Sistemas Distribuídos, 2015/2016
1º MINI Teste

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) Qual frase está ERRADA em relação à propriedade de unicidade referencial dos nomes:
   a) É biunívoca: um nome só deve estar associado a um objeto e um objeto só pode ter um nome
   b) É fundamental para poder descriminar o objeto na identificação
   c) É fundamental para poder localizar o objeto
   d) Deve ser assegurada na criação do nome

   [ ]

2) Nomes hierárquicos:
   a) Permitem assegurar unicidade referencial mais facilmente em redes de grande escala.
   b) São necessariamente homogéneos.
   c) São necessariamente de âmbito global.
   d) Todas as anteriores.

   [ ]

3) Considere o seguinte fragmento de um schema XML. Pode considerar-se que esta definição:

```
<xsd:element name="department" >
   <xsd:simpleType>
       <xsd:restriction base="xsd:string>
   <xsd:pattern value="[0-9]{3}-[0-9]{3}-[0-9]{4}"/>
     </xsd:restriction>
 </xsd:simpleType>
</xsd:element>
:
```

   a) Define as regras para construção do elemento XML correspondente ao departamento
   b) Não define nenhuma regra a que os nomes têm de obedecer
   c) Define um espaço de nomes.
   d) Os espaços de nomes apenas são definidos por entidades de normalização (*standard bodies*)

   [ ]

4) Considere os conceitos de política e mecanismo de segurança:
   a) Os mecanismos de segurança definem a política de segurança.
   b) As políticas de segurança podem ser asseguradas por uma utilização adequada de mecanismos de segurança.
   c) Mesmo que os mecanismos de segurança tenham falhas, a política de segurança está assegurada.
   d) As políticas de segurança servem apenas para documentar os mecanismos de segurança.

   [ ]

5) Com a cifra simétrica AES é possível:
   a) Cifrar informação textual
   b) Cifrar informação binária
   c) Cifrar informação de tamanho arbitrário
   d) Todas as anteriores.

   [ ]

6) A cifra por blocos com realimentação (por exemplo, o AES CBC) permite:
   a) Aumentar a velocidade de cifra.
   b) Acertar o tamanho do último bloco a cifrar.
   c) Ter blocos de cifra de tamanho variável.
   d) Esconder os padrões dos blocos cifrados.

7) Uma capacidade Amoeba pode ser usada para **autorização** de ações e tem a seguinte estrutura:
   porto do servidor, número do objeto, direitos e campo de verificação.
   Qual é a função do campo de verificação?
   a) É um 'checksum' dos campos anteriores.
   b) É um resumo criptográfico (digest) dos campos anteriores.
   c) É um contador (número de capacidade emitida).
   d) É um número aleatório secreto que permite proteger a capacidade de ser forjada.

8) Pretende-se fazer a distribuição manual de **chaves assimétricas** de modo a permitir que três entidades – Alice, Bob e Charlie - se possam autenticar entre si. Cada entidade conhece a sua chave privada respetiva. Deve distribuir as chaves públicas da seguinte forma:
   a) As chaves públicas não são necessárias para autenticar.
   b) Alice deve ter chave pública de B e C; Bob deve ter chave pública A e C; Charlie deve ter chave pública A e B.
   c) Alice deve ter o resumo da chave pública de B e C, Bob deve ter o resumo da chave pública de A e C; Charlie deve ter o resumo da chave pública de A e B
   d) Alice, Bob e Charlie devem partilhar entre si uma chave simétrica secreta.

9) Comparando o protocolo Needham-Schroeder e o Kerberos analisado nas teóricas, qual das seguintes é verdadeira?
   a) O Kerberos usa exclusivamente em cifra assimétrica, enquanto que o Needham-Schroeder é em simétrica.
   b) O objetivo do Kerberos é entregar a chave de longa duração do cliente ao serviço, enquanto que o Needham-Schroeder distribui uma chave de sessão.
   c) O Kerberos assume relógios sincronizados, enquanto que o Needham-Schroeder não.
   d) No Kerberos, o Saut conhece as chaves secretas dos utilizadores; no Needham-Schroeder, o Saut não conhece qualquer segredo dos utilizadores.

10) 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.

11) Um JAX-WS SOAP Handler pode ser usado para cifrar mensagens SOAP, da seguinte forma:
   a) Cifrar o conteúdo numa mensagem à saída, decifrar numa mensagem à chegada.
   b) Resumir e cifrar o resumo da mensagem à saída, decifrar o resumo e comparar com novo resumo à chegada.
   c) Comprimir mensagem à saída, descomprimir à chegada.
   d) Produzir uma assinatura digital à saída, verificar a assinatura digital à chegada.

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