



534F

کد کنترل

534

F

آزمون (نیمه‌مترکز) ورود به دوره‌های دکتری - سال ۱۴۰۲

دفترچه شماره (۱)

صبح پنج‌شنبه

۱۴۰۱/۱۲/۱۱



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

«اگر دانشگاه اصلاح شود مملکت اصلاح می‌شود.»

امام خمینی (ره)

مهندسی فناوری اطلاعات (کد ۲۳۵۸)

زمان پاسخ‌گویی: ۱۳۵ 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 داده‌ها و طراحی الگوریتم‌ها) - شبکه (شبکه‌های کامپیوتری و امنیت شبکه) - مهندسی اطلاعات (پایگاه داده پیشرفته، بازیابی پیشرفته اطلاعات و داده‌کاوی) - 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 می‌باشد و با متخلفین برابر مقررات رفتار می‌شود.



تماس بگیرید. ۹۰۹۹۰۷۵۳۰۷
irantahsil.org

در صورت وجود هرگونه پرسش و ابهام با شماره
تماس از طریق تلفن ثابت

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

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

امضا:

مجموعه دروس تخصصی (حل مسئله (ساختمان داده‌ها و طراحی الگوریتم‌ها) - شبکه (شبکه‌های کامپیوتری و امنیت شبکه) - مهندسی اطلاعات (پایگاه داده پیشرفته، بازیابی پیشرفته اطلاعات و داده‌کاوی) - خدمات فناوری اطلاعات (تجارت الکترونیک و آموزش الکترونیکی)):

۱- الگوریتم فلوید - وارشال از یک الگوریتم برای حل مسئله کوتاه‌ترین مسیرهای تمام جفت رئوس در یک گراف جهت‌دار $G = (V, E)$ در زمان استفاده می‌کند.

(۱) حریمانه، $\Theta(v^3)$ (۲) حریمانه، $\Theta(V^2 \log E)$

(۳) برنامه‌نویسی پویا، $\Theta(v^3)$ (۴) برنامه‌نویسی پویا، $\Theta(V^2 \log E)$

۲- با فرض اینکه $P \neq NP$ باشد، کدام مورد درست است؟

(۱) $NP - hard = NP$ (۲) $NP - complete = P$

(۳) $NP - complete = NP$ (۴) $NP - complete \cap P = \emptyset$

۳- کمترین تعداد مقایسه مورد نیاز برای تعیین اینکه یک عدد صحیح بیش از $\frac{n}{4}$ مرتبه در یک آرایه مرتب از اعداد صحیح به طول n ظاهر می‌شود، از کدام مرتبه است؟

(۱) $\Theta(1)$ (۲) $\Theta(\log n)$

(۳) $\Theta(n)$ (۴) $\Theta(n \log n)$

۴- n آرایه نامرتب A_1, \dots, A_n را در نظر بگیرید (n عددی فرد است). هر کدام از این آرایه‌ها دارای n عنصر متمایز است. هیچ عنصر مشترکی میان هیچ دو آرایه‌ای وجود ندارد. کمترین پیچیدگی زمانی الگوریتمی برای محاسبه میانه این آرایه‌ها از چه مرتبه‌ای است؟

(۱) $\Theta(n)$ (۲) $\Theta(n \log n)$

(۳) $\Theta(n^2)$ (۴) $\Omega(n^2 \log n)$

۵- فرض کنید $W(n)$ و $A(n)$ ، به ترتیب، نشان‌دهنده بدترین حالت و میانگین زمان اجرای الگوریتم اجراشده بر روی ورودی با اندازه n باشند. کدام مورد همواره درست است؟

(۱) $A(n) = O(W(n))$ (۲) $A(n) = \Theta(W(n))$

(۳) $A(n) = \Omega(W(n))$ (۴) $A(n) = o(W(n))$

۶- یک آرایه مرتب‌شده از اعداد داریم. می‌خواهیم دو عدد در این آرایه پیدا کنیم که جمع آن دو عدد مساوی یک عدد داده‌شده x باشد. کمترین پیچیدگی زمانی حل این مسئله کدام است؟

(۱) $\Theta(n)$ (۲) $\Theta(n^2)$

(۳) $\Theta(\log n)$ (۴) $\Theta(n \log n)$

۷- فرض کنید آرایه‌ای از اعداد صحیح $A = [a_1; a_2; \dots; a_n]$ داده شود. فرض کنید یک اندیس (ناشناخته) k وجود دارد به طوری که زیر آرایه $A = [a_1; a_2; \dots; a_k]$ به ترتیب اکیداً افزایشی مرتب شده است و زیر آرایه $A = [a_k; a_{k+1}; \dots; a_n]$ به ترتیب اکیداً نزولی مرتب شده است (یعنی اگر $1 \leq i < j \leq k$ ، آنگاه $a_i < a_j$ ، و اگر $k \leq i < j \leq n$ ، آنگاه $a_i > a_j$ هدف شما تعیین k است. یک الگوریتم بهینه برای حل این مسئله چه زمان اجرایی دارد؟

$$\Theta(n \log n) \quad (۲) \qquad \Theta(n^2 \log n) \quad (۱)$$

$$\Theta(\log n) \quad (۴) \qquad \Theta(n) \quad (۳)$$

۸- کدام یک از موارد زیر درست است؟

(۱) آرایه $A = [۱۰; ۳; ۵; ۱; ۴; ۲]$ یک max heap است.

