Matura iz informatike

Spomladanski rok 2013

POLA 1, NALOGA 2

Napišite štiri jezike za izražanje znanja.

1. _____
2. _____
3. _____
4. _____

Rešitev: pogovorni jezik, likovni jezik, jezik zvokov, jezik gibov

Naloga sledi učbeniku in je premalo določena, zato so pravilni tudi drugi odgovori, npr. slovenski jezik, angleški jezik , programski jezik, C/C++, Python, Java, itd.

ACM skupina:

- *AL. Algorithms and Complexity (AL/AutomataTheory) – Algoritmi in zahtevnost*
- PL. Programming Languages (PL/BasicLanguageTranslation) – Programski jeziki

Razlaga:

Naloga govori o jezikih za izražanje znanja. Vsi jeziki omogočajo prenašanje vsebine oz. znanja, vendar v svojem bistvu omogočajo dvoumnost.

V računalništvu in informatiki želimo uporabljati jezike, ki so nedvoumni. V ta namen definiramo t.i. formalne jezike, ki omogočajo nedvoumen in natančen popis vsebine oz. znanja ali problema. Za razpoznavo sporočil zapisanih v teh jezikih uporabljamo avtomate – zato govorimo o področju teorije avtomatov in formalnih jezikov.

V IKT so formalni jeziki prisotni na vsakem koraku: programski jeziki, jeziki za prenos podatkov (XML, JSON, …), komunikacijski protokoli, itd. Primeri razpoznavalnikov (*parser*) pa so: prevajalniki in tolmači, brskalnik, TCP/IP sklad, itd.

Matura iz informatike

Spomladanski rok 2013

POLA 2, NALOGA 3

Jure je napisal svojo prvo spletno stran. Želi, da je vidna na spletu, zato jo bo prenesel na spletni strežnik z operacijskim sistemom Linux.

V tabelo zapišite napake, poleg napak pa pravilen zapis.

<HTML><HEAD><TITLE> Moja spletna stran </TITLE>

<BODY></HEAD>

<H1><I> Pozdravljeni! </I></H2>

<FONT SIZE="4" COLOR="#FF">

<IMG SRC="c:/moje_slike/tulipan.jpg">

<I><U> To je moje besedilo!</U></I></P>

</BODY>

</HTML>

(10 točk)

Napaka	Pravilen zapis

Rešitev:

Napaka	Pravilen zapis
<BODY></HEAD>	</HEAD><BODY>
</H2>	</H1>

Matura iz informatike

Spomladanski rok 2013

Ni značke <P>	dodan <P> ali izbris </P>
"c:/moje_slike/tulipan.jpg"	"moje_slike/tulipan.jpg"
color="#FF"	color="#FF0000"

ACM skupina:

NC. Net Centric Computing (NC/WebOrganisation) – Omrežno računalništvo

Razlaga:

Naloga zahteva poznavanje strukture zapisa v jeziku HTML.

Pri definiranju jezika HTML bi lahko načrtovalci sestavili poljubno zahtevno slovnico. Odločili so se za kar se da preprosto slovnico, ker je potem razpoznava besed iz takšnega jezika preprostejša in računsko manj zahtevna. V preprostejših besedah; beseda v jeziku HTML je vsaka spletna stran in brskalnik mora besedo razpoznati ter pravilno predstaviti – pokazati spletno stran. Tu postaja jasno, zakaj mora biti slovnica preprosta, saj bi sicer naš brskalnik predolgo preračunaval vsebino, predno bi jo prikazal.

Ena osnovnih odločitev je bila, da bo jezik HTML zasnovan na osnovi značk, ki jih odpiramo in zapiramo (prim. oklepaje), kot je bil pred tem zasnovan že jezik SGML. Tri od zgornjih napak izvirajo iz napačne rabe odpiranja in zapiranja značk. Ob tem moramo dodati, da so načrtovalci pri nekaterih značkah dovolili opuščanje zapiranja, čeprav je zaradi tega možna dvoumnost. Na primer: <P> nekaj <P> drugo </P>. Podobna dvoumnost nastopa v programskih jezikih: IF pogoj1 THEN IF pogoj2 THEN nekaj1 ELSE nekaj2 ENDIF, kjer ne vemo, kam sodi ELSE pri nekaj2. Poiščite načine razreševanja te dvoumnosti.

Četrta napaka izhaja iz dejstva, da je lokalni datotečni sistem pri različnih operacijskih sistemih različen – prim. *File system hierarchy*. Zadnja, peta napaka je ponovno plod jezika HTML, saj zahteva zapis barv v 24-bitni obliki ter je zapis FF dvoumen.

Matura iz informatike

Spomladanski rok 2013

POLA 1, NALOGA 12

Znak ☺ ima v kodni tabeli UNICODE kodo 263A(16). V HTML-ju lahko ta znak zapišemo z delcem oblike &#n; , kjer je n koda znaka zapisana v desetiškem sestavu. Določite število n.

Rešitev:

n = ((2*16+6)*16+3)*16+10

ACM skupina:

- AR. Architecture and organization (AR/DigitalLogicandDataRepresentation) – Arhitektura in organiziranost računalniških sistemov

Razlaga:

Naloga pričakuje poznavanje šestnajstiškega sestava in njegovega pretvarjanja desetiški sestav.

V IKT je vse zapisano v obliki ničel in enic, ki jih združujemo v večje skupine po štiri bite (nibl ali grižljaj) in po osem bitov (bajt ali zlog). Ker štirje biti lahko predstavljajo števila med 0 in 15 (vključno), se v RIN pogosto uporablja šestnajstiški sistem (heksadecimalni po grškem izrazu za šestnajst). Poleg šestnajstiškega sistema se pogosto uporabljata še razumljivo dvojiški in osmiški. Zato je poznavanje sistemov ter pretvarjanje vrednosti med njimi ena temeljnih spretnosti, ki jih moramo obvladati.

