CONCURSO PÚBLICO DE PROVAS E TÍTULOS PARA O CARGO EFETIVO DE PROFESSOR DA CARREIRA DE MAGISTÉRIO SUPERIOR

EDITAL Nº 42/2016 – PROGRAD

PROVA ESCRITA

Área de concurso: 6 – Informática

Número de Identificação do(a) Candidato(a): _____

Orientações Gerais

1. A prova escrita tem **caráter eliminatório e classificatório**;
2. A prova escrita **está sendo realizada simultaneamente** por todos os candidatos;
3. O horário de realização da prova escrita é das **8h às 12h** (horário oficial do Acre);
4. O **candidato deverá permanecer obrigatoriamente** na sala de realização da prova escrita por, no mínimo, uma hora após o seu início;
5. Quando autorizado pelo Fiscal de Sala o candidato deverá preencher a área de concurso e o número de identificação do candidato na folha de rosto do caderno de resposta definitivo;
6. Será **anulada a prova** que contiver assinatura, rubrica, qualquer palavra ou marca que identifique o candidato, exceto o número de identificação fornecido pela Comissão Geral de Concurso no local indicado;
7. Nenhuma folha desta prova ou do rascunho poderá ser destacada, sob pena de desclassificação do candidato;
8. Utilize a(s) **folha(s) definitiva(s) de resposta** para responder a(s) questão(s) formuladas;
9. A prova escrita será feita pelo próprio candidato, à mão, em letra legível, com **caneta esferográfica de tinta de cor azul ou preta, fabricada em material transparente, em espaço destinado para tanto**;
10. As **anotações que estiverem em desconformidade** com este Edital ou com as instruções da prova escrita serão consideradas indevidas e não serão consideradas para efeito de correção;
11. O candidato **não deverá amassar, molhar, dobrar, rasgar, manchar** ou, de qualquer modo, **danificar a sua prova escrita**, sob pena de impossibilitar a leitura por parte dos membros da banca examinadora;
12. **Em hipótese alguma haverá substituição** da prova escrita por erro do candidato;
13. Não serão distribuídas folhas suplementares para transcrição das respostas definitivas ou para rascunho.
14. **Não serão permitidas consultas e a utilização de qualquer equipamento eletrônico, durante a realização da prova escrita**, exceto aquelas solicitadas pela banca examinadora e autorizadas pela Comissão Geral de Concurso, em edital específico, no endereço eletrônico <www.ufac.br>.
15. Será desclassificado o candidato que, durante a realização da prova escrita, for surpreendido portando, em local diverso do indicado pelos fiscais, equipamento eletrônico e/ou material de uso não autorizado, ainda que desligado.
16. De igual forma, será desclassificado o candidato cujo equipamento eletrônico e/ou material de uso não autorizado emitir qualquer tipo de ruído, alerta ou vibração, ainda que o mesmo esteja no local indicado pelos fiscais.
17. Após o término de sua prova, o candidato deverá entregar a(s) folha(a) definitiva(a) de resposta e as folhas de rascunho ao fiscal de sala.

18. O candidato que **entregar a prova não poderá retornar** ao local de sua realização em hipótese alguma;
19. Os **três últimos candidatos deverão permanecer na sala de prova** e somente poderão sair juntos do recinto, após acompanhar o lacre dos envelopes e apor em Ata suas respectivas assinaturas;
20. Os resultados da prova escrita serão publicados pela Comissão Geral de Concurso, no **dia 13 de março de 2017**, em edital de resultado preliminar, juntamente com as chaves de correção das provas;

Questões

1. Na *Hierarquia de Chomsky*, as linguagens do tipo 3 (conhecidas, também, como linguagens regulares) são estudadas por meio de três formalismos, a saber: os *reconhecedores* dessas linguagens, chamados de **autômato finitos**; os *denotadores* dessas linguagens, chamados de **expressões regulares**; e os *geradores* dessas linguagens, chamados de **gramáticas regulares**. Sabendo que $\mathfrak{L} = \{x(yy)^m z \mid x, y, z \in \Sigma \text{ e } x \neq y \text{ e } y \neq z \text{ e } m \geq 1\}$ sobre $\Sigma = \{a, b, c\}$ é uma linguagem regular, construa três formalismos capazes de, respectivamente, reconhecer, denotar e gerar a linguagem $\mathfrak{L}$.

2. Nos sistemas operacionais, os processos são estudados levando-se em consideração um **modelo de processo**, este modelo estabelece um conjunto de estados possíveis para cada processo e um conjunto de transições possíveis entre estes estados. Descreva estes estados e suas transições, apresentando uma figura para resumir diagramaticamente sua reposta.

