



332E



«اگر دانشگاه اصلاح شود مملکت اصلاح می شود.»
امام خمینی (ره)

دفترچه شماره (۱)

صبح جمعه

۹۸/۱۲/۹

جمهوری اسلامی ایران
وزارت علوم، تحقیقات و فناوری
سازمان سنجش آموزش کشور

آزمون ورودی دوره دکتری (نیمه متمرکز) - سال ۱۳۹۹

رشته مهندسی فناوری اطلاعات - کد (۲۳۵۸)

مدت پاسخ گویی: ۱۵۰ دقیقه

تعداد سؤال: ۴۵

عنوان مواد امتحانی، تعداد و شماره سؤالات

ردیف	مواد امتحانی	تعداد سؤال	از شماره	تا شماره
۱	مجموعه دروس تخصصی: حل مسئله (ساختمان داده ها و طراحی الگوریتم ها) - شبکه (شبکه های کامپیوتری و امنیت شبکه) - مهندسی اطلاعات (پایگاه داده پیشرفته، بازیابی پیشرفته اطلاعات و داده کاوی) - خدمات فناوری اطلاعات (تجارت الکترونیک و آموزش الکترونیکی)	۴۵	۱	۴۵

این آزمون نمره منفی دارد.

استفاده از ماشین حساب مجاز نیست.

حق چاپ، تکثیر و انتشار سؤالات به هر روش (الکترونیکی و...) پس از برگزاری آزمون، برای تمامی اشخاص حقیقی و حقوقی تنها با مجوز این سازمان مجاز می باشد و یا متخلفین برابر مقررات رفتار می شود.

* داوطلب درامی، عدم درج مشخصات و امضا در مندرجات جدول ذیل، به منزله عدم حضور شما در جلسه آزمون است.

اینجانب با شماره داوطلبی با آگاهی کامل، یکسان بودن شماره صندلی خود را با شماره داوطلبی مندرج در بالای کارت ورود به جلسه، بالای پاسخنامه و دفترچه سؤالات، نوع و کد کنترل درج شده بر روی دفترچه سؤالات و پائین پاسخنامه را تأیید می‌نمایم.

امضا:

۱- فرض کنید متنی به طول n در اختیار داریم. در خصوص گزاره‌های زیر کدام گزینه صحیح است؟
(الف) کد هافمن یک کاراکتر یک بیتی است، اگر و فقط اگر تعداد تکرار آن کاراکتر کمتر از جمع تعداد تکرار بقیه کاراکترها نباشد.

(ب) اگر کاراکتری بیشترین تکرار را داشته باشد و تعداد تکرارهای آن بیش از $\frac{n}{3}$ باشد، آنگاه کد هافمن آن کاراکتر تک بیتی است.

(۲) (الف) نادرست و (ب) درست

(۱) (الف) درست و (ب) درست

(۴) (الف) نادرست و (ب) نادرست

(۳) (الف) درست و (ب) نادرست

۲- یک گراف کامل 10 رأسی را در نظر بگیرید. که رأس‌های آن از 1 تا 10 شماره‌گذاری شده‌اند. فرض کنید وزن یال بین i و j برابر $i + j$ است. آخرین یال درخت پوشای کمینه که توسط الگوریتم پریم با شروع از رأس 10 اضافه می‌شود، چه وزنی دارد؟

(۱) ۹

(۲) ۱۰

(۳) ۱۱

(۴) ۱۷

۳- در پیاده‌سازی متعارف جستجوی عمق اول و جستجوی سطح اول، به ترتیب از کدام داده ساختارها استفاده می‌شود؟

(۲) صف و پشته

(۱) پشته و صف

(۴) لیست و پشته

(۳) پشته و لیست

۴- مسئله جمع زیرمجموعه بدین شکل تعریف می‌شود: یک مجموعه از اعداد مثبت $S = \{a_1, \dots, a_n\}$ به همراه عدد W داده شده است. آیا زیرمجموعه‌ای از S پیدا می‌شود که جمع اعضای آن W شود؟

برای حل این مسئله به روش برنامه‌ریزی پویا یک آرایه دو بُعدی $X[1..n, 0..W]$ تعریف می‌کنیم که $X[i, j]$ برابر True است. اگر زیرمجموعه‌ای از $S = \{a_1, \dots, a_i\}$ وجود داشته باشد که جمع اعضای آن j شود، در

این خصوص کدام رابطه درست است؟

$$X[i, j] = X[i-1, j] \wedge X[i, j-a_i] \quad (۲)$$

$$X[i, j] = X[i-1, j] \vee X[i, j-a_i] \quad (۱)$$

$$X[i, j] = X[i-1, j] \wedge X[i-1, j-a_i] \quad (۴)$$

$$X[i, j] = X[i-1, j] \vee X[i-1, j-a_i] \quad (۳)$$



۵- مرسی سید $G = (V, E)$ یک گراف بدون جهت و گراف $G' = (V', E')$ یک زیرگراف G است. یالهای G را بدین شکل وزن دار می‌کنیم: اگر $e \in E'$ باشد، وزن آن را صفر و در غیر اینصورت ۱ می‌گذاریم. از رأس دلخواه $v \in V'$ الگوریتم دایکسترا را برای محاسبه کوتاهترین مسیر به بقیه رئوس اجرا می‌کنیم. کدام مسئله را می‌توان با استفاده از طول کوتاهترین مسیرهای محاسبه شده، حل کرد؟

(۱) آیا G' درخت است؟

(۲) آیا G' همبند است؟

(۳) آیا G' تشکیل خوشه می‌دهد؟

(۴) تعداد یال‌ها در کوتاهترین مسیر از v به بقیه رئوس چند است؟

۶- فرض کنید در داخل یک درخت دودویی جستجو، اعداد ۱ تا ۱۰۰۰ ذخیره شده‌اند و ما می‌خواهیم دنباله عدد ۳۶۵ بگردیم. کدام دنباله (از چپ به راست) نمی‌تواند مسیر جستجو باشد؟