Po drugi strani naloga govori o črkovnih naborih. Na začetku so črkovni nabori bili sedem bitni, kjer se je osmi bit uporabljal za paritetno zaščito. Standard, ki govori o tem naboru je ISO 646. Omenjeni standard je že predvideval, da obstajajo nacionalni nabori in med njimi sta pri nas poznana predvsem dva ASCII (ISO 646–US) ter JUS (ISO 646–YU), v katerem se je na primer namesto ASCII znaka ~ pojavila črka č in podobno za ostale šumnike. Z razvojem tehnologije so uporabniki želeli hkrati uporabljati več črkovnih naborov abecednih pisav (latinska, grška, cirilice, arabska, ...) in prišla je družina standardov ISO 8859 ter za naše potrebe še posebej ISO 8859-2. Ta družina je odpravila paritetni osmi bit je uporabljala vseh osem bitov za kodiranje. Vzporedno se je razvijal standard, ki bi hkrati dovolil uporabo vseh črk vključno s kitajskimi pismenkami, indijskimi znaki in še kakšnimi posebnimi kot so puščice in podobno – govorimo o zapisu Unicode, ki je bil na začetku 16-biten. Unicode standard dejansko definira preslikavo med katerokoli 16-bitno številko in znakom (*glyph*) – seveda črke so samo posebni znaki.

In končno, zapis spletnih strani v html datotekah je običajno še vedno zgolj 8 biten, kar ne dovoljuje uporabe 16 bitnih kot znakov. Zato se je v HTML standardu uporablja zapis z ubežnim znakom (*escape character*), ki je & in zaključek zapisa z ;. Dejansko je UTF8 zapis podobno zapis z ubežnim znakom, le da je definiran na ravni vsebine datoteke in ne HTML standarda. Tehniko ubežnega znaka ali zaporedja (*sequence*) se v RIN zelo pogosto uporablja.

Primerjaj naprej: ubežno zaporedje, končni avtomat, kodiranje, Unicode.

Matura iz informatike

Spomladanski rok 2013

POLA 1, NALOGA 8

Obkrožite tri postopke, ki so namenjeni zgoščevanju zapisa videopodatkov.

A. Mpeg2
B. Mpeg4
C. ZIP
D. RAR
E. H.264
F. mp3

Reštev: A, B, E

Za pravilno (pričakovano) rešitev dobi kandidat 2 točki. Ker postopka ZIP in RAR služita zgoščevanju zapisa podatkov, dobi kandidat 1 točko, če je izbral katerokoli kombinacijo treh odgovorov, ki NE vsebuje odgovora F.

ACM skupina:

- GV. Graphics and Visual Computing (GV/FundamentalConcepts) – Grafika in vizualno računalništvo
- DS. Discrete Structures (DS/BasicsOfCounting) – Diskretne strukture
- *NC. Net Centric Computing (NC/MultimediaTechnologies) – Omrežno računalništvo*

Razlaga:

Digitalna pismenost predpostavlja, da dijak pozna različne zapise videopodatkov, nenazadnje, da si je sposoben kupiti ustrezen videopredvajalnik.

Zgoščevanje videopodatkov je specifično, ker njegova izgubnost sloni na omejeni sposobnosti človekovega zaznavanja. Druga posebnost je, da je video vedno kodiran kot zaporedje sličic v določenih časovnih intervalih in ker je sprememba kadra med dvema sličicama v velikem številu primerov majhna to omogoča posebne oblike stiskanja podatkov, ki pa so običajno celo brezizgubne. Tehnološko se obravnava video kot eden od medijev za prenos podatkov.

V svetu se je pojavila vrsta industrijskih standardov zapisa videopodatkov: MPEG2, MPEG4, MPEG7, DivX, … Velika večina standardov vključuje koncepte stiskanja kot so kosinusna transformacija, Huffmannovo kodiranje, RLE (Run Length Encoding).

Matura iz informatike

Spomladanski rok 2013

POLA 1, NALOGA 6

Janez je bolan in ima visoko vročino. Johnu je poslal v Ameriko sporočilo: »Sem bolan in imam vročino 40 stopinj.«

Napišite, ali je John razumel poslano sporočilo enako kot Janez in zakaj.

_____

_____

_____

Rešitev:

- Ne, ker temperaturo v Ameriki merijo v Fahrenheitovi lestvici.
- Da, ker John pozna Slovenijo in ve, da merimo temperaturo v Celzijevi lestvici.
- Ne, ker John ne razume slovensko.

ACM skupina:

- AR. Architecture and organization (AR/DigitalLogicandDataRepresentation) – Arhitektura in organiziranost računalniških sistemov
- NC. Net Centric Computing (NC/NetworkCommunication) – Omrežno računalništvo

Razlaga:

Dijake moramo naučiti pomena koncepta, v katerem je podan podatek.

S problematiko konceptov se v računalništvu in informatiki ukvarja področje umetne inteligence. Poleg tega ta naloga predpostavlja obliko zapisa podatka, ki je nedvoumna za pošiljatelja in prejemnika. Pošiljatelj in prejemnik predstavljata pri tem komunikacijski (entitetni) par, ki izmenjuje določene podatke.

Matura iz informatike

Spomladanski rok 2013

POLA 1, NALOGA 1

Slavko se je odločil, da si bo naredil poštni naslov in poštni nabiralnik pri ponudniku H-pošta. Za ustvarjanje naslova si je moral izmisliti tudi geslo. Ob tem je za nasvet povprašal prijatelja Alojza, ki mu je svetoval naslednje:

A. Gesla ne smeš nikomur zaupati.
B. V geslo ne smeš vključevati osebnih podatkov, imena svojih ljubljenčkov, prijateljev ali glasbenih skupin.
C. Geslo si zapiši v zvezek, da ga ne pozabiš.
D. Geslo naj ima vsaj osem znakov.

Kateri od nasvetov ni dober?

Rešitev: C

ACM skupina:

- DS. Discrete Structures (DS/DiscreteProbability) – Diskretne strukture
- OS. Operating Systems (OS/SecurityAndProtection) – Operacijski sistemi

Razlaga:

Gre za osnovna znanja oz. digitalno pismenost glede varnosti in zaščite uporabnika pri uporabi računalnika in/ali svetovnega spleta.

Naloga predstavlja problem kriptografije – čim boj naključno in daljše je geslo, težje ga je uganiti. Število kombinacij je velikost abecede $^{\text{št mest}}$.

