Segurança
1º Semestre, 2008/09

2º Teste / 1º Exame
16 de Janeiro de 2008

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

1. Explique em que consiste o conceito de domínio de segurança.
2. Considere as cifras poli-alfabéticas. Indique:
    a. O que é o período de uma cifra poli-alfabética.
    b. Uma técnica para descobrir o período (descreva a técnica com algum pormenor).
3. Explique o modelo geral de operação de uma cifra contínua.
4. Uma cifra contínua é uma aproximação prática à cifra de Vernam, ou *one-time pad*, a única totalmente segura. Explique:
    a. Como funciona a cifra de Vernam.
    b. Por que razão em circunstâncias normais não se usa a cifra de Vernam.
5. Explique como funciona o cálculo de um código de autenticação de mensagem (*Message Authentication Code*, MAC) com recurso a uma cifra por blocos e ao modo de cifra CBC (*Cipher Block Chaining*).
6. A qualidade de uma função de síntese mede-se segundo três características: (i) resistência à descoberta de um texto, (ii) resistência à descoberta de um segundo texto e (iii) resistência à colisão. Explique em que consiste cada uma destas características.
7. As assinaturas digitais são normalmente concretizadas sobre sínteses de documentos e não sobre os mesmos. Explique:
    a. Por que razão se usa essa aproximação.
    b. Quais das três características de qualidade indicadas na alínea anterior são críticas para se poder usar esta aproximação.
8. Considere o modo de cifra *Counter Mode* (CTR), que permite transformar uma cifra por blocos numa cifra contínua. Explique:
    a. Como funciona.
    b. Como se consegue com o mesmo obter acesso aleatório rápido (ou homogéneo).
9. No 2º projecto prático da cadeira usaram-se *streams* do NTFS para guardar metainformação relativa a ficheiros protegidos. Explique:
    a. Quais as vantagens de usar essa metainformação por cada ficheiro protegido.
    b. Quais as consequências da eliminação ou adulteração dessa metainformação.
10. O EFS (*Encrypted File System*) do Windows é uma extensão do NTFS que permite cifra de ficheiros de forma integrada com a sua lista de controlo de acesso. Explique:
    a. Como é protegido cada ficheiro através de cifra.
    b. De que modo se integra essa cifra (ou decifra) com a lista de controlo de acesso de cada ficheiro.

11. Considere o modelo de operação normal da autenticação Unix. Explique:
    a. Como funciona.
    b. Por que razão é vulnerável a ataques com dicionários.
12. Considere a alteração da autenticação local numa máquina Unix para um modelo baseado em chaves assimétricas, por exemplo, usando o Cartão de Cidadão. Indique as vantagens e desvantagens da sua utilização como alternativa à autenticação Unix normal.
13. Discuta as diversas vantagens e desvantagens operacionais da autenticação biométrica face aos demais paradigmas de autenticação.
14. Considere a autenticação em redes GSM. Explique:
    a. Como funciona.
    b. Como se impede que um operador que forneça acesso em *roaming* a um subscritor de outro operador obtenha as credenciais de autenticação do subscritor.
15. Explique como funciona o modelo de autenticação de servidores SSH.
16. A qualidade de uma técnica de autenticação biométrica deve ser avaliada segundo diversos critérios, nomeadamente universalidade, unicidade, estabilidade, correcção, conveniência e aceitação.
    a. Explique o que significa cada um destes critérios
    b. Dê exemplos da avaliação de cada um deles em duas técnicas concretas.
17. A gestão de um par de chaves assimétricas envolve a sua geração, a protecção da chave privada, a distribuição da chave pública e o tempo de vida do par. Explique os problemas que importa resolver em cada um destes quatro tópicos.
18. Explique em que medida, e porquê, os *smart cards* são úteis na exploração dos pares de chaves assimétricas.
19. Explique em que consiste um certificado de uma chave pública e por que razão se usam tais certificados.
20. Considere a revogação de certificados de chaves públicas. Explique:
    a. Em que consiste um certificado de revogação.
    b. Por que razão é preciso manter e consultar listas de certificados de revogação.