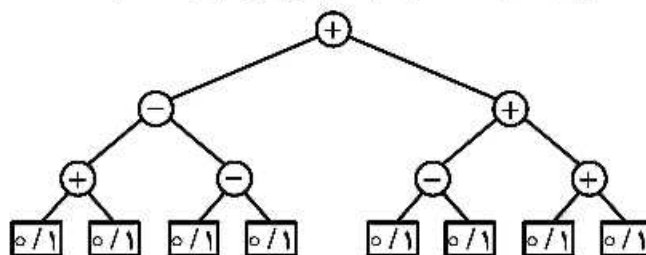
(۱) ۴, ۴۰۱, ۳۸۹, ۲۲۱, ۲۶۸, ۳۸۴, ۳۸۳, ۲۸۰, ۳۶۵

(۲) ۹۲۶, ۲۲۲, ۹۱۳, ۲۴۶, ۹۰۰, ۲۶۰, ۳۶۴, ۳۶۵

(۳) ۴, ۲۵۴, ۴۰۳, ۴۰۰, ۳۳۲, ۲۴۶, ۳۹۹, ۳۶۵

(۴) ۹۲۷, ۲۰۴, ۹۱۳, ۲۴۲, ۹۱۴, ۲۴۷, ۳۶۵

۷- در درخت میانوندی داده شده، مقدار هر برگ می‌تواند صفر یا یک باشد. ماکزیمم خروجی این عبارت کدام است؟



