Java Basis 2014 - 2015
Project 1 :
Cryptografie: handcijfers

K. Verbeeck T. Vermeulen B. Van Damme
P. Demeester J. Maervoet

1 Richtlijnen

- De communicatie met de gebruiker gebeurt via het console venster. Gebruik hiervoor de klasse `Input`.
- Verzorg je algemene programmastructuur: Maak met andere woorden gebruik van zorgvuldig gekozen methoden en velden. Denk goed na over de bedoeling en de functie van elke methode. Werk met parameters en returntypes en lokale variabelen.
- Respecteer de stijlregels! Ga voor een verzorgde en consequente programmeerstijl:
  - zinvolle naamgeving van methoden, velden, variabelen, ...
  - spaties, lege lijnen, indentering, ...
- Maak je methoden niet te lang. Als je methode toch te lang dreigt te worden, splits zinvol uit volgens deelfunctionaliteit.
- Werk met een aparte (start)methode die de control flow van je programma beheert (dus niet alles in je main!). Schrijf geen spaghetti-code, m.a.w; elke methode heeft zijn eigen functionaliteit, bv. iets berekenen. Op het einde van die methode geef je dan netjes het resultaat terug, en doe je geen nieuwe methode oproep voor het vervolg. Dit moet opnieuw gebeuren in je control flow of start methode.
- Voorzie je programma van voldoende (maar ook niet te veel!) en zinvolle commentaar.
- Voorzie java documentatie bovenaan je klasse. Gebruik de reeds gekende Javadoc tags.

2 Afspraken

Je project moet ten laatste op **maandag 1 december, 12u s' middags** geüpload zijn. Naast het indienen van je toepassing via Toledo bezorg je je labodocent ook een geprint exemplaar via je labobundel tijdens het eerstvolgend labo. Bij het betrappen op fraude en/of kopiëren zal er een fraudedossier worden opgesteld en voorgelegd worden aan de examencommissie.

3 Opgave

Cryptografie of geheimschrift houdt zich bezig met het versleutelen van informatie. De dag van vandaag gebeurt dit natuurlijk via de computer, maar vroeger werden handcijfers of veldcijfers ingezet om geheime boodschappen te communiceren tijdens een veldslag bijvoorbeeld en dit zonder speciale toestellen. Handcijfers zijn vercijferingsmethodes die met behulp van een geheim sleutelwoord of zin een tekst omzetten naar op het eerste zicht onleesbare code. De tekst kan echter eenvoudig ontcijferd worden als men in het bezit is van dezelfde geheime sleutel. In de wereld van geocaching vind je nog heel wat van deze handcijfers terug (`http://www.geocachingtoolbox.com/`)

In dit project zal je een programma schrijven dat berichten kan versleutelen en ook weer kan ontcijferen aan de hand van 1 van de volgende techniek(en) (je mag zelf de keuze maken of je techniek1 of techniek2 implementeert) :

Techniek 1 Dit is een versleuteling in 2 stappen : als eerst wordt elke letter van de oorspronkelijke tekst binair gecodeerd (d.i. omgezet naar een 2 letter alfabet). Twee tekens (bijvoorbeeld a en b) worden gebruikt op vijf posities, dus er zijn $2^5 (= 32)$ mogelijkheden waarvan er 26 worden gebruikt. In een volgende stap zal een niets zeggend bericht gebruikt worden met de kleine nuance dat er twee verschillende opmaakstijlen gebruikt worden om deze te schrijven (bvb elke willekeurige kleine letter stelt een a voor; elke willekeurige grote letter een b) op die manier zal het niets zeggend bericht doorgestuurd worden. De ontvanger kan dit omzetten naar een opeenvolging van a's en b's en het bericht ontcijferen met de binaire omzet tabel.

Stel dat de binaire omzettabel eenvoudig de binaire voorstelling is van cijfer 0 (a) tot cijfer 25 (z).

a → aaaaa	h → aabbb	o → abbba	u → babaa
b→ aaaab	i → abaaa	p → abbbb	v → babab
c → aaaba	j → abaab	q → baaaa	w → babba
d → aaabb	k → ababa	r → baaab	x → babbb
e → aabaa	l → ababb	s → baaba	y → bbaaa
f → aabab	m → abbaa	t → baabb	z → bbaab
g → aabba	n → abbab		

Dan zal het bericht :

cOmmUnicatIeAdViseur

zich als volgt vertalen in een serie van a's en b's :

abaabaaaaababababaaaaa

De omzetting via de vertaaltabel geeft dan het woord : `java` .

Techniek 2 De tweede techniek bestaat eveneens uit 2 stappen en de eerste stap is opnieuw een substitutie. Deze keer wordt een letter vervangen door een andere letter die `N` stappen verder staat . Wanneer $N = 4$ dan geeft dit : $a \rightarrow e$, $b \rightarrow f$ enz. Het einde van het alfabet wordt dan omgezet naar het begin : $w \rightarrow a$, ... , $z \rightarrow d$. In een tweede stap gaat een sleutelwoord gekozen worden, bijvoorbeeld de sleutel : `java` en worden de letters uit de vorige stap opgeteld bij deze van het sleutelwoord (modulo 26). Dit geeft het volgende als we het woord `programma` willen versleutelen :

stap 1 tel $N = 4$ stappen verder dan krijgen we het woord : `tvskveqqe`

stap 2 tel vervolgens dit woord op met de sleutel `java` :

	j	a	v	a	j	a	v	a	j
+	t	v	s	k	v	e	q	q	e
	c	v	n	k	e	e	l	q	n

Het optellen modulo 26 verloopt als volgt, vermits j de negende letter is (als we starten vanaf 0) en t de negentiende letter krijgen we : $j+t = 9+19 = 28$. Rekenen modulo 26 wil zeggen dat we er x-aantal maal 26 mogen bij of aftellen totdat we in het gehele interval [0,25] terechtkomen. Hier geeft dit $28 - 26 = 2 = c$. Wat maakt dat de encryptie van het woord `programma` met deze techniek het woord `cvnkeelqn` oplevert.