Pri operacijskih sistemih mora biti uporabnik avtoriziran za dostop do posameznega vira, torej je pravica dostopa vezana na uporabnika. Za zagotavljanje identifikacije uporabnika uporabljamo različne postopke avtentikacije. Eden najbolj pogostih je uporabniško ime in geslo. Drugi primeri so: biometrična avtentikacija, skupna skrivnost, PKI (*public key infrastructure*) itd.

Obstajajo tudi avtentikacijski protokoli (LDAP, RADIUS, SHIBBOLETH, …). AAI je primer uporabe SHIBBOLETH protokola, ki črpa podatke iz LDAP.

Matura iz informatike

Spomladanski rok 2013

POLA 2, NALOGA 1

V elektronskih dokumentih uporabljamo namesto fizičnega podpisa digitalni podpis.

1.1 Kaj pomeni verodostojnost podpisane listine?

_____

_____

1.2 Digitalni podpis določata _____ in _____ ključ.

1.3 Kako deluje digitalno podpisovanje?

_____

_____

_____

_____

1.4 Ali je digitalni podpis enakovreden lastnoročnemu podpisu? Pojasnite svoj odgovor.

_____

_____

Rešitev:

1.1 Verodostojnost podpisane listine zagotavlja, da je taka, kot smo jo podpisali, in da smo se strinjali z njeno vsebino. *(Podpis 1 točka, strinjanje 1 točka)*

1.2 Javni, zasebni

1.3 Avtor izračuna izvleček sporočila, ki ga podpiše s svojim zasebnim ključem (izvleček šifrira). Prejemnik izračuna izvleček sporočila in ga primerja z odšifriranim izvlečkom avtorja. Odšifrira ga z avtorjevim javnim ključem. *(Upoštevajo se tudi drugačni pravilni odgovori; opis podpisovanja 2 točki, opis preverjanja 2 točki)*

1.4 Da. Slovenska zakonodaja enači oba podpisa. *(Upoštevajo se tudi drugačni pravilni odgovori; odgovor 1 točka, pravilna razlaga 1 točka)*

Matura iz informatike

Spomladanski rok 2013

ACM skupina:

- NC. Net Centric Computing (NC/NetworkSecurity) – Omrežno računalništvo
- *AL. Algorithms and Complexity (AL/CryptographicAlgorithms) – Algoritmi in zahtevnost*
- DS. Discrete Structures – Diskretne strukture

Razlaga:

Naloga zahteva poznavanje omrežne varnosti, digitalnega podpisovanja ter osnov kriptografije in kriptografskih algoritmov.

Osnovna matematična koncepta, ki ju srečamo v tej nalogi sta: javno-zasebni par ključev in kriptografska razpršilna funkcija. Pri javno-zasebnem paru ključev gre za preprost postopek uporabe primerne funkcije (npr. RSA, eliptične krivulje ipd.), ki ima dva parametra: podatke (dejansko neka zelooooo velika številka), ki jih želimo zakriptirati; in parameter (ponovno samo število), s pomočjo katerega izvedemo kriptiranje. Iz zornega kota uporabe, je funkcija samo matematična funkcija z dvema parametroma.

Drugemu parametru rečemo tudi ključ. Pri asimetričnih ključih velja, da lahko podatke, ki smo jih zakriptirali z enim ključem, z drugim ključem, ki je različen od prvega, odkriptiramo. Pri tem velja, da če nekdo pozna prvi ključe zelooooo težko naračuna drugi ključ. Matematično gledano sta oba ključa enaka, le kako ravnamo z njimi jima da svoje ime: javni in zasebni ključ. Posledica vsega povedanega je, da praktično nekaj, kar je zakriptiranega z zasebnim ključem lahko odkriptiramo samo z javnim ključem; ali drugače, če smo nekaj odkriptirali z javnim ključem je **moralo biti zakriptirano** z zasebnim ključem. Slednje dejstvo se uporablja pri postopku podpisovanja dokumentov, kot ga opisuje naloga.

Za zagotovitev verodostojnosti listine bi bilo torej dovolj, da bi s svojim zasebnim ključem zakriptirali listino in bi lahko vsakdo preveril, da smo jo res mi zakriptirali tako, da bi uporabil naš javni ključ (glej poudarjeno besedilo zgoraj). Če bi nepridiprav sedaj nekaj popravljal v dokumentu, ga ne bi mogel zakriptirati nazaj, saj ne pozna našega zasebnega ključa.

Celotno rokovanje z dokumentom je malce nerodno. Namreč naša želja ni skrivati vsebine in tako nekdo, ki bi rad prebral dokument, mora najprej dokument odkriptirati ter ga lahko šele nato prebere. V stvarnem (papirnem svetu) to rešujemo na dva načina: če dokument sestoji iz večih listov, jih povežemo z vrvico, ki jo zapečatimo ter lahko vsakdo vidi, če je pečat zlomljen in morda dokument potvorjen; ali številčimo strani tako, da napišemo vedno poleg številke strani še število vseh strani **in** vsak list podpišemo (zakaj oboje?). V digitalnem svetu se zatečemo h kriptografskim razpršilnim funkcijam (MD5, SHA1, SHA256, ...).

Slednje iz dokumenta naračunajo krajši podatek (število), ki mu rečemo izvleček, pri čemer velja, da je težkoooo naračunati drug dokument, ki bi imel isti izvleček; da vsak popravek dokumenta spremeni izvleček in še nekaj lastnosti. Sedaj namesto celotnega dokumenta podpišemo (zakriptiramo s svojim zasebnim ključem) samo izvleček. Če nekdo želi preveriti verodostojnost

dokumenta, mora: i.) sam naračunati izvleček; ii.) odkriptirati zakriptirani izvleček z našim javnim ključem; in iii.) preveriti, če se oba izvlečka ujemata.

V celotnem postopku je še nekaj podrobnosti, a ena najpomembnejših je, da moramo mi verjeti, da je javni ključ v koraku ii.) v resnici javni ključ podpisovalca. Slednje preverimo tako, da o tem povprašamo nekoga, komur zaupamo. Tehnično to pomeni, da neka institucija potrdi (certificira), da je nek ključ (dejansko neko število) res javni ključ neke osebe. To potrdi tako, da napiše dokument (certifikat, glej standard X500), v katerem potrjuje dejstvo in ga podpiše s svojim zasebnim ključem (opis podpisovanja je identičen zgornjemu). Kot uporabnik moramo sedaj poznati javni ključ potrjevalske agencije – ustvari se veriga zaupanja.