3. Segundo John F. Sowa “Em lógica, o quantificador existencial $\exists$ é a notação para afirmar que alguma coisa existe. Contudo, a própria lógica não tem nenhum vocabulário para descrever coisas que existem. A ontologia preenche esse vazio: ela é o estudo da existência, de todos os tipos de entidades – abstratas e concretas – que formam o mundo (...)”. Essa afirmação demonstra a importância do desenvolvimento de uma antologia na representação de conhecimento.

   (a) Defina o que é uma ontologia e explique seus componentes básicos.

   (b) Exemplifique esses componentes utilizando um domínio simples.

4. Sistemas de Apoio (ou suporte) a Decisão (SAD) são ferramentas e modelos analíticos para analisar grandes quantidades de dados e fornecer uma interface de consultas interativas de apoio para gerentes de nível médio que enfrentam situações de decisões semiestruturadas. Descreva os componentes de um SAD e como os mesmos podem ser utilizados para auxiliar na tomada de decisões.

5. Considerando a figura 1 (partes **a** e **b**), que ilustra dois mecanismos de segurança que podem utilizar criptografia de chaves públicas, resolva os seguintes enunciados:

   (a) Explique o que é a criptografia de chaves públicas.

   (b) Indique e explique os dois mecanismos ilustrados.

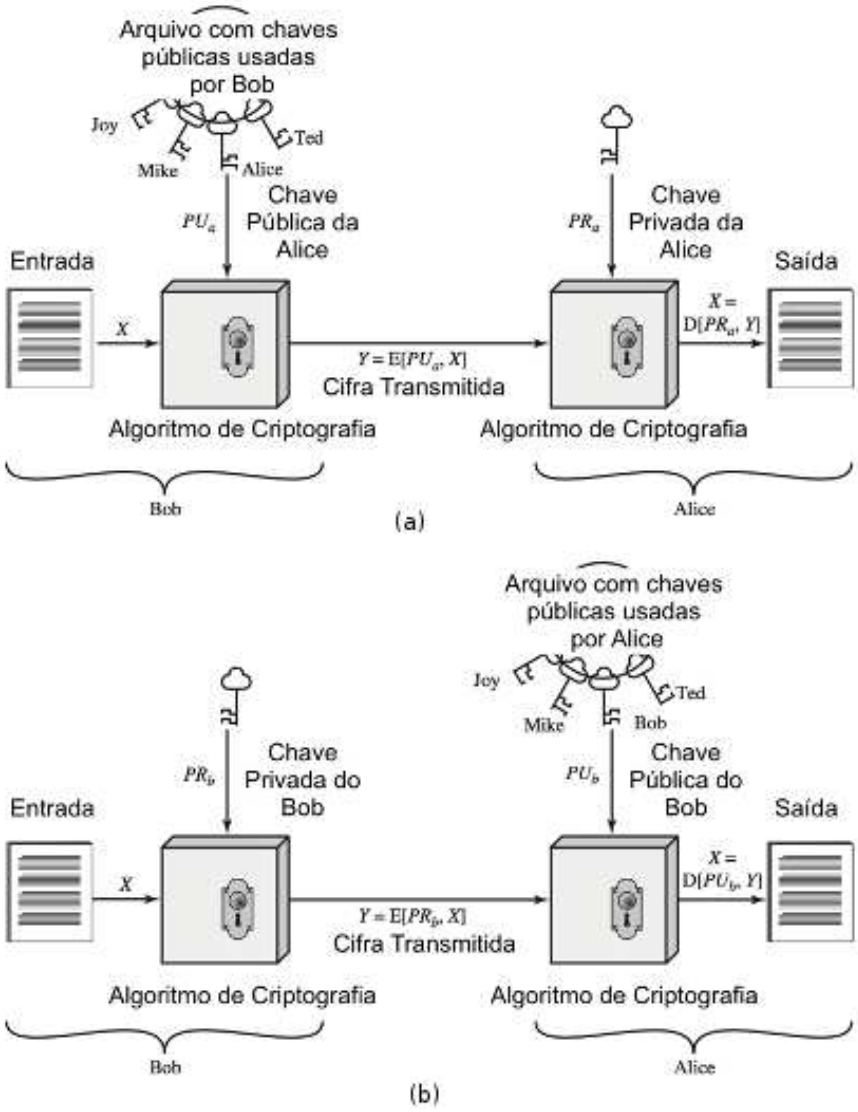

Figura 1: Mecanismos de segurança.

