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

```
program BANCOPROG {
  version BANCOVERS {
    criarRet          CRIAR(criarIn) = 1;
  } = 1;
} = 0x20000005;
```

   a) Nome impuro.
   b) Não é na realidade um nome porque não é garantida pelo sistema a unicidade referencial.
   c) Nome global numa rede que utiliza o SUN-RPC.
   d) Nome local numa rede que utiliza o SUN-RPC.

2) Considere o URI referido pelo atributo *location* da etiqueta soap:address, no extrato seguinte de uma secção do WSDL:

```
<wsdl:service name="SDStore">
       <wsdl:port name="SDStoreImplPort" binding="tns:SDStoreServiceSoapBinding">
              <soap:address location="http://localhost:8080/SDStoreWS"/>
       </wsdl:port>
</wsdl:service>
```

   a) É usado para identificar o servidor.
   b) É um *namespace.*
   c) É um nome impuro.
   d) É um nome que tem de ser traduzido no UDD.

3) Considere o método iterativo e recursivo de resolução de nomes do DNS:
   a) Iterativo torna mais eficaz a cache do servidor.
   b) Iterativo e recursivo afectam a resolução do nome, mas não têm relação com as caches apenas relacionadas com os servidores secundários.
   c) Recursivo sobrecarrega o servidor, mas permite preencher a cache mais rapidamente.
   d) Recursivo diminui a carga do servidor, mas permite preencher a cache mais rapidamente.

4) Relativamente à Base Computacional de Confiança (*Trusted Computing Base*) 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 deve conter o conjunto mínimo de mecanismos que permitem implementar políticas de segurança.
   d) A TCB identifica os utilizadores reconhecidos no sistema.

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

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

7) Para verificar uma assinatura digital recebida, é necessário que o recetor:
   a) Decifre a assinatura com a chave pública do emissor e confirme se o valor é diferente de 0.
   b) Calcule o resumo da mensagem recebida, decifre a assinatura recebida com a chave pública do emissor e compare ambos os resultados.
   c) Calcule o resumo da mensagem e compare diretamente com a assinatura recebida.
   d) Calcule o resumo da mensagem e compare com a assinatura decifrada com chave privada do emissor.

8) Uma função de resumo (*digest*) pode ser usada para assinaturas digitais, se:
   a) É injetiva, não-invertível e resistente a difusões.
   b) É injetiva, invertível e resistente a colisões.
   c) É eficiente, não-invertível e resistente a colisões.
   d) É mais rápida que uma função de cifra simétrica.

9) Pretende-se fazer a distribuição manual de chaves simétricas de modo a permitir que três entidades – Alice, Bob e Charlie - se possam autenticar entre si. Deve gerar e depois distribuir as seguintes chaves:
   a) Alice deve ter chave pública de B e C; Bob deve ter chave pública de A e C; Charlie deve ter a chave pública de A e B.
   b) Alice deve ter Ka, Bob deve ter Kb e Charlie deve ter Kc.
   c) Alice deve ter Kab e Kac; Bob deve ter Kab e Kbc e Charlie deve ter Kac e Kbc.
   d) Alice deve conhecer Kab, Kac; Bob deve ter Kbc e Charlie deve ter Kac.

10) A Alice gerou um par de chaves, pública e privada, e obteve um certificado digital da sua chave pública. Esse certificado:
   a) Tem a chave pública da Alice, validade e data assinadas pela autoridade.
   b) Tem a chave pública e privada da Alice; esta decifra o certificado para obter a chave privada.
   c) Não pode ser revogado durante o seu período de validade.
   d) Na hierarquia de entidades certificadoras existe uma raiz, cuja chave pública nunca pode ser atacável por *man-in-the-middle* devido à utilização de um tipo diferente de certificados.

11) A Alice pretende assinar um documento que vai ser guardado na nuvem e precisa de garantir os seguintes requisitos: integridade, autenticação e não repúdio. Indique a solução apropriada:
   a) Usa um MAC para assinar.
   b) Usa uma função de resumo e depois cifra o resultado com cifra simétrica com uma chave que mantém secreta.
   c) Usa uma função de resumo e depois cifra o resultado com cifra assimétrica com a sua chave privada.
   d) Usa uma função de resumo e depois cifra o resultado com cifra assimétrica com a sua chave pública.

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**