Prüfung A: Bedingungen, Schleifen, Chiffrierung, 4AB

Donnerstag, 31. März 2022

Zeit: 40 Minuten max. Punktezahl: 15.5

Hilfsmittel: keine, ohne Laptop

Name: Lösungen Total Punkte: Note:

Aufgabe 1 (3 Punkte)

Kurzfragen zur Programmierung:

a) Stelle eine Wahrheitstabelle auf für den Ausdruck (1.5)

```
(not A) and B
```

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

A	B	not A	(notA) and B
T	T	F	F
T	F	F	F
F	T	T	T
F	F	T	F

pro Fehler (-0.5)

falls Begründungen stehen + andere Tabellenspalten → FF möglich

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

```
1 x = 0
2 while x < 100:
3     x +=2
```

Total 50 Durchläufe bis x gleich 100 ist.

```
x = 0
repeat :
    x += 2
    if x >= 100:
        break
```

OHNE Zahl

Idee if/break (0.5)

Bedingung (0.5)

Korrektheit (0.5)

Aufgabe 2 (4 Punkte)

Gegeben ist der Programmcode

```
1 x = 0
2 while x < 25:
3     y = input("Zahl = ")
4     if y > 0 and y <= 5:
5         x += y*y
6     elif y < 0 and y >= -5:
7         break
8     print(x)
```

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

4 20 5 0 -40 5 ...

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

Ausgabe

Eingabe 4: Zeile 4&5 x ← 16 → 16

Eingabe 20: Weder 4 noch 6 x bleibt → 16

Eingabe 5: Zeile 4&5 x um 25 erhöht → 41

Bedingung 2 nicht mehr erfüllt.

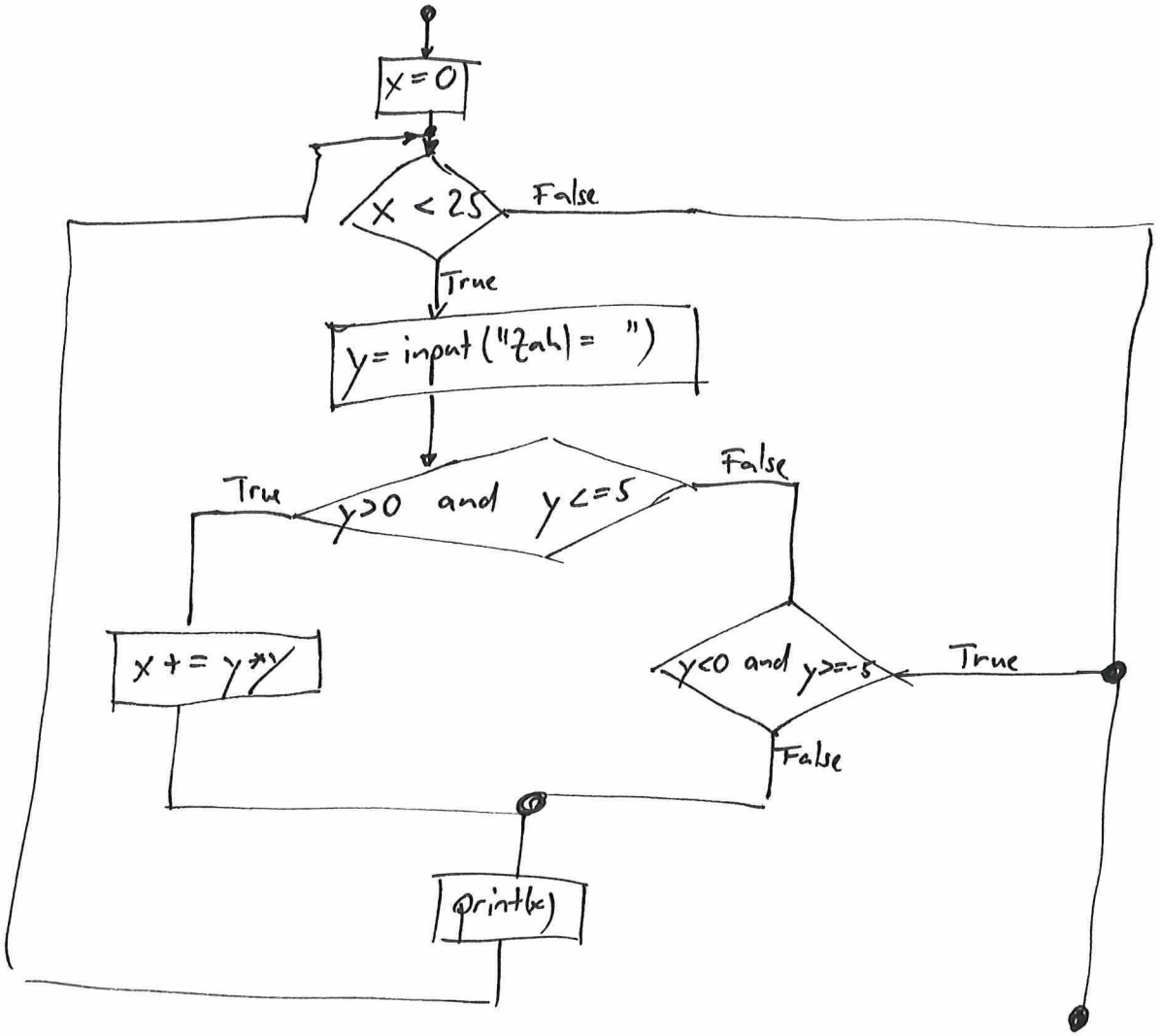
3 Durchläufe (0.75) Keine Ausgabe ist "nicht möglich"

