UNIVERSIDADE
EDUARDO
MONDLANE

Faculdade de Engenharia
Departamento de Engenharia Electrotécnica
Curso de Engenharia Informática
Disciplina: Criptografia e Segurança de Dados

Ficha 5 - Exercícios de Revisão CRIPTOGRAFIA MODERNA

Assinatura Digital e Autoridades de Certificação (AC)

1. Qual é a importância da utilização de assinatura digital?

2. Esquematize e explique o funcionamento da assinatura digital.

3. Qual é o objetivo central da utilização de AC?

4. O que entende por certificado e qual é o papel principal da AC?

5. Explique com as suas palavras a diferença entre certificação cruzada e certificação hierárquica.

6. Dê um exemplo de verificação da autenticidade da chave pública de uma entidade por outra, assumindo que cada uma obtém um certificado de AC diferente.

7. Indique e explique dois problemas relacionados ao uso de ACs.

PKI – Public Key Infrastructure (Infraestrutura de Chave Pública)

1. Defina PKI e explique a sua aplicação.

2. Identifique e descreva os componentes da PKI.

3. Fale dos processos da PKI.

4. Por que razão a tarefa de geração de chaves é normalmente atribuída a uma entidade externa (TTP – Trusted Third Party, ou Terceira Parte Confiável)?

5. Entende ser pacífico que a tarefa de geração e distribuição de chaves seja atribuída a uma TTP? Porquê?

6. Quais são os requisitos que uma TTP precisa reunir para ser confiável no processo de geração e distribuição de chaves?

7. O que entende por PGP?

8. O que significa Web de abordagem Trust e em que situação se aplica melhor?

9. Na PKI, qual é a diferença que existe entre sistemas baseados em identidade e sistemas centrados no servidor?

10. Dê um exemplo de utilização de um criptossistema híbrido apresentando ilustração de dois intervenientes na comunicação.

11. Apresente a diferença entre criptografia e esteganografia.