(۲) هر مسئله محاسباتی با اندازه ورودی n را می‌توان با یک الگوریتمی با زمان چندجمله‌ای بر حسب n حل کرد.

(۳) برای تمام توابع مثبت $f(n)$ ، $g(n)$ و $h(n)$ ، اگر $f(n) = O(g(n))$ و $f(n) = \Omega(h(n))$ باشد، آنگاه $g(n) + h(n) = \Omega(f(n))$ است.

(۴) اگر هر رقم جداگانه در RADIX SORT را با استفاده از INSERTION SORT به جای COUNTING SORT مرتب کنیم، آنگاه RADIX SORT به درستی کار نمی‌کند (یعنی خروجی صحیح را تولید نمی‌کند).

۹- کدام مورد زیر مطمئناً عبارت $f(n) = \Omega(g(n))$ را پشتیبانی می‌کند؟

$$f(n) \leq 4 \times g(n) \quad \text{برای تمام } n \geq 1 \quad (۱)$$

$$f(n) \geq 4 \times g(n) \quad \text{برای تمام } n \geq 136 \quad (۲)$$

$$f(n) \leq 4 \times g(n) \quad \text{برای تمام } n \geq 100 \quad (۳)$$

$$\lim_{n \rightarrow \infty} \frac{f(n)}{g(n)} = 0 \quad (۴)$$

۱۰- کدام یک از گزاره‌های زیر درست است؟

الف- اگر مسئله P_1 بتواند به مسئله P_2 در زمان خطی کاهش (reduce) یابد، آنگاه اگر P_2 یک مسئله NP-hard باشد، می‌توان نتیجه گرفت P_1 نیز NP-hard است.

ب- یک Clique در یک گراف بدون جهت لزوماً یک vertex cover در گراف مکمل نیست.

(۱) فقط گزاره «الف» درست است.

(۲) فقط گزاره «ب» درست است.

(۳) هر دو گزاره «الف» و «ب» درست است.

(۴) هر دو گزاره «الف» و «ب» نادرست است.

۱۱- کدام یک از گزاره‌های زیر درست است؟

الف- اینکه زمان حل یک مسئله P حد پایین $\Omega(n^2)$ دارد به این معنی است که برای هر الگوریتم A که P را حل می‌کند فقط برخی از نمونه‌های P وقتی به عنوان ورودی به A داده شوند، باعث می‌شود A زمان $\Omega(n^2)$ صرف کند.

ب- اینکه زمان حل یک مسئله P حد پایین $\Omega(n^2)$ دارد به این معنی است که برای هر الگوریتم A که P را حل می‌کند هر نمونه از P که به عنوان ورودی به A داده شود، باعث می‌شود A زمان $\Omega(n^2)$ صرف کند.

(۱) فقط گزاره «الف» درست است.

(۲) فقط گزاره «ب» درست است.

(۳) هر دو گزاره «الف» و «ب» درست هستند.

(۴) هر دو گزاره «الف» و «ب» نادرست هستند.

- ۱۲- کدام یک از گزاره‌های زیر درست است؟
- الف- اگر یک الگوریتم زمان چندجمله‌ای برای یک مسئله که NP-hard است ارائه شود، آنگاه می‌توان نتیجه گرفت $P = NP$ است.
- ب- اگر یک مسئله NP-complete است، آنگاه می‌توان نتیجه گرفت که آن مسئله هیچ راه‌حلی ندارد.
- (۱) فقط گزاره «الف» درست است.
- (۲) فقط گزاره «ب» درست است.
- (۳) هر دو گزاره «الف» و «ب» درست هستند.
- (۴) هر دو گزاره «الف» و «ب» نادرست هستند.
- ۱۳- یک مشتری پس از دانلود و مشاهده یک فایل html پایه از یک سایت، نیازمند دانلود سه فایل ۱۲۸ کیلوبایتی دیگر است. به‌ازای هر کدام از نحوه‌اتصالات زیر، مدت زمان دریافت سه فایل چقدر است؟ ($RTT = 10\text{ ms}$)، پهنای باند = ۱۰ مگابیت بر ثانیه و از اندازه بسته‌های TCP SYN / ACK و درخواست HTTP صرف‌نظر کنید.)

