Segurança
1º Semestre, 2009/10

1º Teste
10 de Novembro de 2009

- Todas as perguntas têm a mesma cotação.
- A duração total é de 1 hora e 30 minutos

1. Descreva o modo como se processa um ataque por esmagamento da pilha (*stack smashing attack*).

2. Explique qual o modelo geral de operação de uma cifra contínua, ilustrando-o com um diagrama.

3. O modo de cifra por blocos ECB não esconde padrões repetidos nos blocos de texto original mas pode mesmo assim ser interessante para algumas aplicações concretas, como sistemas de ficheiros seguros com capacidade de cifra de conteúdos. Explique:
    a. Qual o interesse de usar ECB em sistemas de ficheiros seguros com cifra.
    b. Como complementar a cifra com ECB de modo a evitar o surgimento de padrões (pista: as técnicas usadas pelo CFS).

4. As funções de síntese devem dificultar a descoberta de colisões. Explique:
    a. Em que consiste a descoberta de uma colisão.
    b. Qual o risco da descoberta de colisões no âmbito da validação de assinaturas digitais calculadas sobre valores calculados com funções de síntese.

5. Um MAC (*Message Authentication Code*)é um meio de autenticação de dados. Explique porque razão não pode ser usado para provar a autoria dos dados perante terceiros (ou, por outras palavras, porque razão permite repúdio de origem).

6. As assinaturas digitais são normalmente concretizadas sobre sínteses de documentos. Explique por que razão se usa essa aproximação.

7. Considere o sistema de ficheiros EFS (*Encrypting File System*), uma extensão do NTFS. Explique:
    a. Como é feita a gestão de chaves de cifra de cada ficheiro.
    b. Como é integrada a gestão de chaves com a protecção de acesso a cada ficheiro.

8. Considere o padrão PKCS #11. Explique:
    a. O que define este padrão?
    b. Qual a sua relevância para a exploração de *smartcards*?

9. Considere a gestão de chaves públicas. Explique:
    a. O que é um certificado de uma chave pública.
    b. Como se pode limitar o tempo de vida dos certificados emitidos por uma Entidade Certificadora.

10. Explique para que serve o protocolo OCSP e em que circunstância deve ser usado.