Segurança
1º Semestre, 2013/14

1º Teste
13 de novembro de 2013

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

1. Os ataques de ARP *poisoning* são possíveis devido à existência de vulnerabilidades. Explique:
    a. Quais são essas vulnerabilidades?
    b. Indique uma consequência de um ataque específico (a descrever) e a vantagem que pode advir para o atacante.

2. Os ataques de XSS (*Cross-Site Scripting*) exploram vários tipos de vulnerabilidade. Explique:
    a. Em que consiste a vulnerabilidade no caso dos ataques do tipo *Stored* XSS?
    b. Como se pode eliminar essa vulnerabilidade?

3. O seguinte criptograma foi gerado com recurso à cifra de Vigenère: **`SDTOAEGEEBPSHLEGEEDPEGEA`**
    a. Explique como funciona a cifra.
    b. Indique, justificando, qual será o período da cifra.

4. Considere a exploração de uma cifra por blocos AES (com blocos de 128 bits) em modo 8-bit OFB (*Ouput FeedBack*). Indique:
    a. Como funciona a cifra e a decifra.
    b. Quantas operações com o AES são necessárias para cifrar 1 KB de dados.

5. As cifras por blocos, quando aplicadas em modo ECB (*Electronic Code Book*), obrigam a que o texto a cifrar seja alinhado ao comprimento do bloco de entrada do algoritmo de cifra. Explique um método de fazer esse alinhamento de forma que o decifrador consiga extrair a forma como o alinhamento foi feito do criptograma (e.g. PKCS#5).

6. Explique o algoritmo genérico de concretização das funções de síntese (*digest*) do tipo da MD5 ou SHA-1.

7. As cifras assimétricas podem ser usadas para dois fins completamente distinto, consoante a chave que se usa para cifrar ou decifrar. Explique quais são esses fins e como são usadas as chaves em cada um deles.

8. As cifras assimétricas, tal como a RSA, quando são usadas repetidamente para cifrar valores constantes produzem sempre valores diferentes. Explique:
    a. O que provoca este resultado?
    b. Que vantagem advém desse comportamento?

9. Considere a gestão de chaves públicas. Explique:
    a. O que é uma CRL (*Certificate Revocation List*)?
    b. Porque que razão é necessário que uma Entidade Certificadora mantenha uma CRL e disponibilize acesso público à mesma?

10. Quando se verifica se um certificado foi ou não revogado, essa verificação deverá ter em conta uma noção temporal precisa (ou seja, deverá ter em conta um determinado instante temporal). Considerando o caso da assinatura digital de documentos, de que instante estamos a falar? Justifique a sua resposta.