CONCURSO PÚBLICO DE PROVAS E TÍTULOS PARA O CARGO EFETIVO DE PROFESSOR DA CARREIRA DE MAGISTÉRIO SUPERIOR
EDITAL Nº 42/2016 – PROGRAD
FOLHA DEFINITIVA DE RESPOSTA

Área: 6 – Informática **Número de Identificação**: _____

1.	
2.	
3.	
4.	
5.	
6.	
7.	
8.	
9.	
10.	
11.	
12.	
13.	
14.	
15.	
16.	
17.	
18.	
19.	
20.	
21.	
22.	
23.	
24.	
25.	
26.	
27.	
28.	
29.	
30.	

CONCURSO PÚBLICO DE PROVAS E TÍTULOS PARA O CARGO EFETIVO DE PROFESSOR DA CARREIRA DE MAGISTÉRIO SUPERIOR
EDITAL Nº 42/2016 – PROGRAD
FOLHA DE RASCUNHO

1.	
2.	
3.	
4.	
5.	
6.	
7.	
8.	
9.	
10.	
11.	
12.	
13.	
14.	
15.	
16.	
17.	
18.	
19.	
20.	
21.	
22.	
23.	
24.	
25.	
26.	
27.	
28.	
29.	
30.	

Respostas

Questão 1

a) Autômato finito não determinístico: Vide figuras 2 e 3.

δ	a	b	c
$\rightarrow q_0$	$\{q_1, q_3\}$	$\{q_2, q_3\}$	$\{q_1, q_2\}$
q_1	$\emptyset$	$\{q_4\}$	$\emptyset$
q_2	$\{q_5\}$	$\emptyset$	$\emptyset$
q_3	$\emptyset$	$\emptyset$	$\{q_6\}$
q_4	$\emptyset$	$\{q_7\}$	$\emptyset$
q_5	$\{q_8\}$	$\emptyset$	$\emptyset$
q_6	$\emptyset$	$\emptyset$	$\{q_9\}$
q_7	$\{q_{10}\}$	$\{q_4\}$	$\{q_{10}\}$
q_8	$\{q_5\}$	$\{q_{10}\}$	$\{q_{10}\}$
q_9	$\{q_{10}\}$	$\{q_{10}\}$	$\{q_6\}$
(q_{10})	$\emptyset$	$\emptyset$	$\emptyset$

Figura 2: Forma tabular do autômato.

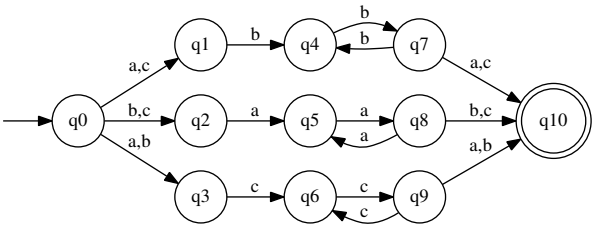

Figura 3: Forma gráfica do autômato.

b) Expressão regular:
$((a+c)bb(bb)^*(a+c)) + ((a+b)cc(cc)^*(a+b)) + ((b+c)aa(aa)^*(b+c))$

c) Gramática regular:
$G = (\{S, A, B, C\}, \{a, b, c\}, P, S)$, onde:
$P = \{S \rightarrow aB|aC|bA|bC|cB|cA,$
$B \rightarrow bbB|bbc|bba,$
$C \rightarrow ccC|ccb|cca,$
$A \rightarrow aaA|aac|aab\}$

Questão 2

No modelo de processo, em questão, os estados possíveis para um processo são listados a seguir e as transições entre eles são enumeradas a seguir, sendo que e a figura 4 resume diagramaticamente esses elementos.

Estados possíveis de um processo são:

- **Em execução**, neste estado o processo está realmente usando o processador;
- **Pronto**, neste estado o processo está aguardando sua vez para usar o processador;
- **Bloqueado**, neste estado o processo está esperando um evento externo, como uma operação de entrada/saída;

As transições possíveis entre os estados listados, acima, são:

1. Esta transição ocorre quando o processo está em execução e descobre que não tem mais condições lógicas de continuar sua execução, ficando bloqueado;
2. Esta transição ocorre quando o processo está em execução e o escalonador decide que é hora de outro processo usar o processador, ficando pronto para esperar a sua vez;
3. Esta transição ocorre quando o processo está pronto e o escalonador decide que é sua hora de usar o processador, entrando em execução;
4. Esta transição ocorre quando o processo está bloqueado e o evento externo pelo qual ele estava aguardando acontece, ficando pronto para esperar a sua vez;

Figura 4: Estados e transições de um processo.

Questão 3

Uma ontologia é uma descrição explícita formal de conceitos em um domínio de conhecimento (classes e suas relações), das propriedades de cada conceito descrevendo suas várias características e atributos (*slots*, papéis ou propriedades) e das facetas (restrições sobre *slots*). Uma ontologia e um conjunto de instâncias individuais de classes constituem uma base de conhecimento.

