Sistemas Distribuídos, 2018/19
3º MINI Teste

- Todas as perguntas têm a mesma cotação. Cada pergunta tem apenas uma resposta completamente certa.
- Na sua resposta pode selecionar uma ou mais alíneas. Preencha-as por ordem crescente, com vírgulas.
- Para cada pergunta, a nota é calculada pelas alíneas que escolheu na sua resposta, da seguinte forma: a alínea correta conta com a cotação completa; cada alínea incorreta desconta 1/3 da cotação da pergunta.
- Exemplo: numa dada pergunta, escolheu as alíneas "A, D". Se a alínea certa for a A, então a nota final será 2/3 da cotação (cotação completa pela alínea certa menos 1/3 pela alínea incorreta).

Número: _____ Nome: _____

1) "Em 2005, criptoanalistas descobriram ataques sobre SHA-1, sugerindo que o algoritmo poderia não ser seguro o suficiente para uso continuado. O NIST exigiu que várias aplicações utilizadas em agências federais mudassem para SHA-2 depois de 2010 devido à fraqueza descoberta." (fonte: *wikipedia*)
   Escolha a frase que melhor resume o excerto acima.
   A. Mantiveram-se os mecanismos de segurança, mudaram-se as políticas de segurança
   B. A Base Computacional de Confiança (TCB) foi alargada.
   C. O excerto não tem qualquer relação com políticas ou mecanismos de segurança, nem TCB.
   D. Houve uma mudança de um mecanismo de segurança, mantendo-se as políticas de segurança.

   [ ]

2) Considere a cifra de blocos AES-128. O modo ECB permite:
   A. Esconder os padrões dos blocos cifrados.
   B. Aumentar a resistência da chave a ataques de força-bruta.
   C. Assinar a mensagem.
   D. Cifrar diferentes blocos em paralelo.

   [ ]

3) Por que razão já não se deve utilizar o algoritmo de cifra DES?
   A. A chave é de pequena dimensão.
   B. Possibilidade de utilização de diferentes modos de combinação de blocos.
   C. Tamanho do bloco de cifra é demasiado pequeno.
   D. Exige enchimento (*padding*) do último bloco de dados.

   [ ]

4) Assuma que a rede de serviços do IST usa o Kerberos como sistema de autenticação. Quando o departamento DEI pretende instalar um novo serviço, a chave respetiva (Ks) deve ser entregue a qual entidade do sistema Kerberos?
   A. Ao Ticket Granting Service que gere o departamento DEI
   B. Ao servidor de autenticação principal, Saut
   C. A nenhuma entidade, Ks é secreta e só conhecida pelo serviço em causa
   D. A todos os clientes que podem vir a aceder ao novo serviço

   [ ]

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

   [ ]

6) A Alice envia uma mensagem M cifrada com a chave pública de Bob usando o algoritmo RSA-2048.
   A. RSA não é uma cifra assimétrica.
   B. Apenas Bob vai conseguir decifrar a mensagem.
   C. Apenas Alice pode ter enviado a mensagem.
   D. B e C

7) Qual a combinação de vantagens que torna atrativa a cifra híbrida?
   A. O bom desempenho da cifra assimétrica com a facilidade de distribuição de chaves secretas.
   B. Só a cifra simétrica permite garantir confidencialidade, só a cifra assimétrica permite garantir integridade.
   C. O bom desempenho da cifra simétrica com a facilidade de distribuição de chaves públicas.
   D. Nenhuma das anteriores.

8) Num certificado digital de chave pública, qual dos seguintes campos não precisa ser assinado digitalmente?
   D D A A D B C D D
   A. A data de expiração
   B. O identificador único do certificado
   C. A chave pública
   D. Nenhuma das anteriores.

9) Suponha que a chave privada do certificado digital do *web site* do Técnico foi roubada por atacantes. O que devem fazer os administradores para que o *web site* continue a funcionar com segurança reposta?
   A. Nada, dado que o certificado digital apenas contém a chave pública.
   B. Contactar a CA que emitiu o certificado e pedir para que este seja revogado.
   C. Emitir um novo par de chaves e pedir a uma CA que certifique a nova chave pública.
   D. B e C.

D D A A D B C D D