

**Questão 1) [1 + 1 + 1 + 1 + 1 + 2 + 1 valores]**

- a) Uma das noções interessantes no sistema PGP que apresenta vantagens em ser aplicada a qualquer sistema de correio electrónico seguro é a noção de assinatura desacoplada (ou *detached signature*). Diga em que consiste esta noção tal como é suportada em PGP e refira pelo menos três possíveis vantagens que essa noção propicia.

- b) No sistema PGP as mensagens confidenciais cifradas com algoritmos simétricos adoptam o modo CFB. Opcionalmente poder-se-ia adoptar o modo CBC para se ter um nível de segurança equivalente dado o propósito da confidencialidade em PGP. Porque é que no entanto se usa CFB e não CBC ?

Notar que para um método criptográfico simétrico e uma chave  $k$

$$C_i = \{ C_{i-1} \text{ xor } P_i \}^k ; P_i = C_{i-1} \text{ xor } \{ C_i \}^k \quad \text{em CBC}$$

$$C_i = P_i \text{ xor } \{ C_{i-1} \}^k ; P_i = C_i \text{ xor } \{ C_{i-1} \}^k \quad \text{em CFB}$$

- c) Na geração de classes de segurança de certificados X509v3 para uso desses certificados de forma compatível com a norma S/MIME existem diferenças importantes. Apresente as diferenças entre essas classes de certificados de segurança com base no procedimento tipo de autoridades de certificação, utilizando como o exemplo os certificados para S/MIME emitidos pela Verisign.

Tipo de classe: \_\_\_\_  
Pressuposto:

Tipo de classe: \_\_\_\_  
Pressuposto:

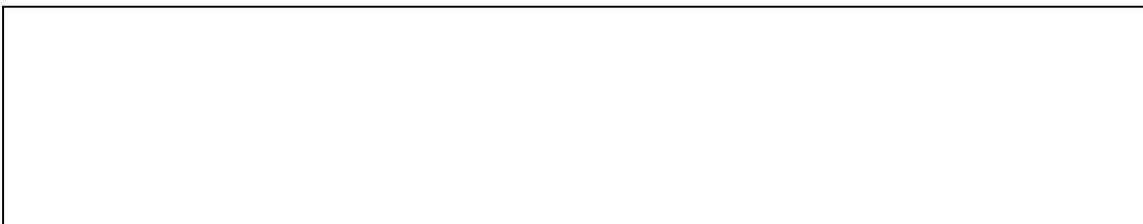
Tipo de classe: \_\_\_\_  
Pressuposto:

- d) Clarifique e estabeleça de forma rigorosa as diferenças associadas às noções de “conexão SSL” e “sessão SSL”.

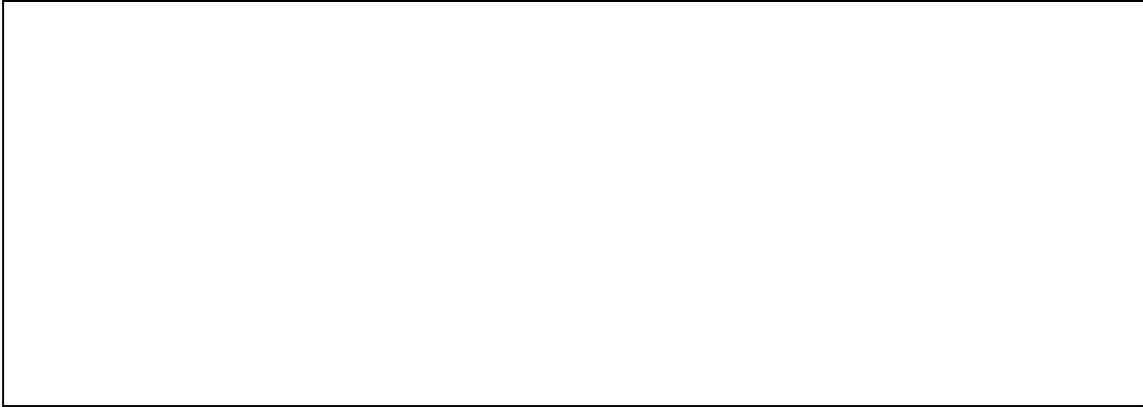
- e) Enumere as tipologias ou diferentes métodos de autenticação e estabelecimento de chaves que podem ser suportadas opcionalmente em SSL ou TLS. Diga em que consiste cada tipologia e argumente sobre as que considera mais robustas do ponto de vista de segurança.