(۱) ۲

(۲) ۳

(۳) ۴

(۴) ۶

۸- می‌دانیم ترتیب شروع و پایان فعالیت‌های A و B و C و D و E و F و G و H و I و J و K و L و M و N و O و P و Q و R و S و T و U و V و W و X و Y و Z و AA و AB و AC و AD و AE و AF و AG و AH و AI و AJ و AK و AL و AM و AN و AO و AP و AQ و AR و AS و AT و AU و AV و AW و AX و AY و AZ و BA و BB و BC و BD و BE و BF و BG و BH و BI و BJ و BK و BL و BM و BN و BO و BP و BQ و BR و BS و BT و BU و BV و BW و BX و BY و BZ و CA و CB و CC و CD و CE و CF و CG و CH و CI و CJ و CK و CL و CM و CN و CO و CP و CQ و CR و CS و CT و CU و CV و CW و CX و CY و CZ و DA و DB و DC و DD و DE و DF و DG و DH و DI و DJ و DK و DL و DM و DN و DO و DP و DQ و DR و DS و DT و DU & DV و DW و DX و DY و DZ و EA و EB و EC و ED و EE و EF و EG و EH و EI و EJ و EK و EL & EM و EN و EO و EP و EQ و ER و ES و ET و EU و EV و EW و EX و EY و EZ و FA و FB و FC و FD و FE و FF و FG و FH و FI & FJ و FK و FL و FM و FN و FO و FP و FQ و FR و FS و FT & FU و FV و FW و FX و FY و FZ و GA و GB و GC و GD و GE و GF & GG و GH و GI & GJ و GK و GL & GM و GN & GO & GP & GQ & GR & GS & GT & GU & GV & GW & GX & GY & GZ & HA & HB & HC & HD & HE & HF & HG & HH & HI & HJ & HK & HL & HM & HN & HO & HP & HQ & HR & HS & HT & HU & HV & HW & HX & HY & HZ & IA & IB & IC & ID & IE & IF & IG & IH & II & IJ & IK & IL & IM & IN & IO & IP & IQ & IR & IS & IT & IU & IV & IW & IX & IY & IZ & JA & JB & JC & JD & JE & JF & JG & JH & JI & JJ & JK & JL & JM & JN & JO & JP & JQ & JR & JS & JT & JU & JV & JW & JX & JY & JZ & KA & KB & KC & KD & KE & KF & KG & KH & KI & KJ & KK & KL & KM & KN & KO & KP & KQ & KR & KS & KT & KU & KV & KW & KX & KY & KZ & LA & LB & LC & LD & LE & LF & LG & LH & LI & LJ & LK & LL & LM & LN & LO & LP & LQ & LR & LS & LT & LU & LV & LW & LX & LY & LZ & MA & MB & MC & MD & ME & MF & MG & MH & MI & MJ & MK & ML & MM & MN & MO & MP & MQ & MR & MS & MT & MU & MV & MW & MX & MY & MZ & NA & NB & NC & ND & NE & NF & NG & NH & NI & NJ & NK & NL & NM & NN & NO & NP & NQ & NR & NS & NT & NU & NV & NW & NX & NY & NZ & OA & OB & OC & OD & OE & OF & OG & OH & OI & OJ & OK & OL & OM & ON & OO & OP & OQ & OR & OS & OT & OU & OV & OW & OX & OY & OZ & PA & PB & PC & PD & PE & PF & PG & PH & PI & PJ & PK & PL & PM & PN & PO & PP & PQ & PR & PS & PT & PU & PV & PW & PX & PY & PZ & QA & QB & QC & QD & QE & QF & QG & QH & QI & QJ & QK & QL & QM & QN & QO & QP & QQ & QR & QS & QT & QU & QV & QW & QX & QY & QZ & RA & RB & RC & RD & RE & RF & RG & RH & RI & RJ & RK & RL & RM & RN & RO & RP & RQ & RR & RS & RT & RU & RV & RW & RX & RY & RZ & SA & SB & SC & SD & SE & SF & SG & SH & SI & SJ & SK & SL & SM & SN & SO & SP & SQ & SR & SS & ST & SU & SV & SW & SX & SY & SZ & TA & TB & TC & TD & TE & TF & TG & TH & TI & TJ & TK & TL & TM & TN & TO & TP & TQ & TR & TS & TT & TU & TV & TW & TX & TY & TZ & UA & UB & UC & UD & UE & UF & UG & UH & UI & UJ & UK & UL & UM & UN & UO & UP & UQ & UR & US & UT & UV & UW & UX & UY & UZ & VA & VB & VC & VD & VE & VF & VG & VH & VI & VJ & VK & VL & VM & VN & VO & VP & VQ & VR & VS & VT & VU & VV & VW & VX & VY & VZ & WA & WB & WC & WD & WE & WF & WG & WH & WI & WJ & WK & WL & WM & WN & WO & WP & WQ & WR & WS & WT & WU & WV & WW & WX & WY & WZ & XA & XB & XC & XD & XE & XF & XG & XH & XI & XJ & XK & XL & XM & XN & XO & XP & XQ & XR & XS & XT & XU & XV & XW & XX & XY & XZ & YA & YB & YC & YD & YE & YF & YG & YH & YI & YJ & YK & YL & YM & YN & YO & YP & YQ & YR & YS & YT & YU & YV & YW & YX & YY & YZ & ZA & ZB & ZC & ZD & ZE & ZF & ZG & ZH & ZI & ZJ & ZK & ZL & ZM & ZN & ZO & ZP & ZQ & ZR & ZS & ZT & ZU & ZV & ZW & ZX & ZY & ZZ & AA & AB & AC & AD & AE & AF & AG & AH & AI & AJ & AK & AL & AM & AN & AO & AP & AQ & AR & AS & AT & AU & AV & AW & AX & AY & AZ & BA & BB & BC & BD & BE & BF & BG & BH & BI & BJ & BK & BL & BM & BN & BO & BP & BQ & BR & BS & BT & BU & BV & BW & BX & BY & BZ & CA & CB & CC & CD & CE & CF & CG & CH & CI & CJ & CK & CL & CM & CN & CO & CP & CQ & CR & CS & CT & CU & CV & CW & CX & CY & CZ & DA & DB & DC & DD & DE & DF & DG & DH & DI & DJ & DK & DL & DM & DN & DO & DP & DQ & DR & DS & DT & DU & DV & DW & DX & DY & DZ & EA & EB & EC & ED & EE & EF & EG & EH & EI & EJ & EK & EL & EM & EN & EO & EP & EQ & ER & ES & ET & EU & EV & EW & EX & EY & EZ & FA & FB & FC & FD & FE & FF & FG & FH & FI & FJ & FK & FL & FM & FN & FO & FP & FQ & FR & FS & FT & FU & FV & FW & FX & FY & FZ & GA & GB & GC & GD & GE & GF & GG & GH & GI & GJ & GK & GL & GM & GN & GO & GP & GQ & GR & GS & GT & GU & GV & GW & GX & GY & GZ & HA & HB & HC & HD & HE & HF & HG & HH & HI & HJ & HK & HL & HM & HN & HO & HP & HQ & HR & HS & HT & HU & HV & HW & HX & HY & HZ & IA & IB & IC & ID & IE & IF & IG & IH & II & IJ & IK & IL & IM & IN & IO & IP & IQ & IR & IS & IT & IU & IV & IW & IX & IY & IZ & JA & JB & JC & JD & JE & JF & JG & JH & JI & JJ & JK & JL & JM & JN & JO & JP & JQ & JR & JS & JT & JU & JV & JW & JX & JY & JZ & KA & KB & KC & KD & KE & KF & KG & KH & KI & KJ & KK & KL & KM & KN & KO & KP & KQ & KR & KS & KT & KU & KV & KW & KX & KY & KZ & LA & LB & LC & LD & LE & LF & LG & LH & LI & LJ & LK & LL & LM & LN & LO & LP & LQ & LR & LS & LT & LU & LV & LW & LX & LY & LZ & MA & MB & MC & MD & ME & MF & MG & MH & MI & MJ & MK & ML & MM & MN & MO & MP & MQ & MR & MS & MT & MU & MV & MW & MX & MY & MZ & NA & NB & NC & ND & NE & NF & NG & NH & NI & NJ & NK & NL & NM & NN & NO & NP & NQ & NR & NS & NT & NU & NV & NW & NX & NY & NZ & OA & OB & OC & OD & OE & OF & OG & OH & OI & OJ & OK & OL & OM & ON & OO & OP & OQ & OR & OS & OT & OU & OV & OW & OX & OY & OZ & PA & PB & PC & PD & PE & PF & PG & PH & PI & PJ & PK & PL & PM & PN & PO & PP & PQ & PR & PS & PT & PU & PV & PW & PX & PY & PZ & QA & QB & QC & QD & QE & QF & QG & QH & QI & QJ & QK & QL & QM & QN & QO & QP & QQ & QR & QS & QT & QU & QV & QW & QX & QY & QZ & RA & RB & RC & RD & RE & RF & RG & RH & RI & RJ & RK & RL & RM & RN & RO & RP & RQ & RR & RS & RT & RU & RV & RW & RX & RY & RZ & SA & SB & SC & SD & SE & SF & SG & SH & SI & SJ & SK & SL & SM & SN & SO & SP & SQ & SR & SS & ST & SU & SV & SW & SX & SY & SZ & TA & TB & TC & TD & TE & TF & TG & TH & TI & TJ & TK & TL & TM & TN & TO & TP & TQ & TR & TS & TT & TU & TV & TW & TX & TY & TZ & UA & UB & UC & UD & UE & UF & UG & UH & UI & UJ & UK & UL & UM & UN & UO & UP & UQ & UR & US & UT & UV & UW & UX & UY & UZ & VA & VB & VC & VD & VE & VF & VG & VH & VI & VJ & VK & VL & VM & VN & VO & VP & VQ & VR & VS & VT & VU & VV & VW & VX & VY & VZ & WA & WB & WC & WD & WE & WF & WG & WH & WI & WJ & WK & WL & WM & WN & WO & WP & WQ & WR & WS & WT & WU & WV & WW & WX & WY & WZ & XA & XB & XC & XD & XE & XF & XG & XH & XI & XJ & XK & XL & XM & XN & XO & XP & XQ & XR & XS & XT & XU & XV & XW & XX & XY & XZ & YA & YB & YC & YD & YE & YF & YG & YH & YI & YJ & YK & YL & YM & YN & YO & YP & YQ & YR & YS & YT & YU & YV & YW & YX & YY & YZ & ZA & ZB & ZC & ZD & ZE & ZF & ZG & ZH & ZI & ZJ & ZK & ZL & ZM & ZN & ZO & ZP & ZQ & ZR & ZS & ZT & ZU & ZV & ZW & ZX & ZY & ZZ

