 Punkte)

Kurzfragen zur Programmierung:

a) Stelle eine Wahrheitstabelle auf für den Ausdruck

1.5

```
(not B) or A
```

`True` darfst Du mit `T` und `False` mit `F` abkürzen.

A	B	not B	(not B) or A
T	T	F	T
T	F	T	T
F	T	F	F
F	F	T	T

Pro Fehler -0.5
falls Begründung stehen + andere Tabellenspalten
→ FF möglich

1.5 b) Schreibe folgenden Code mithilfe einer `repeat :` Anweisung anstelle von `repeat 6:`.

```
1 x = 0
2 repeat 6:
3     x +=2
```

```
x = 0
zaehler = 0
repeat :        OHNE Zahl
    x += 2
    zaehler += 1
    if zaehler >= 6:
        break
```

Idee if/break 0.5
Korrektheit 0.5
Zählervariable 0.5

Aufgabe 2 (4 Punkte)

Gegeben ist der Programmcode

```
1 x = 0
2 while x < 16:
3     y = input("Zahl = ")
4     if y > 0 and y <= 4:
5         x += y*y
6     elif y < 0 and y >= -4:
7         break
8     print(x)
```

a) Was gibt das Programm in der Ausgabe aus, wenn der Benutzer die folgenden Zahlen nacheinander eingeben würde

3 20 -40 -2 0 5 ...

Wichtig: Der Benutzer muss vielleicht gar nicht alle Zahlen eingeben, da sich das Programm schon früher beendet.

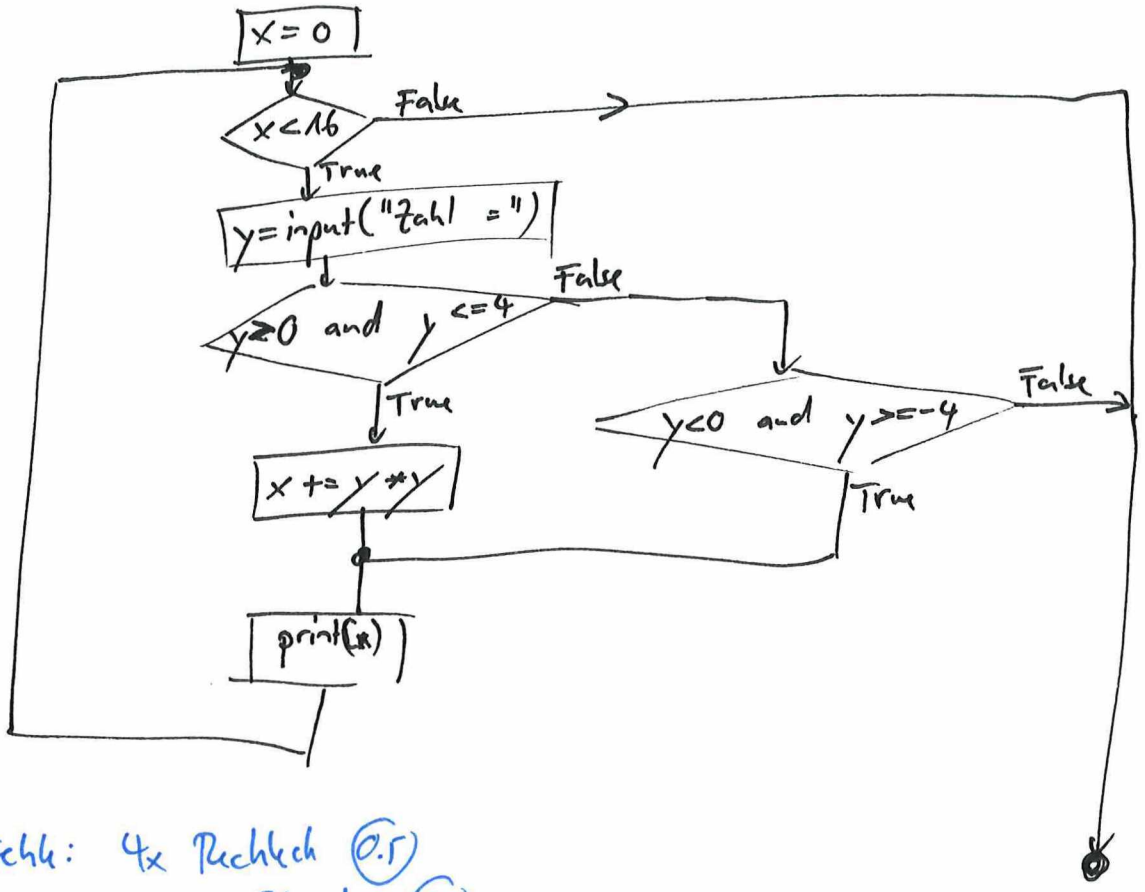
Eingabe: 3 → Zeile 5 : x += 9
Eingabe: 20 → Ausgabe: 9
Eingabe: -40 → Ausgabe: 9
Eingabe: -2 → Zeile 7: break → Ausgabe: 9

4 Durchläufe (0.5) : Kein Ausgabe ist "nicht möglich"
Werte (0.25)

b) Erstelle ein Flussdiagramm für die Zeilen 1–10.