Tehnično gledano, javni ključ agencije (npr. SI-CERT) ročno vnesemo v naš računalnik.

Matura iz informatike

Spomladanski rok 2013

POLA 1, NALOGA 18

Spodaj je zapisano zaporedje ukazov v psevdokodi.

Kakšno vrednost imajo spremenljivke a, b, c in d po izvršitvi navedenega zaporedja ukazov?

```
a ← 1
b ← 2
c ← b
d ← 1
b ← a
a ← c
d ← a + b + c + d
```

Rešitev:

Korak/spremenljivka	a	b	c	d
1. korak	1			
2. korak		2		
3. korak			2	
4. korak				1
5. korak		1		
6. korak	2			
7. korak				6
Vrednosti spremenljivk na koncu	2	1	2	6

a = 2

b = 1

c = 2

d = 6

ACM skupina:

- PF. Programming Fundamentals - Osnove programiranja.

Razlaga:

Pojem spremenljivke in z njim povezana principa branja vrednosti spremenljivke in prireditve vrednosti spremenljivke. Vse spremenljivke v tej nalogi so neposredno naslovljive. Obstajajo tudi posredno naslovljive spremenljivke preko koncepta reference, ki je v različnih programskih jezikih različno implementiran. Pri predmetno naravnanih programskih jezikih je zanimivo, da so vse spremenljivke, ki se nanašajo na predmete, posredne.

Matura iz informatike

Spomladanski rok 2013

POLA 2, NALOGA 6

V preglednici imamo podatke o reševanju testa in podatke o statistični obdelavi testa.

	A	B	C	D	E	F	G	H	I
1	**Ime in Priimek**	**Št. točk**	**Ocena**		**Ocena**	**oznaka**	**št.ocen**	**Delež v %**	
2	Janez Novak	55	2		negativno	1			
3	Miha Božič	89	5		zadostno	2			
4	Ana Kovač	72	3		dobro	3			
5	Jana Nagode	91	5		prav dobro	4			
6	Bine Horvat	68	3		odlično	5			
7	Ana Lampe	80	4		**skupaj**				
8	Simon Koren	74	3						
9	Tone Hočevar	81	4						
10	**Povprečje**								
11									
12									

6.1. Izračunajte povprečno število točk v testu in povprečno oceno tega testa. Zapišite ustrezno funkcijo v celici B10, tako da jo lahko kopirate tudi v celico C10 in bo delovalo pravilno.

Rešitev:

AVERAGE(B2:B9)

6.2. Izračunajte število posameznih ocen v testu. Zapišite izraz v celici G2, tako da jo lahko kopirate še v celice G3 do G6 in bo delovalo pravilno. Uporabite funkcijo COUNTIF (COUNTIF(območje; pogoj)), ki vam v izbranem območju prešteje celice, ustrezne pogoju.

Rešitev:

COUNTIF($C$2: $C$9;F2)

6.3. V celici G7 zapišite funkcijo, ki izračuna število vseh ocen testa.

Rešitev:

SUM(G2:G6)

6.4. Izračunajte deleže ocen. Zapišite izraz v celico H2 tako, da jo lahko kopirate v celice od H3 do H6 in bo delovalo pravilno.

Matura iz informatike

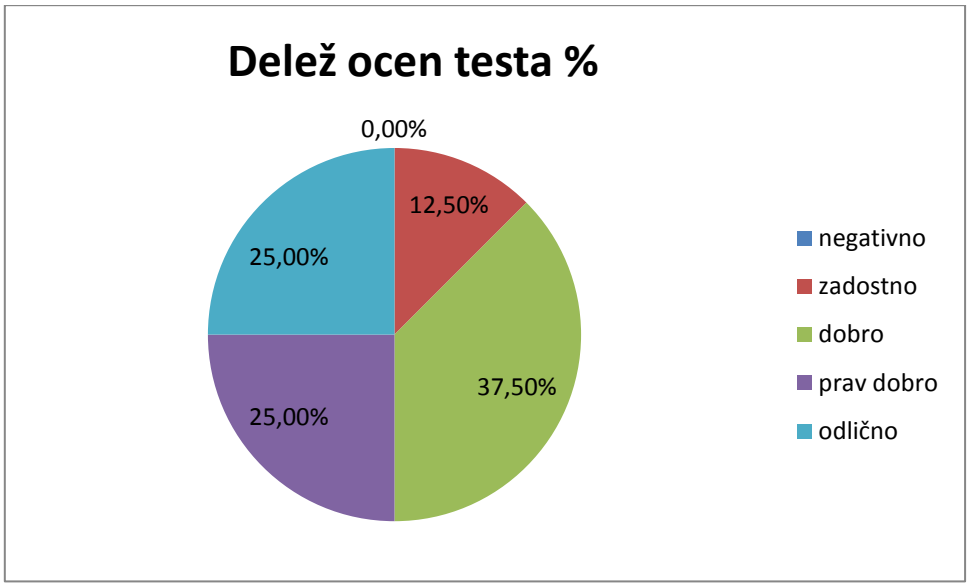
Spomladanski rok 2013

Rešitev:

=G2/$G$7

6.5. Skicirajte grafikon, ki predstavlja deleže posameznih ocen. Grafikon opremite z vsemi potrebnimi podatki.

Rešitev:



ACM skupina:

- *AL. Algorithms and Complexity – Algoritmi in zahtevnost*
- PF. Programming Fundamentals – Osnove programiranja

Razlaga:

Naloga zahteva poznavanje razlikovanja med absolutnim in relativnim naslavljanjem ter uporabo le-tega. Poleg tega pričakuje razumevanje in uporabo pojma funkcija, argument, pogoj, naslovi prostor. Kar je zanimivo pri tej nalogi je to, da je to naloga iz programiranja in ne toliko iz uporabe preglednic. Namreč koncept posrednega in absolutnega naslova spremenljivke je eno temeljnih orodij pri programiranju.

