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 uma interface remota em SUN RPC identificada pelo par PROGRAM, VERSION = 1898, 1:
   A. Este nome é puro e homogéneo.
   B. Este nome é impuro e homogéneo.
   C. Este nome é puro e heterogéneo.
   D. Este nome é impuro e heterogéneo.

   [ ]

2) Considere o nome "`rmi://rmi.tecnico.pt/objsd`", que identifica um objeto remoto em Java RMI.
   A componente "`rmi.tecnico.pt`" 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 extrato de uma secção do WSDL, o URI referido pelo atributo `targetNamespace`

```
<wsdl:definitions name="SdStore"
    targetNamespace="urn:pt:ulisboa:tecnico:sdis:store:ws"
```

   A. É usado para identificar.
   B. É um nome que tem de ser traduzido no UDDI
   C. É o URL do serviço.
   D. É um URL que permite localizar o WSDL.

   [ ]

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

   [ ]

5) Um atacante passivo na rede:
   A. Está geograficamente fixo num dado local.
   B. Escuta e insere novas mensagens na rede.
   C. Escuta apenas as mensagens cifradas.
   D. Escuta todas as mensagens mas não introduz novas mensagens na rede.

   [ ]

6) A cifra AES em modo CBC é:
   A. Uma cifra simétrica por blocos sem realimentação.
   B. Uma cifra simétrica por blocos com realimentação que permite esconder padrões.
   C. Uma cifra simétrica que expõe padrões entre blocos de texto em claro e respetivos blocos de texto cifrado.
   D. Uma cifra assimétrica contínua que permite esconder padrões.

   [ ]

7) 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.

8) 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.

9) 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:Header>
<S:**Body**><CipherBody>WyILHtlM0jeO71tx/14vTxcUNpMdn3g+L/EqTiJ… ==</CipherBody></S:Body></S:Envelope>

   A cifra foi feita para garantir confidencialidade. O que fazer para decifrar a mensagem?
   A. Decifrar CipherBody com chave pública do recetor, substituir CipherBody por resultado da decifra.
   B. Decifrar CipherBody com chave privada do recetor, substituir CipherBody por resultado da decifra.
   C. Decifrar CipherBody com chave igual ao resultado do hash do identificador do Sender, substituir CipherBody por resultado da decifra.
   D. Nenhuma das anteriores.

10) No Kerberos, considere um ticket para o cliente C usar o serviço S:
   A. O ticket é seguro porque é cifrado com a chave pública do servidor S
   B. O ticket é seguro porque é cifrado com uma chave que é um segredo entre o Kerberos e o servidor S
   C. O ticket é seguro porque é cifrado com a chave do cliente
   D. O ticket é seguro porque a chave KC,S é gerada pelo Kerberos e só este a conhece

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