- f) Na norma SET quantos certificados de chave pública têm que ser mantidos por uma entidade actuando como comerciante (*Merchant*) ? Para que servem ?



- g) Quais os métodos variantes de autenticação (e possíveis sub-variantes) estão definidos na especificação do protocolo SSH ? Indique em que consistem e quais são especificadas como minimamente obrigatórias numa implementação do protocolo.



**Questão 2 (sobre o protocolo SSL ou TLS) [1 + 2 valores]**

- a) A funcionalidade do sub-protocolo *ChangeCypherSpec* do protocolo SSL poderia ser integrada como uma sub-fase final do próprio sub-protocolo *Handshake*. No entanto, esses sub-protocolos são concebidos de forma que a sua especificação e possível materialização seja independente. Que vantagens encontra nessa independência do ponto de vista da especificação SSL e da sua implementação concreta ? Justifique a sua resposta.
- b) “Embora numa primeira análise se possa referir que um protocolo como o TLS é independente do transporte (UDP ou TCP), a verdade é que numa análise mais detalhada, do ponto de vista de segurança, é pouco adequado ou inapropriado que as mesmas garantias sejam estabelecidas num ou noutro transporte”. Critique esta frase e apresente uma argumentação a favor ou contra a mesma.

**Questão 3 (SET) [1 + 1 + 1 valores]**

Considere a terminologia de língua inglesa associada ao protocolo SET por facilidade de interpretação da pergunta. Diga como é que o protocolo SET e os pressupostos da sua especificação formal garantem a um consumidor (*Cardholder*) o seguinte:

- a) Que o valor de uma aquisição não possa ser cobrado duas vezes por um comerciante (*Merchant*) fraudulento ou incorrecto.
- b) Que um comerciante não proceda a uma cobrança múltipla de um mesmo produto adquirido por um mesmo consumidor através de dois *Payment Gateways* de duas entidades *Acquirer*.
- c) Que um comerciante não cobra o crédito de uma compra, sem poder exhibir uma garantia de não-repudição que prove que o consumidor já recebeu e aceitou o produto de uma compra.

**Questão 4 (PGP) [1,5 + 1,5 valores]**

**Considere o sistema PGP**

- a) Porque é que para suportar mensagens confidenciais e autênticas usando compressão, as assinaturas são sempre calculadas e geradas antes da operação de compressão ? Indique pelo menos duas razões para justificarem claramente essa opção.
- b) Numa mensagem passada num canal partilhado, um atacante capaz de realizar ataques do tipo “*traffic-analysis*” e “*packet-sniffing*” consegue determinar pelo menos quais são os primeiros 16 bits da síntese subjacente a uma assinatura. Se tal é possível, diga em que medida é que a exposição desses 16 bits não reduz em nada a segurança do sistema PGP.

**Questão 5 (Sobre a especificação SSH e contexto de estudo de trabalho prático efectuado)**

**Deve responder à alínea a) e pelo menos a uma das alíneas b), c) ou d)**  
**[cotação: 2 + 1 valores]**

- a) Diga que contra-medidas ou garantias são fornecidas pelo protocolo SSH para resistir às seguintes tipologias de ataques:
- A1 Ataques de dicionário, do tipo “*known plaintext*” às mensagens do protocolo que transportam passwords no caso de autenticação por *passwords*
  - A2 Retransmissão ilícita de mensagens (message replay)
  - A3 Password *Sniffing*
  - A4 Ataques de dicionário a senhas (passwords) de utilizadores
  - A5 *IP Spoofing*
  - A6 *IP Hijacking*
  - A7 *SYN Flooding*

**----- RESPONDA PELO MENOS A UMA DAS SEGUINTE ALÍNEAS**

- b) Que modelos de confiança estão normalizados na especificação SSH para assegurar que as ligações ou associações correctas entre nomes de computadores (*hostnames*) e as chaves públicas desses computadores (*hostname public keys*) são confiáveis ?
- c) Considerando o seu estudo da especificação e teste de execução do protocolo SSH nas diversas variantes de autenticação, diga como se estabelece o princípio de suporte de revogação ou alteração de chaves públicas de computadores funcionando como clientes ou servidores SSH.
- d) Considere o modo de autenticação por *passwords* e seu processamento de acordo com a especificação SSH. Suponha que um computador cliente processa e representa passwords em formato ISO-8859-1 LATIN, por exemplo, enquanto outro cliente utiliza outra forma de representação, ex., ISO-10646 UTF-8. Diga se ao nível do formato das mensagens do protocolo SSH trocadas entre esses dois clientes e um mesmo servidor seria possível notar qualquer diferença associada àquele facto.