Segurança
1º Semestre, 2014/15

1º Teste
21 de Novembro de 2014

- Todas as perguntas têm a mesma cotação.
- A duração total do teste é de 1h30.

1. Considere os ataques por esmagamento da pilha (*stack smashing attack*) usando C.
    a. Explique como funcionam.
    b. Explique como é que o mecanismo de canários permite evitar a seu sucesso.

2. Uma cifra contínua pode criar problemas caso o seu gerador tenha um número reduzido de estados internos (face ao comprimento da mensagem a cifrar). Explique detalhadamente porquê, ilustrando a sua resposta com um diagrama.

3. O alinhamento com excipiente (*padding*) é uma solução habitual para conseguir realizar a cifra de mensagens de qualquer dimensão com um modo de cifra por blocos. Explique:
    a. Por que razão é preciso realizar esse alinhamento?
    b. Descreva uma forma de o fazer, ilustrando a explicação.

4. Alguns modos de cifra permitem obter acesso aleatório uniforme, tanto na cifra como na decifra. Explique:
    a. O que significa essa qualidade?
    b. Indique, justificando, 2 modos de cifra com essa qualidade.

5. Considere as propriedades que distinguem as funções de síntese (*digest*) de outras funções de dispersão (*hashing*).
    a. Indique quais são, usando um formalismo matemático.
    b. Indique, justificando, qual dessas propriedades (**apenas uma!**) é a mais crítica para a exploração de uma função de síntese em assinaturas digitais.

6. Indique duas razões que considerar fundamentais para explorar *smartcards*, como o Cartão de Cidadão, para realizar assinaturas digitais com valor legal.

7. Considere a gestão de chaves públicas. Explique:
    a. O que é uma cadeia de certificação?
    b. Em que consiste exatamente uma raiz confiável de uma cadeia de certificação?

8. Pretende-se validar uma assinatura digital realizada na data T1 com a chave pública presente num certificado com prazo de validade entre T2 e T3 que foi revogado na data T4. Indique, justificando, para que valores de T1 pode a assinatura ser considerada válida.

9. No âmbito da avaliação biométrica pode acontecer que dois indivíduos apresentem as mesmas características biométricas. Discuta o impacto deste facto para efeitos da avaliação da eficácia de um sistema de autenticação biométrica (**atenção! não confunda identificação biométrica com autenticação biométrica**).

10. Considere a autenticação de pessoas com apresentação direta de senhas descartáveis. Explique:
    a. O que são senhas descartáveis?
    b. Em que cenários operacionais faz sentido usar estas senhas?