الف - درخواست‌های پشت‌سرهم، اتصالات nonpersistent TCP

ب - درخواست‌های موازی، اتصالات nonpersistent TCP

ج - درخواست‌های پشت‌سرهم، اتصالات persistent TCP

د - درخواست‌های موازی، اتصالات persistent TCP

(۱) الف: ۰/۳۶ - ب: ۰/۳۲ - ج: ۰/۳۴ - د: ۰/۳۲

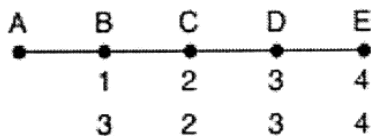
(۲) الف: ۰/۳۶ - ب: ۰/۲۲ - ج: ۰/۳۵ - د: ۰/۳۳

(۳) الف: ۰/۳۷ - ب: ۰/۳۲ - ج: ۰/۳۴ - د: ۰/۳۲

(۴) الف: ۰/۳۷ - ب: ۰/۲۲ - ج: ۰/۳۵ - د: ۰/۳۳

- ۱۴- یک اتصال TCP برقرار شده است که در آن $MSS = 1\text{ kB}$ و $RTT = 100\text{ ms}$ است. وقتی اندازه پنجره فرستنده برابر ۳۲ کیلوبایت است، یک timeout تشخیص داده می‌شود. چند میلی‌ثانیه طول می‌کشد که اندازه پنجره فرستنده برابر ۲۲ کیلوبایت شود؟
- (۱) ۶۰۰
- (۲) ۹۰۰
- (۳) ۱۰۰۰
- (۴) ۱۱۰۰

- ۱۵- در شبکه خطی زیر که شامل روترهای A تا E است از روش بردار فاصله برای مسیریابی استفاده می‌شود. تأخیر لینک بین هر دو روتر را یک واحد در نظر بگیرید. تأخیر همه روترها تا روتر A را قبل از خرابی روتر A در سطر اول و پس از خرابی روتر A را پس از اولین دور مبادله اطلاعات روترها به هم در سطر دوم مشاهده می‌نمایید. کدام یک از گزینه‌های زیر در مورد تأخیر روترها به روتر A پس از دور ششم مبادله اطلاعات درست است؟



(۱) $B = 5, C = 6, D = 5, E = 6$

(۲) $B = 7, C = 8, D = 7, E = 8$

(۳) $B = 7, C = 6, D = 7, E = 6$

(۴) $B = 9, C = 8, D = 9, E = 8$

- ۱۶- کدام یک از پروتکل‌های زیر انصافی که تقریباً شبیه انصاف نسبی است، را رعایت می‌کنند؟

(۱) UDP

(۲) TCP

(۳) CSMA / CD

(۴) MACA

۱۷- فرض کنید در محاسبات CRC مقسوم‌علیه 1011 و پیغام 100110111100 باشد. در کدگذاری به روش CRC پیغام ارسالی از سمت فرستنده کدام است؟

۱) 100110111100101

۲) 100110111100011

۳) 100110111100100

۴) 100110111100010

۱۸- این شکل مراحل ۵ و ۶ از پروتکل Kerberos v4 را نشان می‌دهد. در این شکل $E(K, .)$ نماد رمزنگاری با کلید K ، C نماد کلاینت، V نماد سرور، ID نماد شناسه، AD نماد آدرس (مثلاً $IP\ address$ و یا $MAC\ Address$) و TS نماد Timestamp یا همان مهر زمانی است. اگر کلاینت در $Authenticator_c$ به جای TS_5 از یک عدد تصادفی مانند N استفاده کند و سرور نیز در مرحله ۶، رمز شده $N+1$ را به کلاینت بفرستد، چه اتفاقی می‌افتد؟ (منظور جایگذاری N و $N+1$ دقیقاً در همان محل‌هایی است که TS_5 و TS_5+1 استفاده شده‌اند. تغییر دیگری در پروتکل داده نشده و به سرورها قابلیت و یا حافظه‌ای اضافه نگردیده است).

$$\begin{aligned} (5) \quad C \rightarrow V \quad & Ticket_v \parallel Authenticator_c \\ (6) \quad V \rightarrow C \quad & E(K_{c,v}, [TS_5 + 1]) \\ & Ticket_v = E(K_v, [K_{c,v} \parallel ID_C \parallel AD_C \parallel ID_v \parallel TS_4 \parallel Lifetime_4]) \\ & Authenticator_c = E(K_{c,v}, [ID_C \parallel AD_C \parallel TS_5]) \end{aligned}$$

۱) ایجاد مشکل امنیتی کرده و Replay Attack را امکان‌پذیر می‌کند.
 ۲) ایجاد مشکل امنیتی کرده و احراز هویت سرور V توسط کلاینت C را خدشه‌دار می‌کند.
 ۳) از نظر امنیتی هیچ مشکلی ایجاد نمی‌کند، چون همچنان جلوی Replay Attack گرفته می‌شود.
 ۴) از نظر امنیتی هیچ مشکلی ایجاد نمی‌کند، چون همچنان احراز هویت سرور V توسط کلاینت C انجام می‌شود.