Zanimiva je tudi funkcija COUNTIF, ki ima dva parametra: območje, na katerem se izvede štetje; in pogojno funkcijo, ki se odloča za vsak element območja posebej, ali se naj upošteva pri štetju ali ne.

Matura iz informatike

Spomladanski rok 2013

Opis območja v programskih jezikih ne predstavlja posebnosti, je pa prenos funkcije kot spremenljivke izredno močno orodje. Naj ga pojasnimo na primeru.

Recimo, da imamo funkcijo ODŠTEJ(int x, y), ki od x odšteje y in vrne rezultat. Ko pokličemo funkcijo na primer ODŠTEJ(3, 2), se spremenljivki x priredi vrednost 3 in spremenljivki vrednost 2 ter se opravi preostanek izračuna. V primeru funkcije COUNTIF(območje, pogoj) pa se spremenljivki pogoj priredi vrednost, ki je funkcija. To ima dolgoročne posledice, saj sedaj lahko sedaj spremenljivki vedno priredimo vrednost funkcije in predvsem funkcija kot rezultat lahko vrne novo funkcijo – zato govorimo o funkcijah višjega reda.

Pri sodobnih jezikih, ki zahtevajo ujemanje tipov pri prirejanju vrednosti spremenljivk (typing), slednje zahteva, da tudi definiramo tip spremenljivke, ki je lahko funkcija. Ta je definiran kot n-terica (p1, p2, p3, ..., pn-1, r), kjer so pi tipi parametrov funkcije in r tip rezultata funkcije. Sedaj lahko prirejamo vrednosti samo v primeru, ko se funkcija, ki je prirejena spremenljivki, ujema s spremenljivko.

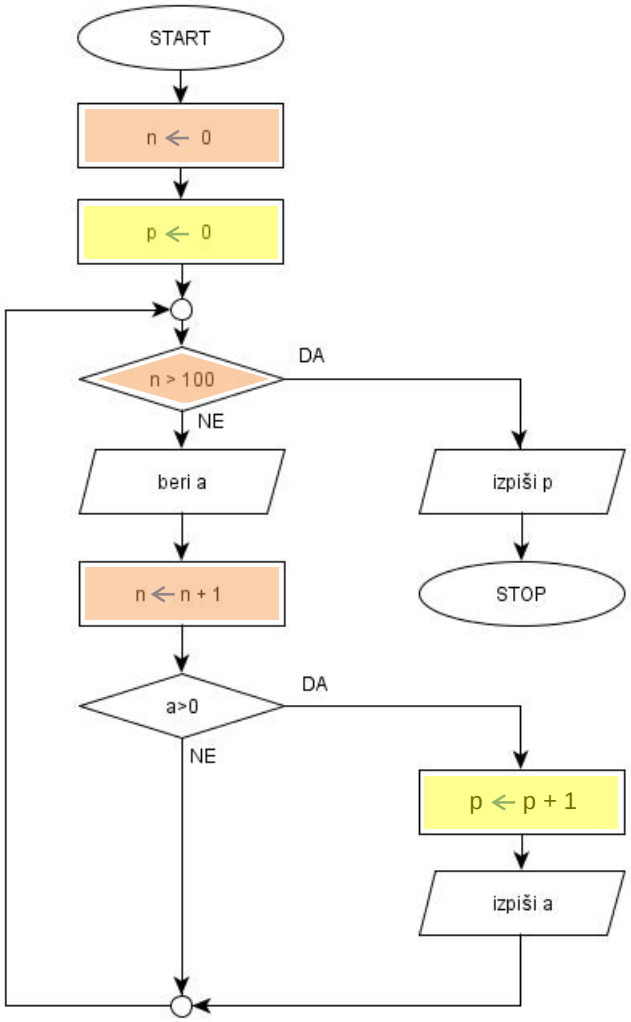
Matura iz informatike

Spomladanski rok 2013

POLA 2, NALOGA 4

Sestavite diagram poteka za postopek, ki omogoča vnos 100 številskih podatkov.
Med vnosom izpiše vsa pozitivna števila.
Na koncu izpiše še število izpisanih števil.

Rešitev:



ACM skupina:

- PF. Programming Fundamentals(PF/FundamentalProgrammingConcepts) – Osnove programiranja

Matura iz informatike

Spomladanski rok 2013

Razlaga:

Naloga zahteva implementacijo naslednjih osnovnih programskih konceptov:

- 100 kratno izvajanje zanke: za slednjo potrebujemo najprej spremenljivko, v kateri beležimo, kolikokrat se je zanka že izvedla. V naši rešitvi ima spremenljivka ime n. Spremenljivko na začetku nastavimo na vrednost 0, ker se ni zanka še nikoli izvedla in ob vsakem izvajanju zanke jo povečamo za 1 – pozor!! n šele po povečanju predstavlja število ponovitev zanke. Preverjanje ali smo zanko že dovoljkrat izvedli opravi pogojna vejitev n >= 100. Ob tem bi želeli poudariti, da bi semantično pravilen bil pogoj ali je n = 100, kar pomeni, da se je zanka stotič izvedla. Vendar je razširjeno preverjanje >= običajno.
- Štetje in izpisovanje pozitivnih prebranih števil ter na koncu izpis njihovega skupnega števila: to nalogo razdelimo na dva dela: štetje pozitivnih števil in oba končna izpisa. Za štetje števil ponovno potrebujemo spremenljivko (podobno kot za štetje ponovitev zanke), ki jo imenujemo v rešitvi p ter jo na začetku nastavimo na 0 – saj nismo prebrali še nobenega pozitivnega števila. Pri branju števil, ki jih beremo v spremenljivko a, sproti preverjamo, če je število pozitivno ter, če je, povečamo števec pozitivnih števil p za 1. Kot zahteva naloga, najdeno pozitivno število tudi izpišemo ter ob zaključku izpišemo število najdenih pozitivnih števil.

Preprosta razširitev: izpiši število ne pozitivnih števil. Malce bolj zapletena razširitev: izpiši spektrum števil: število števil med 1 in 100, med 101 in 200, ... do 1000.

Matura iz informatike

Spomladanski rok 2013

POLA 1, NALOGA 3

Uredite navedene pomnilne enote po hitrosti dostopa do podatkov od najpočasnejše do najhitrejše.

