Segurança
1º Semestre, 2012/13

2º Teste / 1º Exame
9 de Janeiro de 2013

- Todas as perguntas têm a mesma cotação.
- A duração total do teste é de 1 hora e 30 minutos (últimas 10 perguntas).
- A duração total do exame é de 3 horas (20 perguntas).

1. Em que medida as bases de dados de CVE (*Common Vulnerabilities and Exposures*) contribuem para uma maior segurança dos sistemas computacionais em rede?

2. Uma cifra contínua é uma aproximação prática e viável da cifra *One-Time Pad* de Vernam. Explique esta afirmação, usando para o efeito diagramas ilustrativos da operação de ambas as cifras.

3. A cifra RSA baseia a sua segurança em duas propriedades: dificuldade na factorização de grandes números e dificuldade no cálculo de logaritmos discretos de grandes números. Explique porquê?

4. O modo de cifra OFB (*Output FeedBack*) só usa cifra por blocos, mas não decifra. Explique porquê, descrevendo para o efeito cifras e decifras com OFB.

5. Explique que vantagens advêm da utilização conjunta de funções de síntese e cifras assimétricas no cálculo, transmissão e validação de assinaturas assimétricas.

6. Explique como funciona a construção HMAC, usada no cálculo de um MAC (*Message Authentication Code*).

7. As assinaturas digitais realizadas sobre documentos são normalmente acompanhadas por um ou mais certificados de chave pública.
    a. Quais são esses certificados?
    b. Qual é o interesse em os transmitir?

8. Considere o Cartão de Cidadão.
    a. Que importância tem o facto de os pares de chaves do seu titular serem gerados internamente?
    b. Que limitações existem pelo facto de apenas disponibilizar cifra (assinatura) com as chaves privadas, mas não decifra?

9. Como se estabelece à escala mundial a confiança nas Entidades Certificadoras?

10. Um certificado de chave pública é um documento com um prazo de validade.
    a. Como é definido esse prazo?
    b. Como se pode verificar se estava válido numa determinada data, diferente da atual?

11. Explique por que razão a autenticação de entidades é normalmente um requisito fundamental para a concretização de políticas de autorização.

12. Considere o conceito de autenticação com senha única.
    a. Que cenários operacionais justificam o seu uso?
    b. Escolha um protocolo de autenticação com senha única e descreva o seu funcionamento.

13. Considere os protocolos de autenticação com desafio-resposta e segredo partilhado.
    a. Explique de uma forma genérica como funcionam.
    b. Explique como podem ser desenhados para facultar autenticação mútua (com um mínimo de mensagens trocadas).

14. A autenticação de máquinas pode-se fazer com chaves públicas certificadas (ex. SSL) ou com chaves públicas não-certificadas (ex. SSH).
    a. Explique as vantagens e desvantagens de cada uma das aproximações.
    b. Explique a razão das opções tomadas no SSL e no SSH face a esta questão.

15. Um núcleo de um sistema operativo é, entre outras coisas, um monitor de controlo de acesso. Explique porquê.

16. Tradicionalmente os sistemas operativos permitem concretizar políticas de proteção de recursos baseadas em grupos e não em funções, ou papeis (*Role-Based Access Control*, RBAC).
    a. Descreva cada uma destas políticas.
    b. Explique em que medida essas políticas são diferentes.

17. Discuta uma possível aplicação do modelo de Clark-Wilson a sistemas suscetíveis de ataques por injeção de pesquisas SQL.

18. Considere a cifra de conteúdos de sistemas de ficheiros.
    a. Que situações motivam a sua exploração?
    b. Que aproximações genéricas existem para a sua concretização?

19. Explique o objetivo e o princípio da técnica do K-anonimato.

20. As aplicações Java permitem apenas uma atualização do seu SecurityManager em cada execução. Explique porquê.