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) Um Nome pode ter por função identificar um objeto
   a) Um URL tem normalmente esta função de identificar
   b) Um *namespace* tem esta função de identificar num documento XML
   c) Um número de telefone de um operador móvel identifica apenas o operador
   d) Identificar e localizar são a mesma função

   [ ]

2) Considere os diversos modos de resolução do DNS
   a) Iterativo: mais difícil para tratar com falhas
   b) Recursivo: não tem de manter contexto de resolução
   c) Transitivo: simplifica clientes e servidores
   d) Transitivo: a responsabilidade da tradução fica explícita

   [ ]

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 URL que permite localizar o WSDL
   c) É o URL do serviço
   d) É um nome que tem de ser traduzido no UDDI

   [ ]

4) Um atacante passivo na rede:
   a) Escuta e insere novas mensagens na rede.
   b) Escuta apenas as mensagens cifradas.
   c) Está geograficamente fixo num dado local.
   d) Escuta mas não introduz novas mensagens na rede.

   [ ]

5) A cifra AES em modo CBC é:
   a) Uma cifra assimétrica contínua.
   b) Uma cifra simétrica por blocos.
   c) Uma cifra simétrica por blocos com realimentação.
   d) Uma cifra simétrica que expõe padrões entre blocos de texto em claro e respetivos blocos de texto cifrado.

   [ ]

6) A cifra dita híbrida consiste em:
   a) Cálculo de função de resumo (digest) a partir de fontes de dados diferentes.
   b) Duas cifras simétricas consecutivas executadas sobre os mesmos dados.
   c) Combinação de cifra simétrica com cifra assimétrica.
   d) Combinação de cifra assimétrica feita com a chave pública e com a chave privada.

   [ ]

7) Suponha que implementou um Web Service – ca-ws – que devolve certificados de chave pública já assinados pela respetiva CA (Autoridade de Certificação de Chaves Públicas). A comunicação dos clientes com este Web Service:
   a) Não necessita de proteção. O certificado só por si já é seguro.
   b) Necessita de ser protegida usando uma cifra simétrica.
   c) Necessita de ser protegida através de assinatura digital das mensagens SOAP.
   d) Necessita de comunicar através de SOAP sobre HTTPS.

   [ ]

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) Gerar o resumo (digest) de M e ver se é igual à assinatura digital.
   b) Gerar o resumo (digest) de M, cifrá-lo com a chave pública da Alice e ver se é igual à assinatura digital.
   c) Decifrar a assinatura digital usando a chave pública da Alice, gerar o resumo (digest) de M, e comparar se ambos os resultados são iguais.
   d) Decifrar M com a chave privada do Bob, gerar o resumo do resultado e ver se é igual à assinatura digital.

   [ ]

9) O Kerberos V5 tem dois componentes: Saut e TGS. A principal vantagem desta separação do ponto de vista da segurança é:
   a) Aumentar a rapidez da execução de todo o protocolo deste a autenticação inicial junto de Saut até à comunicação segura com o servidor S.
   b) Minimizar a utilização da chave que autentica o cliente: Kc.
   c) A possível utilização de algoritmos de cifra diferentes para falar com o Saut e com o TGS.
   d) Permitir que um dado ticket possa ser reutilizado por um servidor diferente.

   [ ]

10) O controlo de acessos a um recurso pode ser feito através de uma ACL, que contém:
   a) Atributos que descrevem o recurso.
   b) Sujeitos e respetivas permissões de acesso ao recurso.
   c) Nomes alternativos do recurso.
   d) Nomes de todos os sujeitos que já acederam ao recurso.

   [ ]

11) O objetivo do 'handshake' do TLS é:
   a) Cumprimentar o servidor antes de iniciar a utilização do canal seguro.
   b) Autenticar os intervenientes e definir a chave de sessão a usar para proteger o canal.
   c) Trocar apenas os certificados digitais do cliente e do servidor.
   d) Apenas descobrir o algoritmo de cifra a utilizar para garantir a confidencialidade do canal.

   [ ]

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**