Criptografia

Exame da 1ª Chamada

LECOM — 2005/2006

Pergunta 1

Considere o seguinte conteúdo de uma mensagem de e-mail (S/MIME), com protecção da confidencialidade, codificada de acordo com os tipos de dados ASN.1 da norma PKCS#7:

```
 0:d=0  hl=4 l= 535 cons: SEQUENCE
 4:d=1  hl=2 l=   9 prim: OBJECT            :pkcs7-envelopedData
                       ...
              ======> CERTIFICADO <=======
                       ...
116:d=5  hl=2 l=  13 cons: SEQUENCE
118:d=6  hl=2 l=   9 prim: OBJECT            :rsaEncryption
129:d=6  hl=2 l=   0 prim: NULL
131:d=5  hl=3 l= 128 prim: OCTET STRING   <<== Criptograma 1 (128 bytes)
262:d=3  hl=4 l= 273 cons: SEQUENCE
266:d=4  hl=2 l=   9 prim: OBJECT            :pkcs7-data
277:d=4  hl=2 l=  17 cons: SEQUENCE
279:d=5  hl=2 l=   5 prim: OBJECT            :des-cbc
286:d=5  hl=2 l=   8 prim: OCTET STRING   <<== IV (8 bytes)
296:d=4  hl=3 l= 2400 prim: cont [ 0 ]    <<== Criptograma 2 (2400 bytes)
```

1. Qual o nome deste tipo de técnica para transferência de informação com confidencialidade? Explique o seu funcionamento com base neste exemplo concreto justificando, nomeadamente, a presença de dois criptogramas. Por que motivo é comum recorrer-se a este tipo de construção?

2. Explique em detalhe o funcionamento interno do algoritmo `des-cbc`, relacionando com a presença de um vector de inicialização (IV) no conteúdo desta mensagem.

3. Explique a necessidade de utilização de um certificado de chave pública numa transacção deste tipo. Refira nomeadamente a quem pertence (emissor/destinatário) o certificado utilizado neste caso concreto, e como é utilizado neste contexto.

Pergunta 2

Recorde as primitivas criptográficas que permitem conferir garantias de *autenticidade de origem de mensagens* numa troca de informação.

1. Qual das técnicas que estudou se baseia no paradigma da criptografia simétrica? Dê um exemplo de como esta primitiva pode ser implementada e explique como a utilizaria na prática.

2. Considere uma situação em que as garantias de autenticidade podem ter de ser transmitidas a uma terceira parte, por exemplo, a mensagem recebida é um comprovativo de que se participou numa eleição. Seria a técnica que descreveu na alínea anterior apropriada neste caso? Justifique a sua resposta e, no caso de ser negativa, proponha uma alternativa.

Pergunta 3

Recorde o que aprendeu sobre Public Key Infrastructures (PKI).

1. Considere um processo de emissão de um Certificado de Chave Pública em que o pedido de certificado é efectuado via Web, sem contacto directo entre a Autoridade de Registo e o futuro Titular. Que problemas de segurança poderão advir desta implementação simplificada?

2. Explique o processo de validação de um Certificado de Chave Pública. Refira-se, nomeadamente, aos conceitos de *Hierarquia de Certificação*, *Cadeia de Certificação* e *Autoridade de Certificação de raiz*.

Pergunta 4

Considere o protocolo Secure Sockets Layer (SSL):

1. O sistema SSL baseia-se no conceito de sessão. Explique porque razão este é um modo de funcionamento comum em sistemas com segurança criptográfica.

2. Descreva a forma típica de utilização de Certificados de Chave Pública no estabelecimento de ligações SSL.