Mehr Platz auf der nächsten Seite.

Mehr Platz für Aufgabe 2.



Befehle: 4x Rechteck (0.5)
Verzweigungen: 3x Rhombus (0.5)
Reihenfolge/Verketzung bei if (1)
While-Rückkopplung (0.5)
Sauberkeit (T/F, zusammengefasst etc.) (0.5)

Aufgabe 3 (1.5 Punkte)

Erkläre den **Unterschied** zwischen monoalphabetischen und polyalphabetischen Verschlüsselungen. Gib zur Illustration **je ein Beispiel** für eine monoalphabetische und eine polyalphabetische Verschlüsselung an.

Monoalphabetisch: (0.5) Klartextsymbole werden unabhängig von ihrer Position immer mit dem gleich Geheimtextsymbol codiert. Bsp: Caesar (0.25)

Polyalphabetisch: (0.5) Je nach Position wird das gleich Klartextsymbol mit unterschiedlichen Geheimtextsymbole codiert.
Bsp: Enigma, unterschiedlich Caesar mit gerade & ungerade Positionen. (0.25)

Aufgabe 4 (2.5 Punkte)

Christie benutzt eine 2×3 Tabelle zur Verschlüsselung mit Geheimtextsymbolen zusammengesetzt aus A, E, O und ¨, ˆ. Das Klartextalphabet besteht nur aus den ersten sechs Buchstaben des lateinischen Alphabetes A, B, C, D, E, F (damit die Aufgabe nicht zu aufwändig wird):

	E	O	A
¨	A	B	C
ˆ	D	E	F

Tabelle (1)

Dechiffriere den Geheimtext

Ä Ö Ä Ö Ë Ö Ô Â

und vervollständige die obige Verschlüsselungstabelle (graue Felder). Es ist bekannt, dass im Klartext B am häufigsten vorkommt und D gar nie.

Beachte: Der Klartext ergibt eine sinnlose Aneinanderreihung von Buchstaben.

Ö : 3x → B
Ë : 0x → D

Häufigkeit (0.5)

⇒ C B C B A B E F

Klartext (1)

Aufgabe 5 (4.5 Punkte)

Bob benutzt folgendes Kryptosystem mit Schlüssel (i, j) zur Chiffrierung von Text:

Schritt 1: Verschlüsselung mit CAESAR mit Schlüssel i.

Schritt 2: Verwendung der ursprünglichen SKYTALE mit j Zeilen, wobei $j \in \{1, 2, 3, 4, 5\}$.

Als Hilfe ist das Alphabet abgedruckt:

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

Löse dazu folgende Aufgaben:

a) Folgenden Geheimtext hat er mit dem Schlüssel (3, 4) erhalten. Dechiffriere den Text:

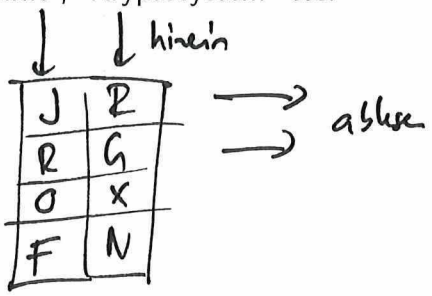
J R O F R G X N

b) Wieviele Schlüssel besitzt das Kryptosystem, das Bob verwendet? Welche davon führen zum Klartext?

c) Eine besonders geheime Nachricht verschlüsselt Bob, indem er sein Kryptosystem zweimal nacheinander anwendet, d.h. er verschlüsselt den Klartext mit einem ersten Schlüssel (i, j) und das Resultat nochmals mit einem anderen Schlüssel (i', j'). Erhöht dies die Sicherheit? Begründe mit Begriffen wie "Anzahl Schlüssel", "Geheimschrift", "Kryptosystem" etc.

1.5

a) SKYTALE 4 rückgängig



⇒ JRRGOXFN (1.5)

Caesar 3 rückgängig machen

⇒ GOODLUCK

b) Caesar i: 26

Skytale j: 5

5 · 26 = 130 (1)

Zum Klartext für i = 0 und j = 1. (0.5)

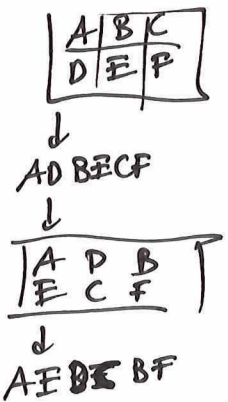
Mehr Platz auf der Rückseite.

c) • 2x Caesar nacheinander nützt nichts: $i+i'$ als Schlüssel (0.5)

• 2x SKYTALE:

Fall 1: j oder $j'=1$ Keine Verbesserung (0.25)

Fall 2: j und $j'>1$ Allgemein wird dies sicherer. (0.5) Diskussion von Fälle z.B. $j=j'=2$



Fazit: Anzahl Schlüssel wird grösser und $\sqsubset$ j und $j' \neq 1$ (0.25) werden die Positionen auch mehr durchgemischt.

Ausnahm: Wenn jj' die Nachrichtenlänge ist → Klartext!

$j=2$ GOOD / LUCK → GLOU OCDK

$j'=4$ GLOU / OCDK → GOODLUCK