Sistemas Distribuídos, 2016/17
1º MINI Teste

Todas as perguntas têm a mesma cotação. Escolha apenas uma resposta em cada alínea.
Cada resposta de escolha múltipla errada desconta 1/4 da sua cotação.
No caso de encontrar mais do que uma resposta certa, escolha a que faz a afirmação mais forte.

Número: _____ Nome: _____

1) Considere o extrato de uma secção de um programa na IDL de SunRPC, o nome do programa é:

```
program BANCOPROG {
  version BANCOVERS {
    criarOut CRIAR(criarIn) = 1;
  } = 1;
} = 0x20000004;
```

A. Nome global numa rede que utiliza o SUN-RPC.
B. Nome impuro.
C. Nome local numa rede que utiliza o SUN-RPC.
D. Não é na realidade um nome porque não é garantida pelo sistema a unicidade referencial.

[ ]

2) Considere o nome "`rmi://rmi.tecnico.pt/sd`", que identifica um objeto remoto em Java RMI.
A componente "`sd`" identifica:
A. A máquina onde está alojado o RMI registry onde o objeto remoto está registado.
B. A máquina onde o objeto remoto está instanciado.
C. A máquina cliente.
D. Nenhuma das anteriores.

[ ]

3) Considere o URI referido pelo atributo *location* da etiqueta soap:address, no extrato seguinte de um WSDL:

```
<wsdl:service name="MediatorService">
    <wsdl:port name="MediatorPort" binding="tns:MediatorSoapBinding">
          <soap:address location="http://localhost:8080/mediator-ws"/>
    </wsdl:port>
</wsdl:service>
```

A. É um *namespace.*
B. É um nome que tem de ser traduzido no UDDI.
C. É usado para identificar o servidor.
D. É um nome impuro.

[ ]

4) Relativamente à TCB de um sistema informático:
A. A TCB não tem defeitos de programação (*bugs*).
B. A TCB deve englobar a maior parte do sistema.
C. A TCB identifica os utilizadores reconhecidos no sistema.
D. A TCB deve conter o conjunto mínimo de mecanismos que permitem implementar políticas de segurança.

[ ]

5) A cifra por blocos com realimentação permite:
A. Ter blocos de cifra de tamanho variável.
B. Aumentar a velocidade de cifra.
C. Esconder os padrões dos blocos cifrados.
D. Acertar o tamanho do último bloco a cifrar.

[ ]

6) No protocolo de Needham-Schroeder com criptografia simétrica, qual é a função dos valores N:
   A. São chaves de cifra.
   B. Manter uma contagem do número total de autenticações já efetuadas.
   C. São resumos das mensagens trocadas entre cliente e servidor.
   D. Impedir ataques por repetição de mensagens.

7) $\{K_X\}_{K_{PB}}$ $\{M\}_{K_x}$

   Suponha que a Alice (A) quer enviar uma mensagem para Bob (B) num canal confidencial, usando o esquema de cifra descrito acima, cujos componentes devem reconhecer.
   A. K_x deve ser substituído por KS_A
   B. K_x deve ser substituído por K_{AB}
   C. K_x deve ser substituído por KP_A
   D. Falta a função de resumo na expressão.

8) Qual a principal desvantagem da cifra assimétrica que torna atrativa a cifra híbrida?
   A. Mau desempenho da cifra assimétrica.
   B. Dificuldade de distribuição de chaves públicas.
   C. Dificuldade de distribuição de chaves secretas.
   D. Chaves de grande dimensão.

9) 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.

10) 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 excepto o elemento Signature, comparar valores obtidos para ver que são iguais.
   D. Nenhuma das anteriores.

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