۱۹- فرض کنید شما یک سیستم رمزنگاری RSA ساخته‌اید که در آن پیمانه (n) عدد 119 است. تعداد کلیدهای عمومی‌ای که می‌توانید برای این سیستم انتخاب کنید به کدام مورد نزدیک‌تر است؟

(راهنمایی: اگر m یک عدد نوعی صحیح مثبت باشد که به صورت $p_1^{e_1} p_2^{e_2} \dots p_k^{e_k}$ تجزیه و فاکتورگیری شود (که در آن p_i ها اعداد اول متمایز هستند)، آنگاه مقدار تابع فی اولر (یا همان Euler Totient Function) برای

$$\phi(m) = (p_1^{e_1} - p_1^{e_1-1}) (p_2^{e_2} - p_2^{e_2-1}) \dots (p_k^{e_k} - p_k^{e_k-1})$$

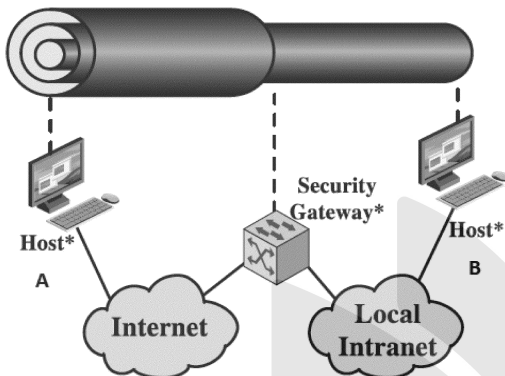
۱) 119

۲) 96

۳) 40

۴) 32

۲۰- این شکل را در IPSec در نظر بگیرید. این سناریو برای اتصال یک کامپیوتر A از راه دور و از طریق اینترنت به یک سرور B در شبکه سازمان از طریق مسیر یاب امنیتی لبه آن (Security Gateway) طراحی شده است. در این مورد خاص، کامپیوتر متصل شونده (A) از IP مسیر یاب لبه سازمان در اینترنت اطلاع دارد و خودش نیز دارای valid IP در اینترنت است. ضمناً A برای ارتباط با سرور مورد نظر که پشت NAT سازمان است نیز یک IP دیگر در subnet سازمان دارد. رنج IP های کامپیوترهای سازمان invalid بوده و از بیرون قابل مسیریابی نیستند. بیرونی ترین (SA) IPSec Security Association که بین کامپیوتر A و Gateway ایجاد می شود در چه مودی باید باشد (فرض کنید پروتکل ESP است)؟ و در صورتی که A به کامپیوترهای شبکه Local Intranet سازمان اعتماد نداشته باشد، برای آنکه بسته وی با کمترین سربار به نحوی محافظت شود که تمام محتوا رمز شده و نیز محتوا و header بسته در برابر دستکاری محافظت شوند، بهترین مود و ترتیب استفاده از پروتکل های IPSec در SA های درونی کدام است؟

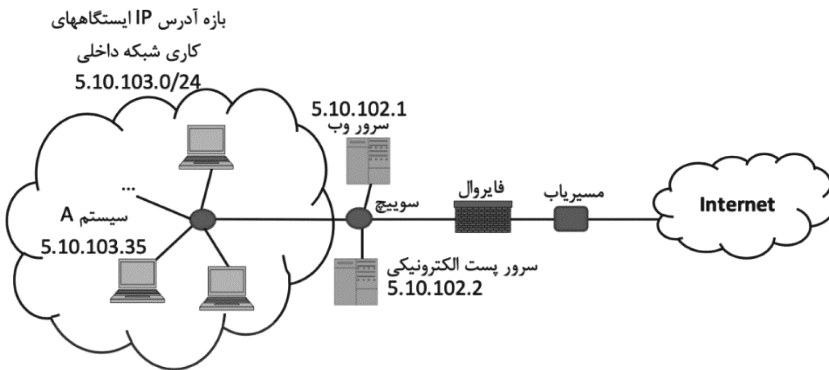


- ۱) بیرونی ترین SA باید در مود Tunnel باشد و دو SA درونی باید به شکل Iterated Tunneling باشند که اول پروتکل AH و سپس ESP به بسته اعمال شود.
- ۲) بیرونی ترین SA باید در مود Transport باشد و دو SA درونی باید به شکل Transport Adjacency باشند که اول پروتکل ESP و سپس AH به بسته اعمال شود.
- ۳) بیرونی ترین SA باید در مود Transport باشد و دو SA درونی باید به شکل Iterated Tunneling باشند که اول پروتکل AH و سپس ESP به بسته اعمال شود.
- ۴) بیرونی ترین SA باید در مود Tunnel باشد و دو SA درونی باید به شکل Transport Adjacency باشند که اول پروتکل ESP و سپس AH به بسته اعمال شود.