A. CD ROM
B. Ključ USB
C. Pomnilnik RAM
D. Zunanji disk USB
E. Disketa
F. Trdi disk

Rešitev:

- 1E, 2A, 3D, 4F, 5B, 6C ali
- 1E, 2A, 3B, 4D, 5B, 6C

ACM skupina:

- AR. Architecture and organization (AR/ComputerArchitectureandOrganization) – Arhitektura in organiziranost računalniških sistemov

Razlaga:

Dijaki naj poznajo lastnosti različnih pomnilnih enot.

Naloga sodi v področje Arhitekture in organiziranosti računalniških sistemov, saj zahteva poznavanje arhitekture oz. zgradbe računalniškega sistema s poudarkom na poznavanju notranjih/zunanjih pomnilnih enot. Pri tem je treba natančno prebrati nalogo, saj dostop do podatkov na pomnilniškem mediju sestoji iz dveh korakov: dostop do lokacije, kjer se nahajajo podatki na mediju in prenos podatkov v glavni pomnilnik. V tem se rešitvi razlikujeta, saj ena ne upošteva časa dostopa do podatkov.

Razvoj tehnologije na področju pomnilniških medijev je skokovit. Pri tem je potrebno slediti tudi dosežkom na področju znanosti o materialih, ki omogočajo nove pomnilniške medije.

Matura iz informatike

Spomladanski rok 2013

POLA 1, NALOGA 10

Za dane datoteke napišite ustrezno zvrst MIME. (Izbirajte med text, image, sound, video, application, model)

Ime datoteke	Zvrst MIME
Avto.jpg	
Avto.mid	
Avto.wav	
Avto.html	
Avto.exe	

Rešitev:

Ime datoteke	Zvrst MIME
Avto.jpg	Image
Avto.mid	Sound
Avto.wav	Sound
Avto.html	Text
Avto.exe	Application

ACM skupina:

- NC. Net-Centric Computing (NC/NetworkedAplication) – Omrežno računalništvo

Razlaga:

Poznavanje različnih vrst vsebin in njihovih končnic datotek sodi k digitalni pismenosti.

Čeprav vsebina datoteke sestoji iz ničel in enic, jih mora znati računalnik, oziroma točneje operacijski sistem ter ostali programi, ki se izvajajo na računalniku, pravilno interpretirati. Stroka je sprejela vrsto standardov za enolično interpretacijo. Eden od njih je standard MIME, ki ga opredeljuje standard RFC 2047. Kratica MIME pomeni *Multipurpose Internet Mail Extensions*, kar pomeni večnamenska Internetna razširitev poštnega protokola. Slednji je definiran v standardu RFC 821 in pozna kot vsebino samo običajno besedilo v ASCII obliki. S standardom MIME lahko po e-pošti pošiljamo poljubno vsebino in jo poštni program razpozna. Standard MIME so kasneje prevzeli tudi drugi protokoli in najbolj poznan je protokol HTTP. Za razliko od standarda MIME končnice datotek niso določene v standardu glede na vsebino datotek, ampak dogovorno.

Matura iz informatike

Spomladanski rok 2013

POLA 1, NALOGA 7

Napišite vsaj pet elementov komuniciranja.

_____

_____

_____

_____

Rešitev: oddajnik, prejemnik, komunikacijski kanal, motnje, povratna zveza, sporočilo

Če kandidat navede pet izmed zgornjih elementov, dobi 2 točki. Če navede vsaj oddajnik, prejemnik in komunikacijski kanal, dobi 1 točko.

ACM skupina:

- NC. Net Centric Computing (NC/NetworkCommunication) – Omrežno računalništvo

Razlaga:

Dijaki se morajo zavedati elementov, ki nastopajo v vsaki komunikaciji.

V računalniških komunikacijah sta osnovna gradnika komunikacije komunikacijski (entitetni) par in jezik, v katerem komunicirata. Sama komunikacija poteka po komunikacijskem kanalu, v katerem si komunikacijski par izmenjuje sporočila v svojem jeziku. Pri tem lahko pride do napak, motenj in podobnih pojavov, ki jih zaznava in morda (odvisno od definicije) odpravlja komunikacijski protokol. Vloga protokola je, da po eni strani podpira izmenjavo sporočil v jeziku komunikacijskega para in po drugi strani zagotavlja storitve prenosa sporočil.

V IKT poznamo vrsto protokolov za izmenjavo sporočil: IP, TCP, UDP, IPsec, PPP in še kopica drugih.

Matura iz informatike

Spomladanski rok 2013

POLA 1, NALOGA 15

Naštejte tri prednosti elektronske pošte pred klasično pošto (pismo ali paket).

a) _____
b) _____
c) _____

Rešitev:

a) Cena
b) Hitrost
c) Preprosta priprava množičnih sporočil
d) Naslov ni vezan na določen kraj

ACM skupina:

- *SP. Social and Professional Issues - Družbena in poklicna vprašanja*
- *HCI. Human-Computer Interaction - Vmesnik človek-računalnik*

Razlaga:

Dijak mora ne samo poznati tehnologijo, ampak poznati tudi njene prednosti in pomanjkljivosti, da se lahko zavestno odloča.

Za poznavanje prednosti ali slabosti je potrebno poznati ne samo tehnologijo, ampak principe, ki so temelj implementacije v tehnologiji. Princip, ki je uporabljen v sodobnih e-poštnih sistemih je identičen principu, ki ga je stoletja uporabljala navadna pošta. Najprej imamo uporabnika, ki želi poslati pošto, potem imamo nek sistem prepošiljanja pošte ter na koncu drugega uporabnika, kateremu je pošta namenjena. Nekje vmes je še oblika sporočila, ki ga celoten sistem zna pošiljati in razumeti – prim. komunikacijski elementi.

Če se najprej pomudimo pri sporočilu, le-tega definira RFC 821 in sicer kot ovojnico, glavo in telo sporočila. Slednje je lahko zgolj ASCII ter šele standard MIME kasneje dovoli razširitev na drugačne vsebine. Glava sestoji iz vrstic (zapisov), ki opisujejo pošiljatelja, prejemnika, zadevo, datum ter predvsem enolični identifikator poslane pošte. Ovojnico uporablja samo sistem za prepošiljanje sporočil.

