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) Porque é que os nomes puros são mais difíceis de usar:
   a) Porque não são hierárquicos.
   b) Porque não tendo informação de localização não permitem orientar o algoritmo de resolução.
   c) Porque são mais difíceis de criar.
   d) Porque são normalmente binários e não podem ser usados em XML.

2) Em DNS, um pedido de resolução do nome www.tecnico.ulisboa.pt:
   a) Dá erro pois o nome indicado acima não é um nome DNS válido.
   b) Implica sempre contactar o servidor do domínio raiz, depois o servidor do domínio pt, depois o servidor do domínio técnico, depois o servidor do domínio www.
   c) Implica sempre contactar o servidor do domínio raiz, depois o servidor do domínio pt, depois o servidor do domínio técnico.
   d) Pode ser resolvido sem ter de contactar todos os servidores dos domínios do nome, caso já exista na cache do cliente ou de um dos servidores.

3) Compare UDDI, RMIregistry, rpcbind:
   a) O UDDI permite obter uma lista de URL para um serviço de que se conhece um identificador.
   b) O RMIregistry permite obter uma lista de referências remotas para um serviço de que se conhece um identificador.
   c) O RPCbind permite obter uma lista de portos para um objeto de que se conhece um identificador.
   d) Todos os servidores de nomes apenas permitem resolver um identificador num endereço de localização.

4) A codificação de base 64 permite:
   a) Comprimir os dados num fator de 64.
   b) Representar informação binária em texto, permitindo assim o seu transporte em protocolos baseados em texto.
   c) Cifrar a informação.
   d) Representar informação textual em binário, permitindo assim uma maior eficiência de transmissão.

5) Compare a distribuição de chaves entre cifra simétrica e assimétrica:
   a) É mais fácil distribuir uma chave pública que uma chave simétrica pois não precisamos de garantir integridade nem autenticidade para distribuir a primeira.
   b) É mais fácil distribuir uma chave pública que uma chave simétrica pois não precisamos de garantir confidencialidade para distribuir a primeira.
   c) É mais fácil distribuir uma chave simétrica que uma chave pública pois não precisamos de garantir integridade nem autenticidade para distribuir a primeira.
   d) É mais fácil distribuir uma chave simétrica que uma chave pública pois não precisamos de garantir confidencialidade para distribuir a primeira.

6) Com a cifra assimétrica RSA é possível:
   a) Cifrar com a chave pública, decifrar com a chave privada.
   b) Cifrar com a chave privada, decifrar com a chave pública.
   c) Combinar com função de resumo para construir assinaturas digitais.
   d) Todas as anteriores.

7) A Alice e o Bob partilham entre si a chave Kab. A Alice pretende autenticar-se perante Bob. Bob envia um desafio D para Alice. A Alice devolve a Bob o desafio D cifrado com a chave Kab. O que deve ser escolhido como valor de D:
   a) A data (dia-mês-ano) do dia.
   b) A hora (hora-minutos-segundos).
   c) Um número aleatório.
   d) Um número aleatório que não volte a ser usado.

8) Usando Kerberos, um cliente obteve um ticket para sessão com o serviço S. O cliente C pretende agora enviar um pedido confidencial a S. Para tal, a mensagem de invocação deve incluir:
   a) {pedido}Kc
   b) {pedido}Kcs
   c) {pedido}Ks
   d) {pedido}Ksaut

9) Qual é a consequência da exposição ilícita da chave privada de uma CA (Autoridade de Certificação de Chaves Públicas):
   a) Nenhuma.
   b) É necessário gerar um novo par de chaves para a CA, mas os certificados já emitidos continuam válidos.
   c) Os certificados emitidos pela CA que já estavam fora do prazo deixam de ser válidos.
   d) Os certificados emitidos pela CA que estavam dentro do prazo deixam de ser válidos.

10) O Bob recebeu um certificado com a chave pública da Alice emitido pela CA "TrueCA", cuja chave pública não era conhecida do Bob. Por essa razão, o Bob obteve a chave pública da "TrueCA" por canal inseguro a partir de uma fonte não certificada. Qual dos ataques seguintes é possível?
   a) Ataque *man-in-the middle* ao momento em que a chave pública da TrueCA é entregue ao Bob.
   b) *Man-in-the middle* em que um atacante substitui a chave pública no certificado pela chave pública do atacante.
   c) *Replay attack* em que um atacante tenta reutilizar o certificado depois do seu prazo de validade expirar.
   d) Nenhuma das anteriores.

11) Um JAX-WS SOAP Handler pode ser usado para assinar 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) Inverter o sentido de processamento das mensagens.

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**