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 nome "rmi://rmi.tecnico.pt/objsd", que identifica um objeto remoto em Java RMI. Para que um cliente possa obter a referência remota para o objeto registado com este nome, é necessário recorrer ao(s) seguinte(s) serviço(s) de nome(s):
   A) Ao serviço *RMI registry* para traduzir o nome do objeto numa referência remota.
   B) Ao DNS para traduzir o nome DNS da máquina do *registry* num endereço IP.
   C) Ao ARP para traduzir o endereço IP da máquina do *registry* num endereço MAC.
   D) Todos os anteriores.

   [ ]

2) No projeto de SD, um web service fornecedor pode ser identificado por um *service name* como "supplier1" ou por um URL como "http://sigma.tecnico.pt/sd/supplier1". Compare ambos os espaços de nomes:
   A) Ambos são puros.
   B) Ambos são impuros.
   C) O primeiro é impuro, o segundo é puro.
   D) O primeiro é puro, o segundo é impuro.

   [ ]

3) 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.

   [ ]

4) Qual é a vulnerabilidade mais conhecida do algoritmo DES?
   A) Possibilidade de utilização de diferentes modos de combinação de blocos.
   B) Tamanho do bloco de cifra.
   C) Chave de pequena dimensão.
   D) Necessidade de enchimento (*padding*) do último bloco de dados.

   [ ]

5) Considere a seguinte mensagem SOAP:
   <S:**Envelope** xmlns:S="http://schemas.xmlsoap.org/soap/envelope/" ><S:**Header** />
   <S:**Body**><ns2:**sayHello**
   xmlns:ns2="http://ws.example/"><arg0>**friend**</arg0></ns2:sayHello></S:Body></S:Envelope>

   O que deve adicionar para proteger **apenas** a autenticidade, integridade e não repudiação da mensagem?
   A) Cabeçalho com resumo dos cabeçalhos da mensagem cifrado com chave privada do emissor.
   B) Cabeçalho com cifra total do corpo com a chave privada do emissor.
   C) Cabeçalho com certificado digital do emissor.
   D) Cabeçalho com resumo da mensagem cifrado com chave privada do emissor.

   [ ]

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

7) Considere uma entidade A cujo par de chaves de cifra assimétrica foi criado pela autoridade certificadora CA. Verificou-se que a entidade não é confiável e lhe deveria ser inibido o uso do certificado.
   A) A entidade A continua a deter o certificado e só quem usar o certificado poderá, contactando a CA, detetar que já não é valido
   B) O período de validade dos certificados de A é colocado a zero
   C) Se a entidade for colocada na blacklist da CA a validação de assinatura da CA deixa de funcionar localmente
   D) O certificado é eliminado em todos os utilizadores

8) Um certificado da entidade A é uma estrutura de informação
   A) Que tem a chave secreta de A
   B) Que tem a chave pública de A, sendo assinada com a chave pública de uma CA
   C) Que tem a chave pública de A, sendo assinada com a chave secreta de A
   D) Que tem uma definição do prazo de validade e a chave pública de A

9) A cifra assimétrica
   A) É superior porque resiste muito melhor a ataques brute-force
   B) Pode-se transmitir a chave pública sem qualquer perigo de ataque
   C) A cifra assimétrica consome significativos recursos de processamento
   D) A cifra assimétrica é usada eficazmente para qualquer tamanho de texto a cifrar

10) Comparando o protocolo Needham-Schroeder e o Kerberos analisado nas teóricas, qual das seguintes é verdadeira?
   A) O Kerberos usa exclusivamente em cifra assimétrica, enquanto que o Needham-Schroeder é em simétrica.
   B) O objetivo do Kerberos é entregar a chave de longa duração do cliente ao serviço, enquanto que o Needham-Schroeder distribui uma chave de sessão.
   C) O Kerberos assume relógios sincronizados, enquanto que o Needham-Schroeder não.
   D) No Kerberos, o Saut conhece as chaves secretas dos utilizadores; no Needham-Schroeder, o Saut não conhece qualquer segredo dos utilizadores.

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