۹- اعداد صحیح بین ۱ تا ۱۳۹۸ به عنوان ورودی داده شده است. کدام تابع درهم‌ساز، اعداد داده شده را به‌طور یکنواخت بین ۱۰ خانه جدول درهم‌سازی توزیع می‌کند؟ (یک توزیع یکنواخت است، اگر تفاضل تعداد اعداد نگاشت شده به هر دو خانه از جدول حداکثر ۱ باشد).

$$h(i) = i^2 \bmod 10 \quad (۲)$$

$$h(i) = i^2 \bmod 10 \quad (۱)$$

$$h(i) = 4i^2 + 6 \bmod 10 \quad (۴)$$

$$h(i) = 12i \bmod 10 \quad (۳)$$

۱۰- آرایه $A[1..13] = 89, 19, 40, 17, 12, 10, 2, 5, 7, 11, 6, 3, 2$ داده شده است. می توانیم هر بار دو خانه دلخواه از این آرایه را با هم جابه جا کنیم. با حداقل چند جابه جایی می توان این آرایه را به یک هرم بیشینه تبدیل کرد؟

- (۱) ۵
- (۲) ۱
- (۳) ۲
- (۴) ۳

۱۱- فرض کنید در گراف وزن دار و جهت دار G با n رأس، تنها وزن یال های خارج شده از رأس s ممکن است منفی باشند. (البته می دانیم گراف دور منفی ندارد.) بزرگ ترین n که به ازای آن الگوریتم دایکسترا روی هر گراف n رأسی با فرض های گفته شده کوتاه ترین مسیر از s به بقیه رئوس را درست محاسبه می کند، کدام است؟

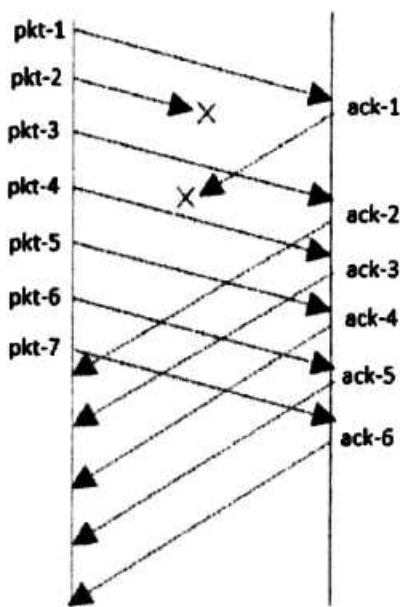
- (۱) ۲
- (۲) ۳
- (۳) ۴

(۴) به ازای هر n همیشه درست کار می کند.

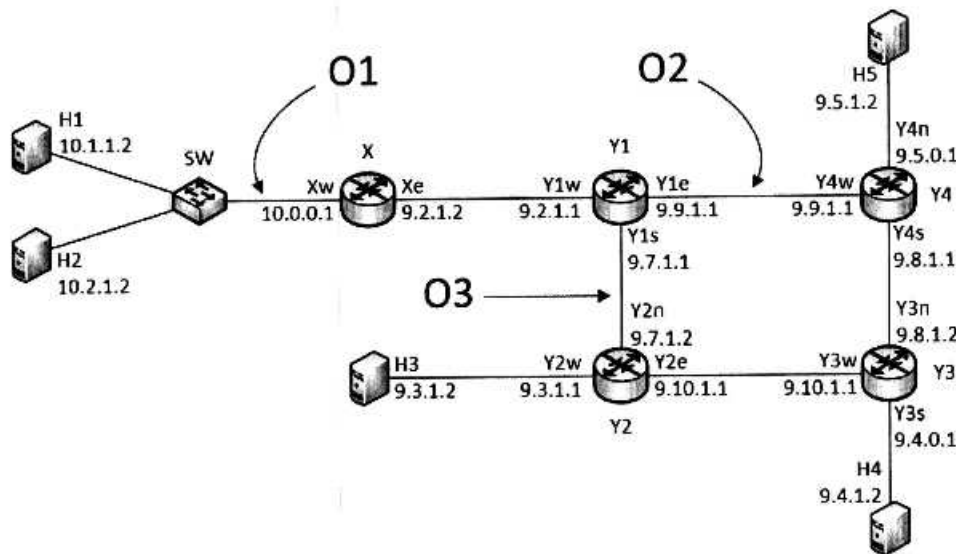
۱۲- زمان اجرای الگوریتمی به صورت $T(n) = T(n/11) + T(6n/11) + n$ است. مرتبه زمانی اجرای این الگوریتم کدام است؟

- (۱) $O(n)$
- (۲) $O(n^2)$
- (۳) $O(\log n)$
- (۴) $O(n \log n)$

۱۳- تبادل پیام های شکل زیر را در نظر بگیرید. فرض کنید که طرفین برای ارتباط اتکاپذیر از TCP نسخه Reno استفاده می کنند. در شکل زیر i امین ack که گیرنده ارسال کرده است را با نماد $ack-i$ نشان می دهیم. در زمان دریافت $ack-5$ در سمت فرستنده کدام مکانیزم فعال می شود؟



- (۱) slow start
- (۲) fast retransmit
- (۳) exponential back-off
- (۴) congestion avoidance



