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) Qual a combinação de vantagens que torna atrativa a cifra híbrida?
   A. Só a cifra simétrica permite garantir confidencialidade, só a cifra assimétrica permite garantir integridade.
   B. O bom desempenho da cifra assimétrica com a facilidade de distribuição de chaves secretas.
   C. O bom desempenho da cifra simétrica com a facilidade de distribuição de chaves públicas.
   D. Nenhuma das anteriores.

   [ ]

2) A Ana e o Bruno não se conhecem mas pretendem comunicar entre si através de uma rede insegura. Para o protocolo de segurança vão recorrer à cifra assimétrica RSA. A Ana envia ao Bruno a seguinte mensagem e anexos:
   M , $\{D(M)\}K_{priv}A$, $K_{pub}A$
   onde: M é a mensagem, D é uma função de resumo criptográfico, {} representa cifra

   A. O Bruno pode usar a sua chave pública para validar que a mensagem não foi alterada.
   B. O Bruno pode usar a sua chave privada para validar que a mensagem se destina apenas a ele.
   C. O Bruno pode usar a chave pública que recebeu para validar que a mensagem foi enviada pela Ana.
   D. O Bruno pode usar a chave pública que recebeu para validar que a mensagem não foi alterada, mas não sabe se foi a Ana que enviou.

   [ ]

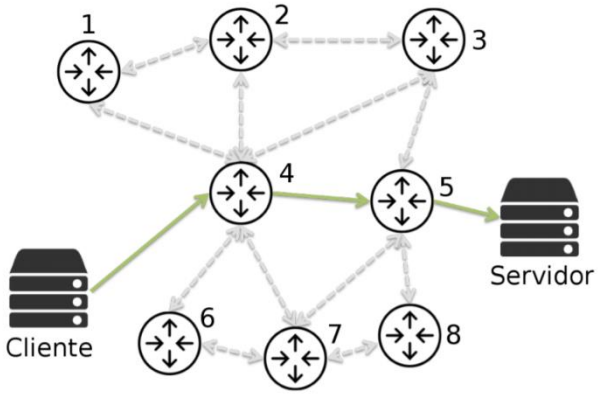
3) O Bob recebeu uma mensagem M da Alice, à qual vinha anexada uma assinatura digital de chave pública. Para validar a assinatura, o Bob deve:
   A. Decifrar a assinatura digital usando a chave pública da Alice, gerar o resumo (digest) de M, e comparar se ambos os resultados são iguais.
   B. Decifrar M com a chave privada do Bob, gerar o resumo do resultado e ver se é igual à assinatura digital.
   C. Gerar o resumo (digest) de M e ver se é igual à assinatura digital.
   D. Gerar o resumo (digest) de M, cifrá-lo com a chave pública da Alice e ver se é igual à assinatura digital.

   [ ]

4) Considere o algoritmo AES-128 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. B e C

   [ ]

5) Considere o seguinte diagrama de rede. O cliente e o servidor comunicam através de HTTP, na Internet.
A ligação em curso segue o seguinte caminho: Cliente -> Router 4 -> Router 5 -> Servidor



A. Um ataque *man-in-the-middle* pode ser realizado nos nós 4 ou 5.
B. Um ataque *man-in-the-middle* pode ser realizado apenas no nó 4.
C. Um ataque *man-in-the-middle* pode ser realizado apenas no nó 5.
D. Um ataque *man-in-the-middle* já não pode ser feito porque a ligação já está estabelecida.

6) Pode um participante abortar a sua transação local antes de receber a ordem doAbort do coordenador?
A. Sim, mal envie o seu voto NÃO ao coordenador.
B. Sim, caso passe um tempo máximo desde que a transação iniciou sem ter recebido mais mensagens do coordenador .
C. Ambas as alíneas acima.
D. Não, não pode.

7) O Participante 2PC, ao expirar o seu *timeout* quando está ainda 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.

8) O protocolo 2-Phase Commit (2PC) recorre a *timeouts* no seu funcionamento. Isso implica que:
A. O 2PC só pode ser usado em sistemas em que o tempo máximo de propagação é bem conhecido.
B. O 2PC pode levar a que uma transação aborte caso uma mensagem se atrase, mesmo que nenhum dos intervenientes tenha falhado.
C. O 2PC só pode ser usado em sistemas em que os relógios dos participantes e coordenador são perfeitamente sincronizados.
D. Nenhuma das anteriores.

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**
C	**D**	**A**	**D**	**A**	**C**	**B**	**B**	