Segurança
1º Semestre, 2010/11

2º Exame
1 de Fevereiro de 2010

- Todas as perguntas têm a mesma cotação.
- A duração total do exame é de 3 horas (20 perguntas).

1. Por que razão podem ocorrer *buffer overflows* em C e não em Java?
2. Considere o circuito lógico conhecido como LFSR (*Linear Feedback Shift Register*), usado para concretizar cifras contínuas. Explique:
    a. Qual é o comprimento máximo do período da sequência de bits que produz?
    b. O que significa o facto de possuir um polinómio de realimentação primitivo?
3. Mostre, matematicamente, de que modo a cifra RSA seria insegura se fosse possível:
    a. Factorizar facilmente grandes números.
    b. Calcular facilmente logaritmos discretos de grandes números.
4. Usando o Paradoxo do Aniversário, indique qual é, aproximadamente, a capacidade máxima de resistência à colisão de uma função de síntese. Justifique apropriadamente a sua resposta.
5. Descreva o modelo de execução da construção HMAC, destinada a calcular o MAC (*Message Authentication Code*) de uma mensagem.
6. Considere o conceito de assinatura digital. Explique o motivo que justifica que na sua construção seja incluída informação adicional (para além do documento a assinar, ou da sua síntese).
7. Explique, de uma forma o mais completa possível, por que razão os certificados de chaves públicas são vitais para suportar a validação de assinaturas digitais.
8. Considere o conceito de CRL (*Certificate Revocation List*). Explique:
    a. Quem gere uma CRL?
    b. Quem, e quando, se deve usar a sua informação?
9. Explique, exemplificando, que riscos corre um utilizador caso o seu repositório de certificados seja atacado por um vírus que lhe introduz informação falsa.
10. Explique, com pormenor, como se processa a autenticação Linux.

11. O GSM usa um processo de autenticação em que se usa, simultaneamente, algo que se tem e algo que se sabe. Explique porquê, complementando a sua explicação com um diagrama.
12. Considerando que o Cartão de Cidadão não realiza decifras com as suas chaves privadas, mas apenas assinaturas, como o usaria para realizar uma autenticação remota através de desafio-resposta?
13. Considere o conceito de controlo de acessos obrigatório (*mandatory*). Indique:
    a. Como funciona?
    b. Dê dois exemplos práticos da sua exploração.
14. Quais as vantagens práticas da aplicação do princípio da separação de deveres para a segurança do sistema?
15. Explique os princípios do modelo de controlo de fluxos de Bell-LaPadula.
16. Considere o modelo de controlo de integridade de Clark-Wilson. Explique em que consiste:
    a. Um CDI (*Constrained Data Item*) e um UDI (*Unconstrained Data Item*)
    b. Uma IVP (*Integrity Verification Procedure*) e uma TP (*Transformation Procedure*).
17. Explique em que medida o conceito de inferência pode representar um problema de segurança na gestão de uma base de dados.
18. Considere uma base de dados multi-nível, onde os dados estão cifrados consoante o seu nível de segurança. Explique:
    a. Qual a consequência deste facto para os utentes da base de dados?
    b. Que cuidados especiais devem ser tomados na cifra dos dados?
19. Na Internet existem sensores que avaliam a perigosidade da rede. Explique:
    a. O que são estes sensores?
    b. Como é que eles avaliam a perigosidade?
20. Explique por que razão as Java *Virtual Machines* (ou os Java *Run-time Environments*) impõem restrições aos locais de onde carregam classes para uma determinada aplicação?