گره‌های H1, H2, H3, H4, H5 میزبان هستند و SW یک سوئیچ است. گره‌های X, Y1, Y2, Y3, Y4 مسیریاب‌هایی هستند که ARP proxy بر روی آنها اجرا نشده است. ترافیک در نقاط O1, O2, O3 بر روی هر دو جهت لینک‌های متناظر قابل مشاهده است. آدرس IP و MAC هر رابط (interface) در کنار آن نشان داده شده است (مثلاً، آدرس IP رابط میزبان H1 برابر 10.1.1.2 و آدرس MAC آن برابر H1 است و نیز آدرس IP رابط غربی Y1 برابر 9.2.1.1 و آدرس MAC رابط غربی آن برابر Y1w است). فرض کنید میزبان‌های H1 و H2 تازه راه‌اندازی شده‌اند. در این حالت، دستورات زیر را بر روی سیستم‌ها اجرا می‌کنیم: (نماد H1>ping 10.2.1.2 -n 1 یعنی میزبان H1 آدرس 10.2.1.2 را یکبار ping می‌کند).

H1>ping	10.2.1.2	-n	1
H2>ping	9.3.1.2	-n	1
H3>ping	9.4.1.2	-n	1
H4>ping	9.5.1.2	-n	1
H5>ping 10.1.1.2 -n 1			

در بسته درخواست ARP از طرف میزبان‌های H1 و H2 به ترتیب آدرس IP مقصد برابر کدام مورد است؟ فرض کنید که default gateway هر دو میزبان مسیریاب X است.

- (۱) برای بسته III - 9.2.1.2 و برای بسته II - 9.2.1.2
- (۲) برای بسته III - 9.2.1.2 و برای بسته II - 10.0.0.1
- (۳) برای بسته H1 - 10.2.1.2 و برای بسته H2 - 9.2.1.2
- (۴) برای بسته H1 - 10.2.1.2 و برای بسته H2 - 10.0.0.1

۱۵- پروتکل selective repeat (SR) برای ارسال اطلاعات بین یک فرستنده و گیرنده روی یک لینک مخابراتی استفاده می‌شود. نرخ ارسال اطلاعات برابر 1Gbps است. سایز بسته داده 1250byte است و از سایز بسته ACK صرف نظر می‌شود. تأخیر انتشار یک طرفه بین فرستنده و گیرنده برابر 45μsec است. اگر طول پنجره SR برابر ۵ باشد، گذردهی (throughput) چند Mbps است؟

- | | |
|---------|---------|
| (۱) 900 | (۲) 750 |
| (۳) 500 | (۴) 450 |

۶- یب پرویس پنجره لغزان را در نظر بگیرید، که اندازه پنجره بهینه را برای شبکه با توپولوژی با مشخصات زیر انتخاب کرده است.

A-----B-----C-----D-----E

هر لینک می تواند 1 بسته در ثانیه ارسال کند. هیچ صفی در گره ها تشکیل نمی شود و منابع دیگر تأخیر غیر از تأخیر ارسال صفر در نظر گرفته می شود. فرض کنید بسته های با شماره ترتیب (sequence number) فرد حذف می شوند. شماره ترتیب از 1 شروع می شود. مقدار time out در فرستنده را 40 ثانیه در نظر بگیرید. گیرنده بسته های خارج از ترتیب را بافر می کند. در نهایت گیرنده بسته های مرتب شده را به لایه کاربرد تحویل می دهد. پس از آنکه فرستنده اولین بسته را در $t = 1$ ارسال کرد، تعداد بسته های موجود در بافر گیرنده در ثانیه $t = 35$ کدام است؟

3 (۲)

7 (۱)

0 (۴)

1 (۳)

۱۷- اگر اندازه یک بسته IP برابر 2000 بایت و MTU لینکی که بسته قرار است روی آن ارسال شود برابر 1500 بایت و بیت D در سرآیند (header) این بسته IP صفر باشد، کدام مورد برای بسته رخ می دهد؟

(۱) بسته دور انداخته می شود و یک پیام ICMP error برای مبدأ ارسال خواهد شد.

(۲) بسته دور انداخته می شود، بدون آنکه هیچ گونه پیغامی از نوع ICMP error برای مبدأ ارسال گردد.

(۳) بسته به 2 قطعه تقسیم می شود، بدون آنکه هیچ گونه پیغامی از نوع ICMP error برای مبدأ ارسال گردد.

(۴) بسته به 2 قطعه تقسیم می شود و قطعات به دنبال هم به سمت مقصد در یک مسیر یکسان حرکت خواهند کرد.

۱۸- کدام گزینه، از موارد استفاده از بات نت ها توسط هکرها نیست؟

(۱) سرقت اطلاعات (۲) ارسال هرزنامه

(۳) انتشار کرم های اینترنتی (۴) اجرای حمله منع سرویس توزیع شده

۱۹- استفاده از salt در کنار گذر واژه ها به هنگام محاسبه چکیده گذر واژه ها با استفاده از توابع چکیده ساز (Hash) به منظور جلوگیری از چه حملاتی صورت می گیرد؟

(۱) حمله لغت نامه ای (۲) حمله مرد میانی (۳) حمله تکرار (۴) حمله روز تولد

۲۰- دو کامپیوتر به نوعی در دو LAN (Local Area Network) قرار دارند که از IP های محلی (Invalid IP) استفاده می کنند. این دو LAN با Router های لبه (Edge Router) به اینترنت متصل هستند. چنانچه بخواهیم از IPsec برای امن سازی ارتباط بین دو این کامپیوتر استفاده کنیم، این کار در کدام گزینه بهتر انجام می شود؟

ESP = Encapsulating Security Payload

AH = Authentication Headr

(۱) چنانچه Router ها از IPsec پشتیبانی نکنند، دو کامپیوتر می توانند به طور مستقیم بین یکدیگر از ESP یا AH در Tunnel Mode استفاده کنند.

(۲) چنانچه Router ها از IPsec پشتیبانی نکنند، دو کامپیوتر می توانند به طور مستقیم بین یکدیگر از ESP یا AH در Transport Mode استفاده کنند.

