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) 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 que 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 pior que a cifra assimétrica caso N <= S
   C. O uso de cifra híbrida é igual ao da cifra assimétrica caso N <= S
   D. A utilização de cifra híbrida é indiferente para o desempenho.

   [ ]

2) 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.

   [ ]

3) Um emissor envia um datagrama UDP, através de uma rede insegura, para um recetor:
   M="depositMoney(1000)" , $\{D(M)\}K_{privEmissor}$
   onde: M é a mensagem, D é uma função de resumo criptográfico, {} representa cifra

   A transmissão pode ser capturada e retransmitida mais tarde por um atacante.
   Para evitar o ataque:

   A. A transmissão necessita de incluir uma marca temporal (*timestamp*) física, que deve ser incluída na mensagem e no resumo, e os relógios de emissor e recetor devem estar razoavelmente sincronizados.
   B. O recetor precisa de comparar para saber se já recebeu uma mensagem igual a M no passado.
   C. Opção A e adicionalmente o recetor tem que confirmar que o *timestamp* é recente.
   D. O recetor consegue detetar o ataque através do *checksum* do datagrama UDP.

   [ ]

4) Considere a seguinte mensagem SOAP:
<S:Envelope xmlns:S="http://schemas.xmlsoap.org/soap/envelope/" ><S:Header />
<S:Body><n2:sayHello xmlns:n2="http://ws.org/"><arg0>friend</arg0></n2:sayHello></S:Body></S:Envelope>

O que deve adicionar para proteger **apenas** a autenticidade e integridade da mensagem?

A. Cabeçalho com resumo dos cabeçalhos da mensagem cifrado com chave privada do emissor.
B. Cabeçalho com cifra total do corpo com a chave privada do emissor.
C. Cabeçalho com certificado digital do emissor.
D. Cabeçalho com resumo do corpo da mensagem cifrado com chave privada do emissor.

5) Um certificado da entidade A é uma estrutura de informação

A. Que tem a chave secreta de A
B. Que tem a chave pública de A, sendo assinada com a chave pública de uma CA
C. Que tem a chave pública de A, sendo assinada com a chave secreta de A
D. Que tem uma definição do prazo de validade e a chave pública de A

6) Um cliente a executar uma transação distribuída chamou a operação closeTransaction(true) para que a transação seja confirmada. Numa situação sem falhas nem atrasos, no momento da chamada:

A. Os participantes serão contactados pela primeira vez no âmbito desta transação distribuída.
B. Cada participante tem uma transação local iniciada e com alguns acessos executados.
C. Cada participante já executou e confirmou a sua transação local.
D. O coordenador vai executar uma transação local.

7) Pode um participante confirmar a sua transação local antes de receber a ordem doCommit do coordenador?

A. Sim, mal envie o seu voto SIM ao coordenador.
B. Sim, caso passe um tempo máximo desde que a transação iniciou sem que a decisão final tenha chegado.
C. Ambas as alíneas acima.
D. Não, não pode.

8) Ao longo da execução de uma transação distribuída, qual/quais destas operações podem levar a transação a abortar?

A. Invocações sobre os Participantes que não respondem.
B. Chamar CloseTransaction.
C. Chamar AbortTransaction.
D. Todas as 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**
B	**B**	**C**	**D**	**D**	**B**	**D**	**D**	