Sistemas Distribuídos, 2014/2015
1º MINI Teste – 8 de Maio de 2015

Todas as perguntas têm a mesma cotação. Escolha apenas uma resposta em cada alínea.
Cada resposta de escolha múltipla errada desconta 1/3 da sua cotação.
No caso de encontrar mais do que uma resposta certa, escolha a que faz a afirmação mais forte.

Número: _____ Nome:_____

1) Em Kerberos, um cliente que tenha solicitado um ticket para uma sessão com um dado serviço S deve enviar esse ticket junto com a invocação que faça a S?
   a) É falso. O ticket nunca é entregue a S.
   b) Sim, pois o ticket permite a S descobrir a chave da sessão com C.
   c) Sim, pois o ticket permite a S descobrir a chave secreta de C.
   d) Sim, pois anexar o ticket aos pedidos que C envia em claro a S garante que esses pedidos são transmitidos de forma segura.

2) Compare um ticket Kerberos com um ticket Needham-Schroeder:
   a) São iguais.
   b) Um ticket Kerberos inclui marcas temporais (timestamps), o que não é verdade no Needham-Schroeder
   c) O ticket Kerberos é enviado em claro, enquanto que o ticket Needham-Schroeder é cifrado com a chave do servidor.
   d) O ticket Kerberos é entregue pelo cliente ao servidor, no Needham-Schroeder é o servidor de autenticação que o entrega.

3) Um bom algoritmo de cifra:
   a) O algoritmo deve ser secreto.
   b) A interface do algoritmo deve ser secreta.
   c) Precisa ser totalmente seguro.
   d) Nenhuma das anteriores.

4) Assuma que a Alice e o Bob queriam dialogar de forma segura usando cifra simétrica, para tal o segundo gerava uma chave secreta. A distribuição da chave secreta para a Alice teria de ser feita assegurando quais requisitos?
   a. Apenas confidencialidade da chave secreta.
   b. Apenas autenticidade e Integridade da chave secreta
   c. Autenticidade, Integridade e Confidencialidade da chave secreta.
   d. Nenhum dos anteriores.

5) Quando uma memória avaria de tal forma que um "bit" de uma determinada palavra ficou posicionado a "1"independentemente do valor que é escrito, diz-se que:
   a) Ocorreu um erro, mas não necessariamente uma falta
   b) Ocorreu uma falha, mas não necessariamente uma falta
   c) Ocorreu uma falta, mas não necessariamente um erro
   d) Nenhuma das anteriores

6) Um pressuposto dos protocolos de replicação é o comportamento da rede, que pode ser síncrono ou assíncrono.
   a) O protocolo de primary backup ensinado nas aulas teóricas tolera qualquer um dos comportamentos.
   b) O protocolo de quóruns tolera qualquer um dos comportamentos.
   c) A replicação activa com rede assíncrona implica f+1 réplicas, sendo f o número de falhas silenciosas simultâneas.
   d) Com um *timeout* suficientemente longo consegue-se detectar a falta de omissão das mensagens em qualquer dos comportamentos.

7) Considere o seguinte situação numa réplica de X:

Valor	Sequência	Client-id/pid
23	260	10

   E que esta recebe um write (X, val=45, seq=260, cliente=25).

   a) Não executa, pois o número de sequência é já 260.
   b) Não executa porque o número de cliente é diferente e tinha que ser igual.
   c) Executa e altera o valor.
   d) Esta situação não é possível porque a escrita é precedida de uma leitura e logo a sequência é sempre incrementada.

8) Usando o protocolo Quorum Consensus, um sistema com 3 réplicas, quóruns de maioria, pesos uniformes, tem o seguinte estado nas réplicas: R1 <val=10, <seq=4, pid=2>>, R2 <val=15, <seq=4, pid=1>>, R2 <val=15, <seq=4, pid=1>>,
   Neste instante, um cliente inicia um pedido de leitura. Que valor(es) pode a leitura devolver?
   a) Devolve garantidamente 10.
   b) Devolve garantidamente 15.
   c) Pode devolver 10 ou 15, dependendo das respostas recebidas.
   d) Devolve um valor que nem é 10 nem 15.