Prenašanje sporočil se izvaja po protokolu SMTP (RFC 821) in njegovimi kasnejšimi razširitvami, ki predvsem nudijo višjo stopnjo varnosti (SSL plast, avtentikacija vmesnih strežnikov in podobno). Uporabnik, pošto pošilja s pomočjo nekega programa, ki je lahko spletna aplikacija (npr. gmail) ali odjemalec na njegovem računalniku (npr. thunderbird), ki preda pošto agentu za prenos pošte (*MTA,*

Mail Transfer Agent). Slednji s pomočjo protokola SMTP preda sporočilo v sistem, da se prenese do naslovnika. Naslovnik mora za prejem pošte imeti svoj nabiralnik, podobno kot pri klasični pošti. Primer ponudnika nabiralnikov je ARNES. Sedaj mora prejemnik prebrati pošto in slednje lahko naredi ponovno preko spletnega vmesnika ali s pomočjo namenskega programa kot je na primer thunderbird. Slednji se pogovarja z nabiralnikom s pomočjo protokola kot sta pogosto IMAP ali POP, lahko pa tudi MAPI. Vsak od teh protokolov lahko uporabi SSL plast za zaščito prenosa ter dobimo IMAPS, POPS ter MAPIS. Omeniti moramo še to, da tudi spletni vmesnik uporablja običajno za dostop do nabiralnika omenjene protokole.

Matura iz informatike

Spomladanski rok 2013

POLA 1, NALOGA 24

Različne naprave uporabljajo različne barvne modele.

24.1. Zapišite, pri kateri napravi se uporablja barvni model RGB.

Rešitev:
Barvni model RGB se uporablja pri prikazovanju barv na zaslonu.,

Kaj pomeni kratica RGB?

Rešitev:
Red – rdeča, Green – zelena, Blue - modra

Kakšen zapis ima v tem modelu barva magenta (vijolična)?

Rešitev:
FF 00 FF

24.2. Zapišite, pri kateri napravi se uporablja barvni model CMYK.

Rešitev:
Barvni model CMYK se uporablja pri tiskalniku.

Kaj pomeni kratica CMYK?

Rešitev:
Cian, Magenta , Yellow – rumena, blacK - črna

Katera barva ima v tem modelu zapis 00 00 FF 00?

Rešitev:
rumena

ACM skupina:

GV. Graphics and Visual Computing - Grafično in vizualno.

Matura iz informatike

Spomladanski rok 2013

Razlaga:

Preverja razumevanje zapisa barve v računalniku in poznavanje barvnih modelov.

Pri delu s slikovnim gradivom želimo opraviti različne operacije nad sliko. Pri tem vprašanju se predvsem osredotočamo na operacije nad barvami v slikovnem gradivu. Predstavitev RGB (Red, Green, Blue) je predstavitev, ki ima svoj izvor v tehnološkem ozadju predstavitve barv na zaslonu, kjer so starejši zasloni, ki so uporabljali katodne cevi, imeli tri vire svetlobe: rdečega, zelenega in modrega. S kombinacijo le-teh so na zaslonu pričarali barvno sliko.

Podobno je pri kodiranju barv CMYK (Cian, Magenta, Yellow, blacK) tehnološko ozadje v delovanju tiskalnikov, ki uporabljajo omenjene štiri barve za čaranje barvnih slik.

Poznamo še druge modele kodiranja barv, kot na primer HSV (Hue, Saturation, Value) in podobni. Le-ti so tako imenovani cilindrični modeli barvnega prostora. Poglejte možnost nastavitve teh vrednosti na domačem televizorju.

Med kodiranji obstajajo bijektivne preslikave.

Matura iz informatike

Spomladanski rok 2013

POLA 1, NALOGA 22

Za zapis slike v računalniku uporabljamo vektorski ali točkovni zapis.
22.1. Naštejte tri prednosti vektorskega zapisa pred točkovnim (bitnim) zapisom slike.

Rešitev:

1. Praviloma manjša velikost datoteke
2. Vsak element/predmet slike lahko oblikujemo samostojno
3. Pri spreminjanju velikosti se oblika elementov ne popači.

ACM skupina:

- GV. Graphics and Visual Computing - Grafično in vizualno računalništvo

Razlaga:

Preverja razumevanje temeljnih pojmov povezanih z vektorsko grafiko.

Osnovna razlika med obema zapisoma je, da eden (vektorski) se zaveda predmeta in njegovih lastnosti, kar pomeni, da lahko programska oprema rokuje s posameznim predmetom. Običajno je ena od lastnosti predmeta to, kako naj se natisne/izriše/.... Tako programska oprema, ki izrisuje predmet, le-tega vsakič posebej izriše glede na uporabnikove parametre. Na nek način vektorski zapis ni zapis slike, ampak zapis predmetov.

Po drugi strani imamo pri bitnem zapisu res samo bitni zapis slike. V njem ne obstajajo več predmeti in ker le-ti ne obstajajo, ne poznamo njihovih posamičnih lastnosti.

Matura iz informatike

Spomladanski rok 2013

POLA 1, NALOGA 25

Pri modeliranju podatkov poznamo različne podatkovne modele.

Določitev glavnih entitet, njihovih atributov in pomembnejših povezav je značilnost

____globalnega____ modela.

Opis konceptov obravnavanega problema je značilnost _____ konceptualnega_____ modela.

Enolično določeni zapisi vseh entitet, njihovih atributov in relacije so značilnost
____ logičnega _____ modela.

Model realnosti, izveden v računalniku, je značilnost _____ fizičnega_____

ACM skupina:

IM. Information Management - Upravljanje informacij.

Razlaga:

Preverja poznavanje pojmov in vrst podatkovnih modelov.

V informacijskih sistemih upravljamo s podatki, ki jih moramo seveda obvladovati. Pri tem smo postavljeni pred izziv, da sliko iz realnega sveta prenesemo v sliko, ki jo bo obvladovalo programje, ki ga načrtujemo. Pri razvoju informacijskih sistemov to naredimo v več urejenih korakih, katerih sosledje nam pomaga doseči cilj.