(۳) چنانچه Router ها از IPsec پشتیبانی کنند و رنج آدرس LAN های دو طرف برای آنها شناخته شده باشد، Router ها بین یکدیگر از ESP یا AH در Transport Mode استفاده کنند.

(۴) چنانچه Router ها از IPsec پشتیبانی کنند و رنج آدرس LAN های دو طرف برای آنها شناخته شده باشد، Router ها بین یکدیگر از ESP یا AH در Tunnel Mode استفاده کنند.

۲۱- سس ریر پیامهای مرحله ۵ و ۶ در KERBEROS v5 را بین Client (C) و Server (V) نشان می دهد. کدام گزینه نقش TS2 (Timestamp) و Subkey را در پیام ۶ بهتر بیان می کند؟

(5) $C \rightarrow V$ Options || Ticket_v || Authenticator_c

(6) $V \rightarrow C$ E_{K_{c,v}}[TS₂ || Subkey || Seq #]

$$\text{Ticket}_v = E(K_v, [\text{Flags} || K_{c,v} || \text{Realm}_c || \text{ID}_C || \text{AD}_C || \text{Times}])$$

$$\text{Authenticator}_c = E(K_{c,v}, [\text{ID}_C || \text{Realm}_c || \text{TS}_2 || \text{Subkey} || \text{Seq \#}])$$

(۱) TS2 برای اطمینان Client از fresh بودن پیام ششم ارسال می شود و Subkey کلید جلسه ای که برای ادامه ارتباطات امن application لازم است را به دست Client می رساند.

(۲) TS2, Server را به Client احراز هویت می کند و Subkey کلید جلسه ای که برای ادامه ارتباطات امن application لازم است را به دست Client می رساند.

(۳) TS2 برای جلوگیری از Replay Attack در پیام ششم ارسال می شود و Subkey کلید جلسه ای که Client در مرحله پنجم ارسال کرده بود را تأیید می کند.

(۴) TS2 برای جلوگیری از Replay Attack در پیام ششم ارسال می شود و Subkey کلید ارتباطات آینده Client و Server را به دست Client می رساند.

۲۲- در سیستم RSA، کلید عمومی $e = 7$ و کلید خصوصی $d = 23$ است. چنانچه یکی از دو عدد سازنده پیمانه برابر $p = 5$ باشد، مقدار ممکن برای دیگر عدد سازنده پیمانه، کدام گزینه می تواند باشد؟

(۱) $q = 11$

(۲) $q = 17$

(۳) $q = 21$

(۴) $q = 31$

۲۳- در خصوص اجرای طرح زیر در پروتکل Strict 2PL، کدام گزینه صحیح است؟

	T1	T2
1	R(A)	
2	W(A)	
3		R(A)
4	R(B)	
5		R(B)
6	W(B)	
7		W(B)

(۱) این طرح توالی پذیر نیست.

(۲) این طرح معادل طرح سریال {T2, T1} است.

(۳) این طرح معادل طرح سریال {T1, T2} است.

(۴) اجرای طرح با پروتکل Strict 2PL به بن بست می انجامد.

۴- سرسوری به $A=10, B=15, C=5, D=20$ باشد، اجرای طرح زیر در پروتکل wound-wait، به چه نتیجه‌ای منجر خواهد شد؟ ($L(A)$ به معنی lock کردن داده A و $U(A)$ به معنی unlock کردن داده A است.)

	T1	T2	T3	T4
	TS(T1)=100	TS(T1)=150	TS(T3)=200	TS(T4)=250
1	L(A), R(A)			
2		L(A), R(A)		
3			L(B), R(B)	
4	L(B), R(B)			
5				L(A), L(D)
6				
7	$B=B+A/2$			
8			L(C), R(C)	
9			$C=C*(B/5)$	
10			W(C)	
11				R(A), R(D)
12			U(B), U(C)	
13		L(C), R(C)		
14		$A=A-C$		
15		W(A)		
16				$A=A+D$
17				W(A)
18				U(D), U(A)
19	W(B)			
20	U(A), U(B)			
21		U(C), U(A)		

(۱) $A = 25, B = 20, C = 20, D = 20$

(۲) $A = 15, B = 22.5, C = 15, D = 20$

(۳) $A = -10, B = 20, C = 15, D = 20$

(۴) $A = -15, B = 20, C = 20, D = 20$

۲۵ در مورد اجرای طرح زیر (از چپ به راست) کدام مورد صحیح است؟

$R_1(B), W_1(A), R_2(A), R_3(A), W_2(B), W_1(B), W_3(B)$

(۱) این طرح توالی‌پذیر نیست.

(۲) این طرح توالی‌پذیر نمایی نیست.

(۳) این طرح توالی‌پذیر تعارضی است.

(۴) این طرح توالی‌پذیر نمایی است ولی توالی‌پذیر تعارضی نیست.

۲۶- کدام گزینه در مورد nested-loop join (از استراتژی‌های پیاده‌سازی عمل join) صحیح است؟

(۱) باید حتی‌الامکان تعداد بیشتری بلاک از فایل رابطه حلقه درونی خوانده شود.

(۲) nested-loop join در حالتی که یکی از رابطه‌ها در حافظه اصلی جا شود، کارایی بهتری دارد.

(۳) در صورتی که رابطه بزرگتر به صورت کامل در حافظه جای گیرد، بهتر است این رابطه در حلقه درونی پیمایش شود.

(۴) در نظر گرفتن رابطه با کاردینالیته بزرگتر به عنوان رابطه حلقه بیرونی، سبب افزایش کارایی اجرای الگوریتم می‌شود.



