Criptografia

MIETI

Exame de recurso – 30 de Janeiro 2018

Questão 1

1. Explique a diferença entre os seguintes conceitos:
   - Segurança computacional vs. segurança absoluta;
   - Adversário passivo vs. adversário activo.
2. Forneca exemplos de técnicas que permitam "separar" os conceitos referidos na alínea anterior.

Questão 2 O *modo de operação* é um aspecto crucial na segurança da utilização de uma cifra por blocos.

1. Descreva um cenário onde a escolha inapropriada do modo de operação da cifra compromete a segurança. Justifique.
2. Como é que, nesse mesmo cenário, a escolha de um modo mais apropriado permite ultrapassar as falhas identificadas? Justifique.

Questão 3 Uma empresa na área da segurança desenvolveu um produto que consiste num par de *canetas USB* em que a chave para as operações de cifra/decifra é instalada aquando da respectiva produção de forma segura. A cifra adoptada é o `Salsa20` e o funcionamento pretendido é o seguinte:

- uma das *pens* é responsável por cifrar a informação, recebendo para o efeito 8 bytes (nonce) seguidos da mensagem a cifrar. Devolve o criptograma resultante.
- a outra *pen* é análoga, mas realiza a operação de decifrar.

1. O `Salsa20` é um exemplo de uma cifra sequencial síncrona que faz uso de um *Nonce*. Explique qual a utilidade desse mecanismo e impacto na usabilidade e segurança da cifra.
2. Considere o seguinte cenário de utilização: por forma a permitir que toda a gente possa comunicar de forma segura comigo, disponibilizo um computador num lugar público equipado com a *pen* responsável por cifrar a informação (mantendo a *pen* para decifrar em minha posse). Ao final do dia recolho os criptogramas e utilizo a minha *pen* para decifrar.
   (a) Entende que se pode afirmar que a confidencialidade dos ficheiros transmitidos está garantida? Justifique.
   (b) Ocorre-lhe alguma alternativa criptográfica para responder de forma mais prática e/ou mais segura aos requisitos apresentados? Justifique.

Questão 4 A criptografia assimétrica assenta na dificuldade computacional de certos problemas.

1. Refira exemplos de "problemas difíceis" empregues em criptografia e de técnicas concretas cuja segurança se baseie na intratabilidade desses problemas.

2. Comente a seguinte afirmação: *a criptografia assimétrica "desloca" o problema da pré-distribuição de chaves para o da autenticação das chaves.*

3. Refira como é que, na prática, o problema da autenticação das chaves é minorado/ultrapassado? (obs: justifique em particular qual dos termos minorado/ultrapassado entende mais apropriado).

Questão 5

1. As *assinaturas digitais* e os *message authentication codes* foram duas das técnicas estudadas no curso. Descreva as similaridades e as diferenças que é possível estabelecer entre essas técnicas, em particular ao nível das propriedades associadas.

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 pela sua própria (fazendo assim crer a B que a origem de M foi I)? (obs: discuta/justifique convenientemente a sua resposta).

3. A utilização de *certificados de chave pública* altera o sentido da resposta dada na alínea anterior? Justifique.

Questão 6 O *envelope digital* (*hybrid encryption*) combina técnicas simétricas e assimétricas.

1. Explique o seu funcionamento e quais as vantagem que traz relativamente à utilização isolada de cada uma dessas técnicas.

2. Refira uma aplicação concreta desse mecanismo de entre os protocolos/aplicações estudadas no curso.