۲۱- کدام مورد در خصوص امضای دیجیتال و زیرساخت کلید عمومی (PKI) درست است؟

- ۱) در صورت استفاده از الگوریتم RSA برای امضاء، دو پیام یکسان دارای امضاهای متفاوت هستند ولیکن در صورت استفاده از استاندارد امضای دیجیتال DSS چنین خاصیتی برقرار نیست.
- ۲) در لیست گواهی های باطل شده (CRL) نیازی به درج همه گواهی های باطل شده نیست و فقط کافی است گواهی های باطل شده ولی منقضی نشده (از لحاظ زمان اعتبار) را نگهداری کنیم.
- ۳) با استفاده از امضای دیجیتال می توان سرویس عدم انکار فرستنده یک پیام و عدم نقض صحت (یکپارچگی) پیام را در شبکه فراهم کرد، ولی نمی توان سرویس احراز اصالت پیام (message authentication) را فراهم کرد.
- ۴) در صورت ابطال گواهی مرکز صدور گواهی ریشه (root CA)، گواهی های مراکز میانی (intermediate CA) صادر شده توسط مرکز ریشه (با کلید متناظر با گواهی باطل شده) غیر معتبر می شود، ولیکن گواهی های صادر شده توسط مراکز صدور گواهی میانی برای کاربران نهایی همچنان معتبر است.

۲۲- اگر قواعد مندرج در جدول زیر در فایروال حالت‌مند موجود در شبکه‌ای با هم‌بندی زیر تنظیم شده باشد، کدام مورد درست است؟



شماره پورت	سرویس
80	http
443	https
25	email (smtp)
53	dns

Scr-IP	Src-Port	Dst-IP	Dst-Port	Protocol	Connection State	Action
5.10.103.35	Any	Any	Any	Any	Any	Reject
Any	Any	5.10.102.1	443	TCP	New, Established	Accept
5.10.102.1	443	Any	Any	TCP	Established	Accept
5.10.103.0/24	Any	Any	80,443,25	TCP	New, Established	Accept
Any	80,443,25	5.10.103.0/24	Any	TCP	Established	Accept
Any	Any	Any	Any	ICMP	Any	Accept
Any	Any	Any	Any	Any	Any	Reject

(۱) سیستم A می‌تواند به سرویس‌های http، https و smtp در اینترنت فقط اتصال جدید برقرار کند.
 (۲) امکان ping کردن سرورهای وب و پست الکترونیکی (با آدرس‌های 5.10.102.1 و 5.10.102.2) از اینترنت وجود ندارد.

(۳) اگر در شبکه داخلی سرویس DNS نداشته باشیم، کاربران شبکه داخلی در دسترسی به وبسایت‌ها در اینترنت از طریق URL آنها با مشکل مواجه خواهند شد.

(۴) سرور وب شبکه داخلی (با آدرس 5.10.102.1) هم می‌تواند به کاربران اینترنتی سرویس بدهد و هم خود می‌تواند به وبسرویس یک سازمان بیرونی که بر روی اینترنت سرویس‌دهی می‌کند متصل شود و سرویس دریافت نماید.

۲۳- دو تراکنش T_i و T_{i-1} را در نظر بگیرید ($TS(T_i) > TS(T_{i-1})$). ما می‌خواهیم این دو تراکنش را به صورت هم‌روند با پروتکل اعتبارسنجی (Validation protocol) اجرا کنیم. نوشتن مجموعه داده‌های تراکنش T_{i-1} با خواندن مجموعه داده‌های T_i اشتراکی ندارد و با فرض اینکه مقدار مهرهای زمانی (Timestamp) به صورت زیر است. در این خصوص کدام مورد درست است؟

$$Start(T_{i-1}) < Start(T_i) < Validation(T_i) < Finish(T_i) < Validation(T_{i-1}) < Finish(T_{i-1})$$

(۱) تراکنش T_{i-1} نمی‌تواند اجرا شود و abort می‌شود.

(۲) تراکنش T_i نمی‌تواند اجرا شود و abort می‌شود.

(۳) هر دو تراکنش به درستی و بدون abort و بدون بن‌بست اجرا می‌شوند.

(۴) هیچ‌یک از تراکنش‌ها abort نمی‌شوند و باعث ایجاد بن‌بست می‌شوند.

۲۴- پروتکل کامیت دو مرحله‌ای (2PC) را به همراه ترمیم Undo/Redo با قانون WAL را در نظر بگیرید. فرض کنید که سیستمی داریم که در آن شکست فقط شامل متوقف شدن میزبان‌ها است به طوری که لاگ و دیسک سالم می‌ماند و پس از آن سیستم (احتمالاً) ریپوت می‌شود و هیچ پیامی در شبکه گم نمی‌شود. فرض کنید که یک هماهنگ‌کننده (Coordinator) به نام C و دو شرکت‌کننده P1 و P2 داریم. فرض کنید دنباله‌ای از رویدادها به صورت زیر داریم:

C sends Prepare Transaction T1 to P1, P2
P1 sends Ready to C
P2 sends Abort to C

پیام بعدی که ارسال می‌شود کدام است؟

C sends Abort T1 to P1, P2 (۱)

