Sistemas Distribuídos, 2017/18 - 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 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. O mais importante é que a chave pública e restante informação seja assinada por uma CA de confiança.
   C. Para poder guardar a chave em ficheiro é necessário usar o formato X.509.
   D. A assinatura do certificado é opcional e não acrescenta garantias de segurança.

   [ ]

2) Considere que o um Web Service recebeu a seguinte mensagem SOAP:
   <S:Envelope xmlns:S="http://schemas.xmlsoap.org/soap/envelope/" >
   <S:Header><S:Sender> test-client</S:Sender><S:Signature> WyILHtlM0jeO71txDud/14vTxcUNpMdn3g+L/EqTiJ…
   ==</S:Signature></S:Header>
   <S:Body><ns2:sayHello xmlns:ns2="http://ws.example/"><arg0>friend</arg0></ns2:sayHello></S:Body></S:Envelope>

   O que fazer para verificar a autenticidade e integridade da mensagem?
   A. Decifrar assinatura com chave pública do emissor, calcular resumo de toda a mensagem, comparar valores obtidos para ver que são iguais.
   B. Decifrar assinatura com chave privada do recetor, calcular resumo de toda a mensagem, comparar valores obtidos para ver que são iguais.
   C. Decifrar assinatura com chave pública do emissor, calcular resumo de toda a mensagem exceto o elemento Signature, comparar valores obtidos para ver que são iguais.
   D. Nenhuma das anteriores.

   [ ]

3) Numa determinada máquina, pretende-se cifrar um documento com dimensão de N bytes com cifra assimétrica usando uma chave pública. Considere que:
   - O desempenho da cifra assimétrica é 1 Megabyte/s e o da cifra simétrica é 1 Gigabyte/s ;
   - Um bloco de cifra assimétrica tem a dimensão S, e um bloco de cifra simétrica tem a mesma dimensão;
   - Uma chave simétrica cabe sempre num único bloco de cifra assimétrica.

   Tendo em vista o desempenho global da operação de cifra:
   A. A utilização de cifra híbrida em vez de cifra assimétrica compensa sempre, independentemente de N.
   B. O uso de cifra híbrida é igual ao da cifra assimétrica caso N > S
   C. O uso de cifra híbrida é melhor que cifra assimétrica caso N > S
   D. A utilização de cifra híbrida é indiferente para o desempenho.

   [ ]

4) Considere o algoritmo DES que foi utilizado para cifrar um documento eletrónico. Um ataque de força-bruta para ler o documento:
   A. É impossível.
   B. Não é possível em tempo útil.
   C. Não é possível com custo razoável.
   D. É possível em tempo útil e com um custo razoável.

   [ ]

5) A Ana e o Bernardo não se conhecem mas pretendem comunicar entre si através de uma rede insegura. Para o protocolo de segurança vão recorrer à cifra assimétrica RSA. O Bernardo envia a seguinte mensagem à Ana e ela depois responde com a mensagem seguinte:

B->A: $K_{pub}B$
A->B: $\{M\}K_{pub}B$
onde: M é a mensagem, {} representa cifra

A. O Bernardo pode usar a sua chave privada para decifrar a mensagem e ver que não foi alterada.
B. O Bernardo pode usar a sua chave privada para ter a garantia que só ele consegue ter acesso ao conteúdo da mensagem.
C. A Ana tem a certeza que apenas o verdadeiro Bernardo vai poder ler a mensagem.
D. O Bernardo pode usar a sua chave privada para confirmar que foi a verdadeira Ana que enviou a mensagem.

6) O Coordenador 2PC quando recebe um pedido de CloseTransaction deve:
A. Enviar CanCommit? a todos os Participantes.
B. Enviar doCommit a todos os Participantes.
C. Enviar doAbort a todos os Participantes.
D. Consultar o *log* para verificar quais foram os votos dos Participantes e decidir o desfecho da transação.

7) Quando um cliente a executar uma transação distribuída pretende que a mesma seja abortada, o coordenador tem de executar o protocolo 2PC (em duas fases) para cumprir esse pedido?
a) Sim.
b) Não, nesse caso basta ao coordenador enviar a ordem de abortar numa única fase.
c) Não, nesse caso o coordenador não é envolvido.
d) Não é permitido ao cliente pedir para abortar a transação que já iniciou.

8) O Participante 2PC se receber um *timeout* no estado Inicial:
A. Tem obrigatoriamente que aguardar ordem do Coordenador.
B. Pode optar por cancelar a transação de forma unilateral.
C. Deve consultar outro Participante para decidirem em conjunto o desfecho da transação.
D. Pode passar ao estado Preparado.

1	2	3	4	5	6	7	8	**Total**
2,5	2,5	2,5	2,5	2,5	2,5	2,5	2,5	**20**
B	C	C	D	B	A	B	B	