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

Ficha 2 - 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.

Criptografia Quântica

Tabela :1: Convenção Binária

BASE	0	1
V-H	↑	→
D-C	↗	↖

Tabela 2: Transmissão do Protocolo BB84

	1ª	2ª	3ª	4ª	5ª	6ª	7ª	8ª
Bits do Emissor a ser transmitidos:	1	0	1	1	0	0	1	0
Transmissão:								
Base do Emissor	V-H	V-H	D-C	V-H	D-C	D-C	D-C	V-H
Q-bits do emissor								
Base do Invasor	D-C	D-C	V-H	V-H	D-C	D-C	V-H	V-H
Q-bits capturados pelo invasor								
Base do receptor:	V-H	D-C	D-C	D-C	V-H	D-C	V-H	V-H
Q-bits capturados pelo Receptor								
Bits do Receptor a ser comparados:								
Bits do Emissor a ser comparados:								

1. De acordo com as Tabelas 1 e 2, responda às questões que se seguem:

   a) Indique a sequência de Q-bits do emissor.
   b) Indique a sequência de Q-bits capturados pelo invasor.
   c) Assumindo que na entrada quântica do receptor chegou a sequência de q-bits do invasor, indique a leitura do receptor.
   d) Qual é a sequência de bits correspondente às posições onde as bases do emissor e do receptor coincidem?
   e) Qual é a sequência de bits que o receptor irá comparar com o emissor para verificar a ocorrência da intromissão?
   f) Qual será o desfecho da comunicação?