Werte (0.25)

(3) b) Erstelle ein Flussdiagramm für die Zeilen 1–~~10~~ 8.

Mehr Platz auf der nächsten Seite.

Mehr Platz für Aufgabe 2.



Befehle 4x Rechteck (0.5)

Verzweigung 3x Rhombus (0.5)

Reihenfolge / Vernetzung bei if (1)

While - Rückkopplung (0.5)

Sauberkeit (T/F, Zusammenführt etc.) (0.5)

Aufgabe 3 (1.5 Punkte)

Erkläre den Unterschied zwischen einer Geheimschrift und einem Kryptosystem. Gib zur Illustration **je ein Beispiel** für eine Geheimschrift und ein Kryptosystem an.

Kryptosystem: Sammlung von Geheimschriften, die durch die Angabe eines Schlüssels bestimmt wird. (0.5) (0.25)

Bsp: Geheimschrift z.B. Polybios

Kryptosystem z.B. CAESAR (26 Schlüssel) (0.75)

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):

Tabelle (1)

	Ô	A	Ê
ˆ	A	B	C
¨	D	E	F

Häufigkeit (0.5)

Als Hilfe ist das Alphabet abgedruckt:

Ô: 3x → A
Ê: 0x → C

Â Ô Â Ô Ë Ô Ö Ä

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

Beachte: Der Klartext ergibt eine sinnlose Aneinanderreihung von Buchstaben.

Klartext: B A B A F A D E

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: Vertauschen von Symbolen nach folgendem Muster: Der Klartext wird in 4er Blöcke aufgeteilt und dann jeweils das erste Symbol eines Blockes mit dem j-ten Symbol des Blocks vertauscht, wobei $j \in \{1, 2, 3, 4\}$ ist.

Als Hilfe ist das Alphabet vorbereitet:

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:

1.5 a) Folgenden Geheimtext hat er mit dem Schlüssel $(2, 4)$ erhalten. Dechiffriere den Text:

G W V I I V C P

1.5 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.

a) G W V I | I V C P

1.5 | W V G | P V C | Caesar -2

G U T E N T A G ⇒ Guten Tag.

b) • Caesar: 26
Tausch: 4
Total: $4 \cdot 26 = 104$ (1)

• $i=1$ und $j=1$ ⇒ Klartext (0.5)

c) • 2x Caesar nacheinander mit i und i' ist einfach Caesar mit $i+i'$ → Macht es nicht sicherer. (0.5) Caesar

• Zweimal Vertauschen nacheinander kann schwieriger oder einfacher werden

(0.5) Schritt 2

$j=1$, $j' \neq 1$ → heben sich auf

Fall 1: ⇒ $j = j'$ wird einfach

Fall 2: $j \neq j'$, $\neq 1$ bleibt gleich

Fall 3: $j \neq j'$; beide $\neq 1$

(2,3), (2,4), (3,4)

A B C D
B A C D
C A B D

⇒ 3 Buchstaben vertauscht

Anzahl Schlüssel viel grösser, aber nur in wenigen Fällen sicherer, manchmal sogar schlechter. ⇐ (0.5) Fazit

Mehr Platz auf der Rückseite.