C sends Commit T1 to P1, P2 (۲)

C Aborts T1 and no message is sent. (۳)

C sends Commit T1 to P1 and Abort T1 to P2 (۴)

۲۵- اگر برای ترمیم از یک طرح ترمیم فقط UNDO استفاده شود (یعنی برای ترمیم پایگاه داده فقط نیاز به UNDO است و نیازی به REDO نیست)، آنگاه کدام یک از سیاست‌های مدیریت بافر اعمال شده است؟

STEAL/NO-FORCE (۲)

STEAL/FORCE (۱)

NO-STEAL/FORCE (۴)

NO-STEAL/NO-FORCE (۳)

۲۶- اگر DBMS از کنترل همروندی مبتنی بر مهرزمان سختگیرانه (با قاعده نوشتن توماس) استفاده کند، با اجرای تراکنش‌ها مطابق طرح زیر چه اتفاقی می‌افتد؟

$ST_1 \rightarrow ST_2 \rightarrow ST_3 \rightarrow ST_4 \rightarrow R_1(X) \rightarrow R_2(X) \rightarrow W_2(X) \rightarrow W_1(X) \rightarrow W_3(Y) \rightarrow W_2(Y) \rightarrow C_3 \rightarrow W_4(Z) \rightarrow C_4 \rightarrow R_2(Z)$

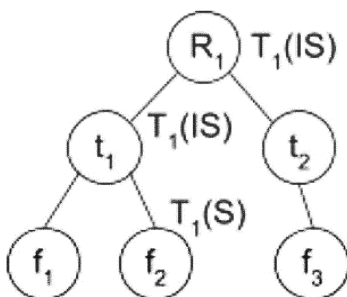
(۲) تراکنش T_1 و T_2 طرد می‌شوند.

(۱) فقط تراکنش T_2 طرد می‌شود.

(۴) هیچ تراکنشی طرد نمی‌شود.

(۳) فقط تراکنش T_1 طرد می‌شود.

۲۷- در پایگاه داده زیر با قفل‌گذاری سلسله‌مراتبی، تراکنش T_1 قفل‌هایی را گرفته است که در شکل مشخص شده است. کدام یک از تراکنش‌های زیر نمی‌تواند قفل‌هایی را که نیاز دارد، دریافت کند؟



(۱) تراکنش T_5 : درج یک فرزند برای t_2

(۲) تراکنش T_3 : درخواست نوشتن t_2

(۳) تراکنش T_2 : درخواست نوشتن t_1

(۴) تراکنش T_4 : درخواست خواندن f_2 و نوشتن f_1

۲۸- یکی از ایده‌هایی که Cleverdon برای ارزیابی سیستم‌های بازیابی اطلاعات مطرح کرده است، توانایی سیستم در عدم بازیابی اسناد نامرتب است. چه تعداد از معیارهای زیر این توانایی را دارند؟

F1 •

Precision •

Recall •

Fallout •

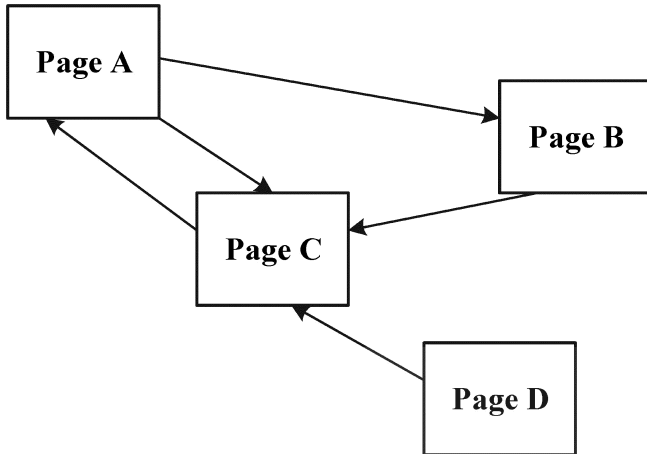
۲ (۲)

۱ (۱)

۴ (۴)

۳ (۳)

۲۹- شکل زیر، چند صفحه وب و ارتباط‌های آنها با هم را نشان می‌دهد. رتبه PageRank کدام صفحه بزرگ‌تر است؟



- D (۱)
- C (۲)
- B (۳)
- A (۴)

۳۰- یکی از روش‌های پاسخ به پرس‌وجوهای متغیر (Wild card or * query) استفاده از اندیس‌های جایگشتی (Permuterm index) است. عیب عمده این روش کدام است؟

- (۱) ساختار داده لازم برای پیاده‌سازی آن پیچیده‌تر است.
 - (۲) خطاهای املایی، پسوندها و پیشوندها را به خوبی پوشش نمی‌دهد.
 - (۳) افزودن یا حذف نمودن اسناد به این ساختار بسیار پیچیده‌تر از Posting list پایه است.
 - (۴) واژه‌نامه بسیار بزرگی ایجاد می‌کند که سبب افزایش هزینه محاسباتی پردازش پرس‌وجوها می‌شود.
- ۳۱- چه تعداد عبارت زیر در مورد مدل بازیابی (Robertson & Sparck Jones) RSJ درست است؟
- یک مدل بازیابی احتمالاتی است.
 - این مدل فقط حضور و عدم حضور ترم‌ها را در نظر می‌گیرد.
 - اگر از این مدل بازیابی استفاده کنیم، امکان relevance feedback نیز فراهم است.
 - برای به‌کارگیری این مدل حتماً باید Relevance Judgments در اختیار داشته باشیم.

