Sistemas Distribuídos, 2018/19
2º MINI Teste

Todas as perguntas têm a mesma cotação. Escolha apenas uma resposta em cada alínea.
Cada resposta de escolha múltipla errada desconta 1/4 da sua cotação.
No caso de encontrar mais do que uma resposta certa, escolha a que faz a afirmação mais forte.

Número: _____ Nome: _____

1) Uma falta arbitrária (ou bizantina) acontece:
   A. Quando o componente pode exibir qualquer comportamento.
   B. Quando o componente pára e não responde a nenhum estímulo externo.
   C. Quando o componente recebe uma determinada sequência de entradas (*inputs*).
   D. Quando o componente continua a funcionar mas demora muito a responder.

2) No modelo de sistema assíncrono.
   A. Os pressupostos aproximam-se mais da realidade do que num sistema síncrono, em particular se houver uma partição na rede, ou um ataque de "denial-of-service".
   B. É possível a deteção remota de falhas por paragem (*crash failures*).
   C. Pode considerar-se a existência de um limite superior no tempo de latência da rede.
   D. Nenhuma das anteriores é válida.

3) Suponha que no seu projeto em produção durante 1 ano, dois servidores falharam (e foram repostos corretamente em funcionamento os seus substitutos). Na situação de falta o tempo médio da troca primário-secundário observado pelos clientes foi de 10 minutos.

   A. Disponibilidade = $\frac{(365 \times 24 \times 60 - 10)}{365 \times 24 \times 60}$

   B. Disponibilidade = $\frac{(365 \times 24 \times 60 - 20)}{365 \times 24 \times 60}$

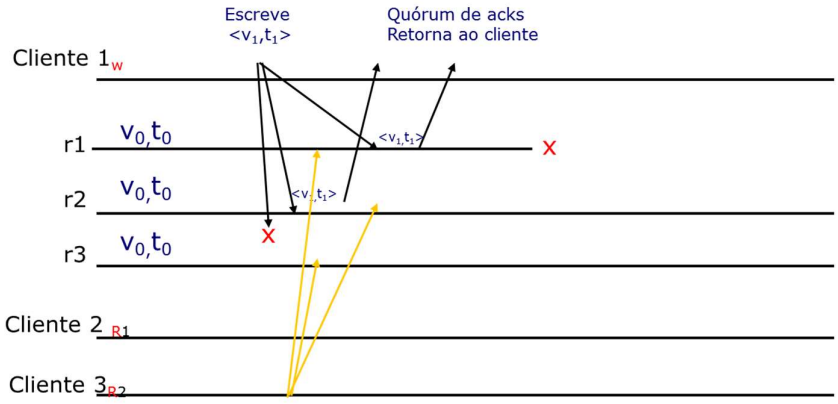
   C. Disponibilidade = $\frac{\left(\frac{365 \times 24 \times 60}{2} - 10\right)}{365 \times 24 \times 60}$

   D. MTBF dos servidores = $\frac{20}{365 \times 24 \times 60}$

4) Num sistema de 3 réplicas que usa o protocolo quorum consensus (pesos idênticos, quóruns de maioria), o estado das réplicas num dado instante é o seguinte (seq – sequence number, cid – client identifier):
Réplica A: valor = 18; tag = {seq=5, client-id=1}
Réplica B: valor = 15; tag = {seq=6, client-id=4}
Réplica C: valor = 13; tag = {seq=7, client-id=5}
   A. Este estado não é possível neste protocolo.
   B. Há pelo menos uma escrita que está ainda em curso.
   C. Ocorreram escritas concorrentes.
   D. Nenhuma das anteriores.

5) Em sistemas replicados com quorum consensus, o uso de pesos variáveis nas réplicas faz sentido se:
   A. Um sub-conjunto de réplicas for mais fiável ou rápido que as restantes.
   B. A frequência de escritas no sistema for superior à percentagem de leituras.
   C. Se pretender tolerar falhas bizantinas.
   D. A frequência de leituras no sistema for superior à percentagem de escritas.

6) Considere o seguinte diagrama de um protocolo de quóruns de maioria com 3 réplicas ativas. As setas representam mensagens enviadas.



   A. Perante o esquema o Cliente 3 vai ler V0 porque dois dos servidores têm este valor.
   B. O cliente vai sempre ler V1 porque tem o contador mais elevado.
   C. Se R2 responde o resultado é V1.
   D. O diagrama não está correto porque se a mensagem de escrita não chegou a R3 então este tem de ficar em falha silenciosa.

7) Com a cifra assimétrica RSA é possível:
   A) Cifrar com a chave pública, decifrar com a chave privada.
   B) Cifrar com a chave privada, decifrar com a chave pública.
   C) Combinar com função de resumo para construir assinaturas digitais.
   D) Todas as anteriores.

8) Um certificado digital de chave pública confiável deve conter, pelo menos:
   A) A chave pública da entidade.
   B) A chave pública e o nome da entidade certificada.
   C) O par de chaves da entidade certificada.
   D) A chave pública, o nome da entidade certificada e a assinatura de uma autoridade de certificação.

9) Uma chave pública RSA é guardada num certificado em formato X.509.
   A. A data de validade do certificado é o que garante que a chave pública não foi adulterada.
   B. Para poder guardar a chave em ficheiro é necessário usar o formato X.509.
   C. A assinatura do certificado é opcional e não acrescenta garantias de segurança.
   D. O mais importante é que a chave pública e restante informação seja assinada por uma CA de confiança.

10) Considere uma entidade A cujo par de chaves de cifra assimétrica foi criado pela entidade certificadora CA. Verificou-se que a entidade não é confiável e lhe deveria ser inibido o uso do certificado.
   A) A CA muda a sua chave pública para que o certificado deixe de ser válido
   B) A CA invalida o certificado e deixa de responder a pedidos do certificado de A
   C) O certificado da entidade A deve ser acrescentado à blacklist (lista negra) da CA
   D) A CA informa os detentores de certificados que já não são válidos

11) Qual a principal desvantagem da cifra simétrica que torna atrativa a cifra híbrida?
   A) Mau desempenho da cifra simétrica.
   B) Dificuldade de distribuição de chaves públicas.
   C) Dificuldade de distribuição de chaves secretas.
   D) Chaves de grande dimensão.

12) $\{X\}_Y$ $\{M\}_Z$

Suponha que a Alice (A) quer enviar uma mensagem M ao Bob (B) de forma confidencial, num sistema de cifra híbrida. Escolha as chaves que deveriam ser usadas na expressão acima, de entre as diversas opções:
   A) $X= K_{A,B}$; $Y= K_{PB}$; $Z= K_{PB}$
   B) $X= K_{A,B}$; $Y= K_{PA}$; $Z= K_{A,B}$
   C) $X= K_{A,B}$; $Y= K_{PB}$; $Z= K_{A,B}$
   D) $X= K_{PB}$; $Y= K_{PA}$; $Z= K_{A,B}$

1	2	3	4	5	6	7	8	9	10	11	12	Total
1,67	1,67	1,67	1,67	1,67	1,67	1,67	1,67	1,67	1,67	1,67	1,67	**20**

AABBACDDDCCC