Najprej izvedemo tako imenovano funkcionalno analizo, katere rezultat je popis entitet in njihovih lastnosti (atributov), ki jih bo moral obravnavati naš informacijskih sistem. Slednje imenujemo globalni model. V naslednjem koraku definiramo odnose med entitetami oziroma njihovimi lastnostmi in dobimo konceptualni relacijsko-entitetni (R-E) model.

Konceptualni model je sicer načeloma matematično in posledično programsko obvladljiv, vendar ne upošteva osnovnih principov končnega modela, ki zagotavjajo učinkovito obvladovanje podatkov. Eden najobičajnejših konceptov, ki jih ne upošteva je enoličnost preslikave – imamo namreč lahko še vedno mnogo na mnogo preslikave. Zato se lotimo normalizacije modela in dobimo logični R-E model.

Različne izvedbe podatkovnih baz različno delujejo (MySQL, PostgreSQL, Oracle, DB, MicrosoftDB, ...) in zato v zadnjem koraku prilagodimo logični R-E model konkretni podatkovni bazi, ki jo bo za upravljanje podatkov uporabljal naš informacijskih sistem.

Matura iz informatike

Spomladanski rok 2013

POLA 1, NALOGA 21

Pri navajanju virov za različne vrste virov vključujemo različne podatke.
21.1. Katere podatke o knjigi vključimo v njen opis pri navajanju virov?

Rešitev:
1. ___avtor/avtorji_____
2. ___naslov_____
3. ___založba_____
4. ___leto izdaja_____
5. ___kraj izdaje_____

ACM skupina:

- IM. Information Management - Upravljanje informacij

Razlaga:

Preverja osnovna znanja za uporabo in navajanje virov. Je tudi vzgojna.
Odgovor na to vprašanje zahteva najprej razumevanje vloge navajanja virov. Vire navajamo iz dveh razlogov. Prvi je ta, da bralcu ponudimo možnost nadaljnjega branja o podrobnostih, ki jih ne navajamo v našem sestavku. Drugi razlog pa je, da moramo biti pravični do resničnega avtorja ter mu priznati njegove pravice ter se ne kititi s tujim perjem.
V obeh primerih mora biti vir naveden tako nedvoumno, da ga lahko bralec pridobi. V primeru knjige so elementi, ki nedvoumno določajo knjigo zapisani zgoraj. Za ostale enote (članki in podobno) so elementi drugačni in si jih lahko pogledate pri opisu programa BibTeX ali še kje drugje.
Zanimivo je navajanje spletnih virov. Pri slednjih moramo biti zelo pazljivi iz dveh razlogov. Najprej so običajno ti viri nepreverjeni, saj jih lahko takorekoč vsakdo postavi na splet – vključno s prispevki v wikipediji. Zato jih sicer lahko navajamo, le zavedati se moramo njihove trdnosti. Prav pri wikipediji je v prispevku spodaj pogosto navedena dodatna literatura, ki je običajno verodostojnejša. Drugi razlog pa je spremenljivost virov, saj lahko nekdo spletno stran, ki jo navajamo, med tem spremeni. Zato se pri spletnih virih vedno dopiše, kdaj smo dostopali do vira.

Matura iz informatike

Spomladanski rok 2013

POLA 1, NALOGA 20

Poznamo naslednje vrste lastništva programske opreme: javno, prosto, odprto in tržno.
20.1. Za vsakega od spodaj navedenih programov določite vrsto lastništva programske opreme.

Program	Vrsta lastništva
Microsoft Word	
Open Office	
WinZip	
Firefox	
IrfanView	

ACM skupina:

- SP. Social in Professional Issues - Družbena in poklicna vprašanja.

Razlaga:

Naloga preverja poznavanje programov in njihovih licenc.

Najprej se moramo zavedati, da programska oprema ni kot kolesa, saj jo zelo preprosto podvajamo. To je eden od razlogov, da programske opreme ne kupujemo, ampak jo najemamo za uporabo – pravimo, da pridobimo licenco za uporabo – podobno kot skladbe ne kupimo, ampak jo lahko dobimo na uporabo za poslušanje. To je tudi razlog, da dostop do obeh vrst lastnine določa podobna zakonodaja (*copyright*) – mi dobimo pravico do uporabe, lastnik se ne menja.

Razlike nastopijo v pravicah, ki nam jih daje licenca. Na eni strani je licenca s pravico zgolj do uporabe (in običajno arhivske kopije). V tem primeru dobimo običajno prevedeno programsko opremo, ki je primerna za izvajanje. Takšna licenca lahko prepoveduje obratno inženirstvo (tvorjenje izvorne kode iz prevedenega programa), kar se izkaže posebej pomembno pri opremi, ki se interpretira.

Na drugi strani spektra so tako imenovane odprte ali proste (angleški free pomeni prost dostop in ne brezplačen) licence, ki uporabniku dovoljujejo podvajanje ali celo dostop do izvorne kode. Pri slednjem nastopajo največje razlike med licencami. Na eni strani imamo licence, ki od novega uporabnika zahtevajo, da svoje morebitne popravke v programski kodi tudi nudi prosto ostalim uporabnikom (GPL in izvedenke), ali pa ne (BSD licenca in izvedenke). Komercialno so zaradi tega BSD licence bolj zanimive, ker so do novega uporabnika prijaznejše ter mu puščajo več možnosti. Slednje je posebej pomembno pri določanju poslovnega modela v primeru izdelave lastnega izdelka na osnovi prosto dostopne programske opreme. Nihče namreč novemu uporabniku ne prepoveduje, da svoje popravke prav tako ne izda pod BSD licenco.

Zanimive so tudi licence Creative Commons (CC). Njihov namen je poenostaviti uporabniku postavljanje licenčnih pravic za nove izdelke. Več na spletu.

Poleg tega velja opozoriti, da licenca poleg pravice uporabe običajno določa tudi odgovornosti lastnika programske opreme. Običajno v licenčnih pogodbah piše, da proizvajalec nima nobene odgovornosti.

Vse doslej zapisano govori o pravici do dostopa uporabnika do programske opreme. Nikjer ni govora o ceni le-te. Tega licence ne urejajo. Tako je lahko absurdna situacija, kjer nekdo kupi izvorno kodo Linux od nekoga drugega povsem legalna, le morda ne najbolj smiselna.