- (۱) ۴
- (۲) ۳
- (۳) ۲
- (۴) ۱

۳۲- نتیجه طبقه‌بندی یک مجموعه داده در جدول زیر آمده است. کلاس‌های اختصاص یافته شامل Low و Medium و High هستند. برای طبقه Low، مقدار دقت (Precision) و بازخوانی (Recall) به ترتیب، (از راست به چپ) کدام است؟

		طبقه پیش‌بینی شده		
		LOW	MEDIUM	HIGH
طبقه واقعی	LOW	۲۰۰	۱۰۰	۱۰۰
	MEDIUM	۵۰	۱۰۰	۵۰
	HIGH	۵۰	۵۰	۳۰۰

- (۱) ۰/۶۷ - ۰/۵
- (۲) ۰/۵ - ۰/۶۷
- (۳) ۰/۶ - ۰/۶
- (۴) ۰/۶۷ - ۰/۶۷

- ۳۳- چه تعداد از عبارات زیر در مورد الگوریتم‌های خوشه‌بندی درست است؟
- DIANA از نوع خوشه‌بندی‌های Hierarchical است.
 - CLARA از نوع خوشه‌بندی‌های Density-Based است.
 - الگوریتم K-Means روی داده‌های به فرم محدب بهتر عمل می‌کند.
 - پیچیدگی محاسباتی الگوریتم K-Medoids بیشتر از K-Means است.
 - K-Means از الگوریتم K-Medoids به داده‌های پرت بیشتر حساس است.
 - پیچیدگی زمانی K-Means وقتی که تعداد کل نمونه‌ها برابر n و تعداد گام‌های یادگیری برابر t باشد، از درجه $O(tKn)$ است.

- (۱) پنج
(۲) چهار
(۳) سه
(۴) دو

- ۳۴- فرض کنیم در یک مسئله از نوع Classification، تعداد کلاس برابر n باشد. در این صورت بیشترین مقدار Entropy در چه شرایطی به دست می‌آید؟
- (۱) $n = 2$ و توزیع در ۲ کلاس متوازن باشد.
(۲) $n = 4$ و توزیع در ۴ کلاس متوازن باشد.
(۳) $n = 2$ و توزیع در ۲ کلاس نامتوازن باشد.
(۴) $n = 4$ و توزیع در ۴ کلاس نامتوازن باشد.

- ۳۵- فرض کنید مجموعه C شامل تمامی frequent closed itemsets و مجموعه M شامل تمامی maximal frequent itemsets، روی مجموعه داده D را در اختیار داریم. همچنین مقدار support هر itemset موجود در C و M را نیز داریم. در این صورت چند عبارت زیر درست است؟
- برای هر itemset دلخواه می‌توان تعداد تکرار آن را از روی C به دست آورد.
 - برای هر itemset دلخواه می‌توان تعداد تکرار آن را از روی M به دست آورد.
 - برای هر itemset دلخواه می‌توان از روی C مشخص کرد که frequent است یا خیر.
 - برای هر itemset دلخواه می‌توان از روی M مشخص کرد که frequent است یا خیر.

- (۱) یک
(۲) دو
(۳) سه
(۴) چهار

- ۳۶- کدام مورد، مراحل فرایند تصمیم‌گیری مصرف‌کننده را به درستی نشان می‌دهد؟
- (۱) خواندن نظرات مصرف‌کنندگان در سایت‌ها، مشاهده تبلیغات، خرید
(۲) تشخیص نیاز، جستجو، ارزیابی گزینه‌ها، خرید، رفتار پس از خرید
(۳) فرهنگ‌سازی، برندسازی، رفتار در حین خرید، تحلیل رفتار مصرف‌کننده
(۴) ارزیابی و مقایسه گزینه‌ها، جستجو در موتورهای جستجو، دریافت ایمیل‌های تبلیغاتی؛ خدمات پس از فروش
- ۳۷- کدام یک از موارد زیر، متشکل از نهادها یا انجمن‌هایی است که به نوعی نقش راهبری و حاکمیت اینترنت را برعهده دارند؟