Deze stappen kunnen ook omgedraaid worden om het woord te decoderen :

stap 2 omgedraaid Trek de sleutel af

	c	v	n	k	e	e	l	q	n
-	j	a	v	a	j	a	v	a	j
	t	v	s	k	v	e	q	q	e

stap 1 omgedraaid tel $N = 4$ stappen terug en je krijgt opnieuw het woord `programma`

3.1 Keuzemenu

Om deze functionaliteit van coderen en decoderen eenvoudig te kunnen aanbieden zal je volgend keuzemenu implementeren :

```
Welkom bij CRYPTOTechniekXX
Wat wil je doen? Je kan :
1. Coderen
2. Decoderen
3. Dit programma verlaten
```

Optie 3 is duidelijk, de andere opties worden verder besproken in de volgende secties.

3.2 Versleutelen

Wanneer gekozen wordt voor optie 1, zal je de gebruiker vragen een woord of zin in te geven. Let wel, elk woord wordt met kleine letters ingegeven.
Voor techniek 1 wordt dit bijvoorbeeld :

```
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
Welkom bij CRYPTOTechniek1
Wat wil je doen? Je kan :
        1. Coderen
        2. Decoderen
        3. Stoppen
Geef je keuze: (1/2/3) :
1

Geef de tekst die je wil omzetten, gebruik alleen kleine letters :

program
Omgezet geeft dit:
aRBEIDsonGeSCHiktHEiDsveRzekeriNGen

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
Welkom bij CRYPTOTechniek1
Wat wil je doen? Je kan :
        1. Coderen
        2. Decoderen
        3. Stoppen
Geef je keuze: (1/2/3) :
3

tot de volgende keer
```

Tip : Bij deze techniek zal je zelf woorden moeten verzinnen waarvan de lengte een meervoud van 5 is, om de codering te voltooien. Je kan bestaande woorden als constante klaarzetten, bijvoorbeeld :

```
final String WOORD5  = "wodka";
final String WOORD10 = "dekmantels";
```

```
final String WOORD15 = "aandelenfondsen";
final String WOORD20 = "communicatieadviseur";
final String WOORD25 = "voetbalscheidsrechtertjes";
final String WOORD30 = "betrouwbaarheidsintervalletjes";
final String WOORD35 = "arbeidsongeschiktheidsverzekeringen";
final String WOORD40 = "geeninspiratiemeertotaandeveertigletters";
```

Tip: Het omzetten naar een binaire codering kan met behulp van het omzetten naar een bitstring. Het is niet de bedoeling dat je al arrays gebruikt.

Wanneer je techniek 2 implementeert ziet je console scherm er als volgt uit :

```
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
Welkom bij CRYPTOTechniek2
Wat wil je doen? Je kan :
        1. Coderen
        2. Decoderen
        3. Stoppen
Geef je keuze: (1/2/3) :
1

Geef de tekst die je wil omzetten, gebruik alleen kleine letters :

programma
Omgezet geeft dit:
cvnkeelqn
```

3.3 Ontcijferen

In optie 2, is het de bedoeling dat het versleutelde woord of de versleutelde zin die gegenereerd werd door optie 1 opnieuw omgezet kan worden in zijn oorspronkelijke vorm. Voor techniek1 geeft dit dus :

```
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
Welkom bij CRYPTOTechniek1
Wat wil je doen? Je kan :
        1. Coderen
        2. Decoderen
        3. Stoppen
Geef je keuze: (1/2/3) :
2

Geef het gedecodeerde woord:

aRBEIDsonGeSCHiktHEiDsveRzekeriNGen
Omgezet geeft dit:
program
```

Voor techniek 2 wordt dit :

```
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
Welkom bij CRYPTOTechniek2
Wat wil je doen? Je kan :
        1. Coderen
        2. Decoderen
        3. Stoppen
Geef je keuze: (1/2/3) :
2

Geef het gedecodeerde woord:

cvnkeelqn
Omgezet geeft dit:
programma

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
Welkom bij CRYPTOTechniek2
Wat wil je doen? Je kan :
        1. Coderen
        2. Decoderen
        3. Stoppen
Geef je keuze: (1/2/3) :
3

tot de volgende keer
```

4 Quotering

- `Structuur (8pt)`
  - opdeling in methodes (parameters en returntypes)
  - gebruik variabelen en hun types
  - control flow van het programma (startmethode)
  - gebruik keuze en lusstructuren
  - correct gebruik van constanten
- `Functionaliteit (9pt)`
  - codering (woord / zin van woorden)
  - decodering (woord / zin van woorden)
  - werken met een menu / terugkeren naar een menu

  - robuustheid van de input

- `Stijl (2pt)`
- `Documentatie en Commentaar (1pt)`

Veel codeerplezier en succes !!