Criptografia Aplicada

LESI / LMCC

Exame da 2^a Chamada – 28 de Janeiro 2006

Questão 1 Considere o modo de utilização de cifras por blocos *Output Feedback Mode* (OFB).

1. Descreva o seu funcionamento na cifragem e decifragem.
2. Suponha que se pretende proteger um canal de comunicação utilizando este modo de funcionamento. Explique, justificando, em que situações procederia à alteração do vector de inicialização.
3. Haveria alguma forma de minimizar a influência do atraso introduzido pela função de cifragem no débito da ligação?

Nome:_____ **Número:**_____ **Curso:**_____

Criptografia Aplicada

LESI / LMCC

Exame da 2^a Chamada – 28 de Janeiro 2006

Questão 2 A comunicação utilizando criptografia assimétrica permite substituir repositórios de chaves com fortes requisitos de confidencialidade, por soluções de armazenamento com fortes requisitos de autenticidade.

1. Comente esta afirmação.
2. Apresente um exemplo prático das consequências que a inexistência de garantias de autenticidade no armazenamento de chaves pode ter sobre um protocolo criptográfico que conheça.
3. Explique por que razão, apesar das suas evidentes vantagens, as cifras assimétricas não tornaram as cifras simétricas obsoletas. Como são utilizados dois tipos de técnica na prática?

Nome:_____ **Número:**_____ **Curso:**_____

Criptografia Aplicada

LESI / LMCC

Exame da 2^a Chamada – 28 de Janeiro 2006

Questão 3 As funções de *hash* criptográficas são desenhadas para apresentarem, entre outras, as seguintes três propriedades:

- Dado $H(x)$ é difícil encontrar x.
- Dados x e $H(x)$ é difícil encontrar $x' \neq x$ tal que $H(x') = H(x)$.
- É difícil encontrar quaisquer $x \neq x'$ tal que $H(x') = H(x)$.

1. Qual a designação usual para funções de *hash* que satisfazem cada uma destas propriedades? Na sua opinião, qual destas propriedades é mais difícil de garantir? Justifique.
2. Considere a seguinte construção que poderia ser utilizada como gerador de chaves numa cifra sequencial (K é a chave da cifra):

   - $k_0 = H(K)$
   - $k_{i+1} = H(k_i)$

   Qual/quais das propriedades enumeradas acima é importante para a segurança de uma cifra sequencial baseada neste gerador de chaves? Que outra propriedade seria imprescindível neste contexto? Justifique as suas respostas com base nas propriedades desejáveis para um gerador de chaves deste tipo.
3. Descreva e explique a utilização típica de funções de *hash* criptográficas no contexto das assinaturas digitais. Relacione com pelo menos uma das propriedades enunciadas acima.

Nome:_____ **Número:**_____ **Curso:**_____

Criptografia Aplicada

LESI / LMCC

Exame da 2^a Chamada – 28 de Janeiro 2006

Questão 4 Suponha que pretende obter um certificado de chave pública pessoal. A Autoridade de Certificação que resolveu contactar para esse efeito pertence a uma hierarquia de certificação reconhecida pela maioria das distribuições de sistemas operativos comerciais.

1. Explique o que entende por **pedido de certificado** indicando todas as parcelas de informação relevantes para este tipo de transacção.

2. Quais são as vantagens/desvantagens em escolher uma Autoridade de Certificação com estas características para o caso de querer **enviar** informação confidencial? E no caso de querer **enviar** informação autêntica e não repudiável? Justifique.

3. No caso de estimar que a utilização que irá dar ao seu certificado poderá, em caso de quebra de segurança, significar um prejuízo máximo de 100000 Euro, que documentos deveria consultar para verificar que a sua escolha é adequada? Justifique.

Nome:_____ **Número:**_____ **Curso:**_____

Criptografia Aplicada

LESI / LMCC

Exame da 2^a Chamada – 28 de Janeiro 2006

Questão 5 Considere o sistema PGP (Pretty Good Privacy).

1. Descreva o processo de troca de uma mensagem com garantias de confidencialidade, e não repúdio entre dois utilizadores. Que denominação genérica se dá a essa técnica?

2. Explique porque é que todos os certificados PGP são auto-assinados, fazendo um paralelo com o X.509.

3. Explique, de forma sucinta, o modelo de **Rede de Confiança** implementado pelo PGP.

Nome:_____ **Número:**_____ **Curso:**_____