- (۱) SSL, IXP, ISOC
(۲) HTTP, W3C, IETF
(۳) ISP, ICANN, W3C
(۴) ICANN, W3C, IETF

- ۳۸- کدام مورد، به ترتیب، نشان‌دهنده یک نمونه مدل کسب‌وکار (Business model) از نوع B2B و B2C است؟
- (۱) شبکه صنعتی خصوصی - بورس
(۲) پرتال - تدارکات الکترونیکی
(۳) تولید محتوا - خرده‌فروشی الکترونیکی
(۴) توزیع‌کننده الکترونیکی - تدارکات الکترونیکی

۳۹- کدام مورد در خصوص تفاوت بین تجارت الکترونیکی (e-Commerce) و کسب و کار الکترونیکی (e-Business) درست است؟

(۱) هر دو به مفهوم یکسانی اشاره دارند و به جای یکدیگر به کار می‌روند.
 (۲) تجارت الکترونیکی هر نوع تراکنش و دادوستدی را شامل می‌شود و می‌توان آن را حالت عام‌تری از کسب و کار الکترونیکی دانست.

(۳) کسب و کار الکترونیکی به هر نوع فعالیتی که بین دو شرکت انجام شود گفته می‌شود، درحالی‌که تجارت الکترونیکی لزوماً بین شرکت‌ها و اشخاص انجام می‌شود.

(۴) کسب و کار الکترونیکی به بهره‌گیری از توانمندسازهای دیجیتال در اجرای فرایندها و تراکنش‌ها در داخل شرکت می‌پردازد، ولی تجارت الکترونیکی به تراکنش‌های تجاری بین شرکت‌ها و بین شرکت‌ها و اشخاص می‌پردازد.

۴۰- کدام یک از موارد زیر، تماماً جزو ویژگی‌های منحصر به فرد تجارت الکترونیکی به شمار می‌آید؟

- (۱) محتوای غنی، شخصی‌سازی، شبکه‌های اجتماعی، بانکداری اینترنتی
 - (۲) دسترسی به بازارهای محلی، تولید محتوا توسط کاربران، استانداردهای جهانی
 - (۳) تولید و طراحی محصولات دانش‌بنیان، فراگیری خدمات، شبکه‌های اجتماعی
 - (۴) دسترسی به بازارهای جهانی، فناوری اجتماعی، تعامل‌پذیری، فراگیری خدمات
- ۴۱- تولید ایده‌های جدید و مفید و حل مسائل ناشناخته به کدام یک از انواع مهارت‌های تفکر زیر نزدیک‌تر است؟

- (۱) فرا ادراک
- (۲) تفکر انتقادی
- (۳) تفکر نوآورانه
- (۴) تفکر ایستا

۴۲- کدام مورد، نشان‌دهنده لایه‌های مدل نظریه ادراکی یادگیری چند رسانه‌ای است؟

- (۱) مشاهده، ادراک، افزایش دانش، آموزش به دیگران
- (۲) ارائه چندرسانه‌ای، حواس، حافظه فعال، حافظه طولانی‌مدت
- (۳) حافظه کوتاه‌مدت، حافظه بلندمدت، ضمیر ناخودآگاه، دانش پیش‌زمینه
- (۴) انتخاب کانال چندرسانه‌ای، ارائه مطالب در کانال انتخابی، تأثیرگذاری بر ذهنیت مخاطبین، نهادینه‌سازی مطالب آموزشی

۴۳- در کدام یک از روش‌های یادگیری زیر، سهم مشارکت ذهنی بیش از مشارکت رفتاری است؟

- (۱) پیاده‌کردن صدای ضبط‌شده کلاس
- (۲) هایلایت کردن مطالب
- (۳) یادداشت‌برداری و خلاصه‌نویسی
- (۴) جزوه‌نویسی

۴۴- کدام مورد در خصوص اندازه گروه‌ها در یادگیری گروهی (تعاملی) درست است؟

(۱) اندازه بزرگ‌تر گروه‌ها، باعث می‌شود به‌جای اینکه توان ذهنی افراد صرف هماهنگی‌های روابط بین افراد شود، صرف حل مسئله شود.

(۲) هر قدر اندازه گروه‌ها بزرگ‌تر باشد، امکان بحث و تبادل نظر بیشتر شده و اثربخشی بیشتری دارد.

(۳) هر قدر اندازه گروه بیشتر شود، امکان تقسیم‌کار عادلانه بین اعضا بیشتر فراهم می‌شود.

(۴) گروه‌هایی با اندازه ۲ تا ۵ نفر، بهترین نتیجه را دربردارد.

۴۵- کدام مورد از نظر اصول یادگیری الکترونیکی درست است؟

(۱) بهتر است متن مربوط به یک تصویر در صفحه جداگانه ارائه شود تا به یادآوری مطالب و یادگیری بهتر کمک کند.

(۲) یادگیرنده از کانال ادراکی یکسانی برای درک صوت و تصویر استفاده می‌کند.

(۳) بهتر است از ترکیب تصویر و صوت به‌جای تصویر و متن استفاده شود.

(۴) کانال ادراکی متن و تصویر در یادگیرنده مجزا است.