As **classes** são o foco principal da maioria das ontologias. Elas descrevem conceitos em um domínio. Por exemplo, uma classe Vinho representa todos os vinhos. Vinhos específicos são instâncias dessa classe, como, por exemplo, o Bordeaux. Uma classe pode ter subclasses que representam conceitos que são mais específicos que uma superclasse. Por exemplo, podemos dividir a classe de todos os vinhos em tinto, branco ou rosé. Podemos dividi-los também em espumante e não-espumante.

Slots, papéis ou propriedades descrevem as características de classes e instâncias. Por exemplo, o vinho Château Lafite Rothschild Pauillac é encorpado e produzido na vinícola Château Lafite Rothschild. Nele, temos dois *slots* que o descrevem: o corpo, com valor encorpado, e o fabricante, com o valor Château Lafite Rothschild. No nível de classe, podemos dizer que instâncias da classe Vinho tem *slots* descrevendo seu sabor, corpo, nível de açúcar e fabricante.

As **facetas** descrevem os tipos de valores, valores permitidos, cardinalidade e outras características que um *slot* pode ter. Por exemplo, um *slot* nome (nome do vinho) é uma string. Assim como o *slot* corpo só pode ter um único valor (um vinho só pode ter um tipo de corpo).

Na correção não será cobrada a utilização desse mesmo exemplo na chave de resposta. Contudo, o domínio escolhido pelo candidato deve ser adequadamente utilizado para exemplificar os componentes básicos da ontologia.

Questão 4

Os componentes de um SAD e como podem ser utilizados para auxiliar na tomada de decisões são descritos a seguir:

- **Banco de dados SAD** – é uma coletânea de dados correntes ou históricos provenientes de uma série de aplicaÇões. Os dados do banco de dados SAD são extratos ou cópias de banco de dados em produção. Os dados provenientes do banco de dados SAD serão utilizados pelos outros componentes para auxiliar a tomada de decisão.
- **Sistema de software SAD** – Ferramentas de softwares empregadas para análise dos dados provenientes do banco de dados SAD. Pode utilizar várias ferramentas OLAP, mineração de dados e modelos matemáticos e analíticos para auxiliar na tomada de decisão. Este componente pode estar ou não integrado aos componentes abaixo.
- Um dos principais componentes dos SAD são os **modelos**, que são representações abstratas de componentes de um fenômeno, podendo ser modelos estatísticos, de otimização, previsão, análise de sensibilidade, entre outros. Os modelos são uma das formas que os SAD tem para inferir fenômenos futuros, o que pode ter grande valia na tomada de decisão.
- **Relatórios** – Outro componente importante dos SAD são os módulos responsáveis pela geração de relatórios, que são componentes de informação compilada pelos modelos e que devem ser apresentados para os tomadores de decisão, levando a escolhas melhor informadas.

Questão 5

A criptografia de chaves públicas é assimétrica, envolvendo o uso de duas chaves separadas. Seus principais componentes são a entrada (*Plaintext*), o algoritmo de criptografia, as chaves públicas e privadas, a cifra transmitida (*Ciphertext*) e o algoritmo de decriptografia (o mesmo de criptografia em ordem inversa).

Os passos principais são:

1. Cada usuário gera um par de chaves para serem usadas na criptografia e decriptografia.
2. Cada usuário coloca uma das chaves em um registro público e mantém a outra em segredo. Como mostrado na figura 1(a), cada usuário mantém uma coleção de chaves públicas obtidas de outros usuários.
3. Se o Bob precisa enviar uma mensagem privada para a Alice, ele criptografa a mensagem usando a chave pública de Alice.
4. Quando a Alice recebe a mensagem, ela a decifra usando sua chave privada. Nenhuma outra chave pode ser usada para decifrá-la.

Logo, na Figura 1(a), o mecanismo garante a **confidencialidade**.

A figura 1(b) demonstra outra forma de operação da criptografia de chave pública. Nesse esquema, um usuário criptografa os dados usando sua própria chave privada. Qualquer um que saiba sua chave pública poderá decifrar a mensagem. Nesse caso, o mecanismo garante a **autenticidade** do usuário, pois apenas ele tem acesso a sua chave privada.

Com o objetivo de contornar o alto custo dos sistemas de criptografia de chaves públicas, os sistemas de segurança a utilizam apenas para a criptografia das chaves criptográficas dos algoritmos de chaves simétricas (AES, 3DES, etc.). Após a troca de chaves, o algoritmo simétrico, que é mais rápido, passa a ser utilizado para a confidencialidade das mensagens.