Criptografia

MIETI

2º teste – 18 de Dezembro 2015

Questão 1 A cifra *one-time-pad* foi estudada no curso como um exemplo de uma cifra incondicionalmente segura. É legítmo afirmar-se que o RSA, utilizado como cifra, exibe essa mesma propriedade? Justifique.

Questão 2 Os certificados digitais são provavelmente o aspecto mais visível da utilização corrente da criptografia.

1. No que consiste um certificado de chave pública X509 e quais os problemas que estes procuram ultrapassar?

2. A utilização dos certificados pressupõe a sua validação. Descreva os principais passos envolvidos nesse processo.

3. Suponha que um utilizador A pretende enviar uma mensagem de correio electrónico cifrada e assinada para B. Explique os procedimentos envolvidos (no envio e na recepção) referindo em particular que certificados estão envolvidos e como são utilizados.

Questão 3 As assinaturas digitais consituem provavelmente o principal contributo oferecido pela criptografia assimétrica.

1. Quais as propriedades de segurança que as caracterizam, e como é que estas decorrem da utilização da primitiva assimétrica subjacente.

2. Nas assinaturas digitais estudadas, a assinatura é concatenada à mensagem assinada. Suponha então que A envia uma mensagem M juntamente com a respectiva assinatura a B. Não pode então um adversário I substituir a assinatura de A por a dele próprio, fazendo assim crer que a origem de M foi I e não A? Discuta/justifique convenientemente a sua resposta.

Questão 4 O *framework JCA/JCE* foi utilizado no âmbito do curso na codificação de soluções criptográficas em Java.

1. A tecnologia criptográfica é caracterizada por uma constante evolução (em termos de algoritmos, tamanhos recomendados para os segredos, etc.). Quais as características que destaca desse *framework* que permitem que ele não fique condenado a ficar também desactualizado?

2. O protocolo STS implementado durante o curso faz uso de assinaturas digitais. Apresente o esqueleto de código envolvido na verificação de uma assinatura digital.

Criptografia

MIETI

Teste intermédio – 13 de Novembro 2015

Questão 1 Considere uma cifra sequêncial síncrona (e.g. RC4).

1. Explique o princípio geral de funcionamento dessa cifra.
2. Porque motivo se recomenda que as chaves sejam utilizadas uma única vez? Ilustre com um ataque que tire partido da repetição da utilização da chave.
3. Comente, de forma fundamentada, a seguinte proposta de utilização da cifra RC4: "para aumentar a segurança oferecida pela cifra, procede-se a uma dupla operação de cifra (com uma mesma chave), i.e. Enc(k,M) = RC4(k,RC4(k,M))".

Questão 2 Considere os diferentes modos de operação das cifras por blocos.

1. Descreva de forma suscinta o modo ECB. Explique porque é que esse modo só deve ser utilizado para mensagens que não necessitem de mais do que um bloco.
2. Explique porque é que o modo CBC (*cipher block chaining*) ultrapassa as limitações apontadas.
3. Comente a seguinte afirmação: *mesmo quando utilizado para cifrar mensagens com um único bloco, o modo ECB é vulnerável ao ataque "codebook"*. Comente em particular se é (ou não) relevante a escolha do procedimento de *padding*.

Questão 3 Considere que um utilizador de um sistema multi-utilizador pretende garantir que é detectada qualquer tentativa de alterar o conteúdo de uma sua directoria por parte de um outro utilizador do sistema (em particular, pelo administrador). Sugira uma solução baseada em técnicas criptográficas que lhe forneça essa garantia.

Questão 4 Considere o protocolo de acordo de chaves *Diffie-Hellman*.

1. Descreve resumidamente o seu funcionamento e os aspectos de segurança relativamente a um adversário passivo e activo respectivamente.
2. Na codificação desse protocolo no *framework JCA/JCE* estão envolvidas várias *engine classes*. Explique, de forma sucinta, o papel exercido por cada uma dessas classes.
3. Para uma das classes referidas na alínea anterior (à sua escolha), descreva o respectivo padrão de utilização (i.e. as linhas de código correspondentes).