۷- سرسورب برای طرح زیر در پروتکل certification یا همان validation، کدام گزینه صحیح است؟
(RS = مجموعه خواندن تراکنش و WS = مجموعه نوشتن تراکنش است)

T1: {RS = A, B}, {WS = A, C}

T2: {RS = B}, {WS = D}

T3: {RS = D}, {WS = A, C}

T4: {RS = B}, {WS = D}

	T1	T2	T3	T4
1	S			
2		S		
3		V		
4	V			
5			S	
6		F		
7				S
8			V	
9	F			
10				V
11			E	
12				E

- (۱) تراکنش‌های T2, T3, T4 تأیید و T1 لغو می‌شود.
(۲) تراکنش‌های T1, T2, T4 تأیید و T3 لغو می‌شود.
(۳) تراکنش‌های T1, T2, T3 تأیید و T4 لغو می‌شود.
(۴) تراکنش‌های T1 و T2 تأیید و T3 و T4 لغو می‌شوند.

۲۸- یک پرس‌وجو را در نظر بگیرید که در کل 5 سند مرتبط با آن در مجموعه اسناد موجود است. لیست مرتب پاسخ‌های سه سیستم S1 و S2 و S3 در پاسخ به این پرس‌وجو در جدول زیر آمده است. "1" در ستون پاسخ‌های یک سیستم نشان‌دهنده مرتبط بودن سند بازگردانده شده در آن رتبه به پرس‌وجو و "0" نشان‌دهنده نامرتب بودن سند بازگردانده شده است. کارایی این سه سیستم براساس معیار F1 سنجیده شده است. با توجه به این معیار، کارایی این سه سیستم به نسبت هم چگونه است؟ ($S_i > S_j$ به این معنی است که S_i از S_j بهتر عمل کرده است).

Rank	S1	S2	S3
1	0	1	1
2	0	0	1
3	1	0	0
4	1	0	0
5	1	1	0
6	1	1	0

- (۱) $S1 > S2 > S3$
(۲) $S1 > S3 > S2$
(۳) $S3 > S1 > S2$
(۴) $S3 > S2 > S1$

۲۹- یک مجموعه داده را در نظر بگیرید که تعداد ترم‌های یکتای آن 5 است ($|V| = 5$). تخمین مدل زبانی مرجع ($p(w|Ref)$) که از روی کل مجموعه داده به دست آمده، در جدول زیر آورده شده است. سند d با 5 ترم را در نظر بگیرید. تعداد تکرار هر ترم در این سند نیز در جدول آورده شده است. می‌خواهیم مدل زبانی unigram را برای سند d تخمین بزنیم. برای این منظور از تخمین بیشینه درست‌نمایی (maximum likelihood) و روش هموارسازی Dirichlet Prior استفاده می‌کنیم. با زیاد کردن مقدار پارامتر μ در هموارسازی Dirichlet، احتمال هموار شده ترم w_2 چگونه تغییر می‌کند؟

Term	$p(w Ref)$	$c(w, d)$
w1	0.1	0
w2	0.2	1
w3	0.05	0
w4	0.6	3
w5	0.05	1

- (۱) کم می‌شود.
(۲) زیاد می‌شود.
(۳) تغییر نمی‌کند.
(۴) تغییرات غیرقابل پیش‌بینی است.

۳۰- فرض کنید CF_i تعداد دفعات رخداد w_i باشد و w_i ، w_j ، w_k کلمه پر رخداد در مجموعه اسناد C است. براساس

قانون Zipf، کدام گزینه تخمین خوبی برای $\frac{CF_{10}}{CF_{11}}$ است؟

(۱) $\frac{10}{11}$

(۲) $\frac{11}{10}$

(۳) $\left(\frac{10}{11}\right)^2$

(۴) $\left(\frac{11}{10}\right)^2$

۳۱- کدام تکنیک برای فشرده سازی Postings به کار می رود؟

(۱) Skip Pointer

(۲) Blocked Storage

(۳) Dictionary as a String

(۴) Variable Byte Code

۳۲- هشت شیء A, B, C, D, E, F, G, H را به شکل زیر در یک فضای دو بعدی در نظر بگیرید. با استفاده از

الگوریتم Agglomerative hierarchical clustering و معیار شباهت complete link، این مجموعه از اشیاء

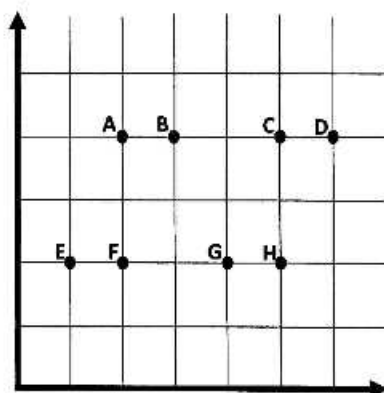
را به دو خوشه تقسیم می کنیم. خوشه های نتیجه، کدام مورد است؟

(۱) {A, B, C, D}, {E, F, G, H}

(۲) {A, B, G, H}, {C, D, E, F}

(۳) {A, B, E, F}, {C, D, G, H}

(۴) {E, F}, {A, B, C, D, G, H}



۳۳- این مجموعه داده را در نظر بگیرید. می خواهیم با استفاده از این داده های آموزشی یک رده بند درخت تصمیم

بسازیم. اگر از معیار Information Gain به عنوان تابع سنجش استفاده کنیم، کدام صفت برای آزمون در ریشه

درخت انتخاب می شود؟

X1	X2	X3	X4	Class Label
T	A	N	T	+
T	A	P	F	-
T	A	N	F	+
F	A	P	F	+
F	B	P	T	-
T	A	P	T	+

