平成 19 年度 基礎プログラミング II / 情報表現 試験問題

試験日時: 2008 年 1 月 30 日 (水) 5 時限
出題者: 神田・西村・広瀬
持ち込み: 教科書、参考書、ノート、電卓可、PC 不可。携帯電話鳴動は即退場。
解答は解答用紙の所定の欄に書くこと。問題用紙は持ち帰ってよし。

学生証を机の上通路側におくこと

第 1 問 以下の式を計算せよ。解答は 16 進数で示せ。なお、先頭に付加してある $0x$ は 16 進数を、$0b$ は 2 進数をあらわしているものとする。何もついていない数は 10 進数である。

(1) $998 + 8580$　(2) $0x77 + 0x25$　(3) $0b11000 \times 0b10011$

第 2 問 時間、分、秒 を表す 3 つの引数をそれぞれ h, m, s として受け取り、秒に換算した値を返すメソッド seconds を定義せよ。メソッドの最初と最後の各 1 行は

```
def seconds(h, m, s)
end
```

とする。

第 3 問 秒を表す 1 つの引数を s として受け取り、それを時・分・秒に換算した文字列を出力するメソッド hms を定義せよ。たとえば、

```
hms(3700)
```

とすると、

1 時間 1 分 40 秒

と出力される。

第 4 問 次のような Hash が定義されている。

```
animal = {"ネズミ" => "ウシ", "トラ" => "ウサギ", "トカゲ"=> "ヘビ", "サル" => "ニワトリ", "イヌ" => "イノシシ"}
```

(1) "ウサギ" を得るにはどのような実行文が必要か。

(2) "イノシシ" を key にし、value として "ネズミ" を得る Hash の対を追加したい。上の行に続いて実行文を記すことによって Hash 対を追加するとき、その実行文を記せ。

(3) 前問の実行文に続けて以下のような実行文を付け加えた。実行結果を書き出し、理由を付して答えよ。

```
for prev in animal.keys.sort
   printf("%s の次は %s ですね\n",
       prev, animal[prev])
end
```

第 5 問 子どもには親が 2 人いる。その親も親が 2 人いる。1 世代遡るごとに、その子どもを作った祖先の数が 2 ずつ増加する。

(1) 世代を引数 n とし、n 世代前の祖先の数を求めるメソッド ances を作成せよ。

(2) ances(5) の実行結果と、そこに至る過程を解説せよ。

第 6 問 決められた法則に基づいてデータを変換することを「暗号化」、暗号化されたデータ からもとのデータを取り出すことを「復号」という。以下のルールで整数の暗号化、復号を行うプログラム DES.rb について質問に答えなさい。

［ルール］

- もとのデータを x、キーを y、変換後のデータを z とした場合、暗号化は $z = x + y$, 復号は $x = z - y$ となる
- 例えば、もとのデータ が 100、キーが 150 の場合、変換後のデータは 250 となり（暗号化）、変換後のデータが 5000、キーが 1200 の場合、もとのデータは 3800 となる（復号）
- プログラム実行時にモード、キーを引数として与える。ここでモードは「-e」と「-d」の 2 種類であり、「-e」を与えた場合は暗号化、「-d」を与えた場合は復号を行う。キーは任意の整数とする
- つまり Kterm より実行する際に、% ./DES.rb -e 1234 というように 2 つの引数を与えて実行する

［DES.rb］

```
#!/usr/koeki/bin/ruby
if [ア]
   print "モードとキーを引数に与えて実行してください\n"
   print "モードは -e で暗号化、-d で復号になります\n"
   print "キー　1000　で暗号化をする場合 ./DES.rb -e 1000 になります\n"
   [イ]
end

if ARGV[0] == "-e"
   print "もとの数字を入力してください："
   number = [ウ]
   number += [エ]
else
   print "変換後の数字を入力してください："
   number = [ウ]
   number -= [エ]
end

printf("結果：%d\n",number)
```

(1) ア ～ エの空欄を埋めよ。引数を誤って指定した場合に、望ましくない結果がでないよう配慮すること。

(2) A さんがこのプログラムを用いてもとのデータを暗号化し、遠隔地の B さんに変換結果を電子メールで送信すると仮定した場合、どのようなセキュリティ上の問題点があると考えられるか。なおキーは A さんが独自に定めるものとする。

— 以上 —