(۱) X1

(۲) X2

(۳) X3

(۴) X4

- ۴- در سوسوی سبخت استخراج الگوهای پرتکرار، کدام گزینه صحیح است؟
(۱) همه الگوهای پرتکرار closed maximal هستند.
(۲) اگر همه زیرمجموعه‌های یک الگو پرتکرار باشند، آنگاه آن الگو هم پرتکرار است.
(۳) در یک قانون انجمنی، اگر جای گزاره مقدم و تالی را عوض کنیم، مقدار اطمینان (Confidence) قانون تغییری نخواهد کرد.
(۴) اگر ما الگوهای پرتکرار maximal را همراه با فراوانی (Support) آنها بدانیم، آنگاه از روی آنها می‌توانیم همه الگوهای پرتکرار دیگر و فراوانی‌شان را استخراج کنیم.
- ۳۵ یک مکعب داده دارای m بُعد و هر بُعد دارای p مقدار متمایز در کیوبیوید پایه (Base Cuboid) است. با فرض اینکه در هیچ بُعدی سلسله مراتب مفهومی نداشته باشیم، ماکزیمم سلول‌های غیرتهی (شامل سلول‌های موجود در کیوبیوید پایه و کیوبیویدهای تجمیعی) کدام است؟
(۱) 2^m (۲) p^m
(۳) m^p (۴) $(p+1)^m$
- ۳۶- کدام مورد تحت عنوان کاربردهای تجارت الکترونیکی طبقه‌بندی نمی‌شود؟
(۱) امنیت سایبری (۲) بانکداری برخط (۳) دولت الکترونیکی (۴) تدارکات الکترونیکی
- ۳۷- تیمی از متخصصین برای طراحی یک خودروی جدید با هم همکاری می‌کنند و برای سهولت انجام کارهای خود از یک سیستم استفاده می‌کنند. این نوع از ارتباط را تحت چه عنوانی می‌توان طبقه‌بندی کرد؟
(۱) B2B Commerce (۲) B2C Commerce
(۳) C2C Commerce (۴) Collaborative Commerce
- ۳۸- کدام اظهارنظر در خصوص بازارهای الکترونیکی درست نیست؟
(۱) بازارهای الکترونیکی را می‌توان به بازارهای عمودی و افقی تقسیم‌بندی نمود.
(۲) بازار بورس الکترونیکی را می‌توان حالت خاصی از بازار الکترونیکی به‌شمار آورد.
(۳) مزایده الکترونیکی را می‌توان حالت خاصی از قیمت‌گذاری پویا به‌شمار آورد.
(۴) بازارهای الکترونیکی عمومی از تضمین بقای بالاتری نسبت به بازارهای خصوصی برخوردارند.
- ۳۹- مهم‌ترین مشکلی که پیش‌روی شرکت‌هایی قرار دارد، که می‌خواهند از چندین کانال مختلف برای فروش محصولات خود استفاده کنند، کدام است؟
(۱) یکپارچگی سیستمی (۲) پدیده تداخل کانال‌ها
(۳) پدیده اثر شلاق چرمی (۴) پدیده جایگزینی واسطه‌ها
- ۴۰- تبلیغات ارائه شده توسط موتور جستجوی گوگل، در کدام مورد بهتر طبقه‌بندی می‌شود؟
(۱) تبلیغات اشتراکی (۲) تبلیغات هوشمند
(۳) تبلیغات کلیک (PPC) (۴) بهینه‌سازی برای موتور جستجو (SEO)
- ۴۱- مفهوم تعیین‌گری متقابل (Reciprocal Determinism) در کدام نظریه یادگیری مطرح شده است؟
(۱) گشتالت (۲) مشاهده‌ای بندورا (۳) شناختی خبرپردازی (۴) معنادار کلامی آزوبل
- ۴۲- امروزه کدام ابزار، کاربردهای غیرتولید محتوایی دارد و به‌صورت خاص برای تولید محتوای آموزشی استفاده نمی‌شود؟
(۱) Camtasia (۲) Captivate
(۳) Story line (۴) Multimedia Builder



۳- کدام بخش جزء اسکورم نیست؟

Aggregation Model Content (۲)

Offline Content Consumption (۱)

Run time environment (۴)

Sequencing and navigation (۳)

۴۴- کدام مورد معیار اصلی برای انتخاب رویکرد آموزش الکترونیکی است؟

(۲) سطح سواد یادگیرندگان

(۱) هزینه

(۴) هم راستایی استراتژیک

(۳) مقطع آموزشی

۴۵- آموزش الکترونیکی در کدام یک از اجزای توسعه سازمانی می تواند اثر بخش تر باشد؟

(۲) مدیریت استخدام

(۱) جذب نیروی انسانی

(۴) مدیریت گردش کاری

(۳) مدیریت استعداد

به اطلاع می‌رساند، کلید اولیه سوالات که در این سایت قرار گرفته است، غیر قابل استناد است و پس از دریافت نظرات داوطلبان و صاحب نظران کلید نهایی سوالات تهیه و بر اساس آن کارنامه داوطلبان استخراج خواهد شد. در صورت تمایل می‌توانید حداکثر تا تاریخ 1399/05/14 با مراجعه به سامانه پاسخگویی اینترنتی (request.sanjesh.org) نسبت به تکمیل فرم "اعتراض به کلید سوالات"/"آزمون دکتری سال 1399" اقدام نمایید. لازم به ذکر است نظرات داوطلبان فقط تا تاریخ مذکور و از طریق فرم ذکر شده دریافت خواهد شد و به موارد ارسالی از طریق دیگر (نامه مکتوب یا فرم عمومی در سامانه پاسخگویی و ...) با پس از تاریخ اعلام شده رسیدگی نخواهد شد.



عنوان دفترچه	نوع دفترچه	شماره پاسخنامه	گروه امتحانی
مهندسی فناوری اطلاعات	E	1	مهندسی و فنی

شماره سوال	گزینه صحیح	شماره سوال	گزینه صحیح
1	4	31	4
2	2	32	3
3	1	33	2
4	3	34	1
5	2	35	4
6	4	36	1
7	4	37	4
8	2	38	4
9	2	39	2
10	4	40	3
11	4	41	2
12	1	42	4
13	2	43	1
14	4	44	1
15	3	45	3
16	1		
17	3		
18	3		
19	1		
20	4		
21	2		
22	1		
23	3		
24	1		
25	4		
26	2		
27	2		
28	1		
29	3		
30	2		

خروج