Anexo

Perguntas de Exames

Neste anexo são apresentadas perguntas relativas aos conteúdos dos vários capítulos do livro. As perguntas estão organizadas segundo a divisão por capítulos do livro e, no final, na secção A.11, há um grupo de perguntas que abrangem conteúdos apresentados em diversos capítulos.

Estas perguntas não foram especialmente elaboradas para este livro; elas foram efetivamente usadas em exames concebidos pelo Autor para disciplinas de Segurança Informática no IST e na Universidade de Aveiro, pelo que a sua adaptação para este livro foi diminuta. Por essa razão, é normal que existam perguntas semelhantes, ou perguntas diferentes para a mesma resposta ou ainda perguntas que forneçam a resposta a outras. Finalmente, é esse ainda o motivo para a não existência de um número de problemas homogéneo por cada capítulo.

A.1 Introdução

1. Explique a diferença entre uma política de segurança e um mecanismo desegurança. Dê um exemplo envolvendo autenticação de pessoas.

2. Quando se fala em segurança importa considerar duas vertentes: políticase mecanismos. Indique, justificando, quais das seguintes expressões referem políticas ou mecanismos e, para cada política, descreva uma situação concreta em que seja usado um dos mecanismos indicados: a) Confinamento.
   b) Autenticação.
   c) Princípio do privilégio mínimo.
   d) Autorização.

3. Explique e relacione os seguintes conceitos:
   a) Vulnerabilidade.
   b) Ataque.
   c) Risco/ameaça.
   d) Defesa.

4. No âmbito dos sistemas computacionais:
    a) Explique a relação que existe entre vulnerabilidades, ataques, riscos e defesas.
    b) Dê um exemplo que abarque todos os conceitos acima referidos.
5. No âmbito dos sistemas computacionais:
    a) Explique a relação que existe entre vulnerabilidades e riscos.
    b) Quais as vantagens e desvantagens de eliminar riscos em vez de eliminar vulnerabilidades.
6. No âmbito dos sistemas computacionais:
    a) Explique o conceito de domínio de segurança.
    b) Qual a relação que deverá existir entre (i) o desenho e planeamento de redes locais e da sua ligação à Internet e (ii) a implantação de domínios de segurança.
7. Considere o princípio do privilégio mínimo. Indique vantagens e desvantagens operacionais decorrentes da sua aplicação em abstrato.

A.2Criptografia

1. Explique como funciona a construção HMAC, usada no cálculo de um MAC (*Message Authentication Code*).
2. Explique que vantagens advêm da utilização conjunta de funções de síntesee cifras assimétricas no cálculo, transmissão e validação de assinaturas assimétricas.
3. O modo de cifra OFB (*Output FeedBack*) só usa cifra por blocos, mas não decifra. Explique porquê, descrevendo para o efeito cifras e decifras com OFB.
4. A cifra RSA baseia a sua segurança em duas propriedades: dificuldade nafatorização de grandes números e dificuldade no cálculo de logaritmos discretos de grandes números. Explique porquê.
5. Uma cifra contínua é uma aproximação prática e viável da cifra *one-time pad* de Vernam. Explique esta afirmação, usando para o efeito diagramas ilustrativos da operação de ambas as cifras.
6. Explique por que razão as cifras assimétricas, tal como a RSA, são realizadassobre valores que incluem (i) o conteúdo que se quer efetivamente cifrar, (ii) uma marca constante e (iii) um valor aleatório.

7. Um MAC pode ser calculado com uma cifra por blocos em modo CBC da mensagem (método conhecido como DES-MAC). Explique:
   a) Por que razão não se pode considerar que uma qualquer mensagem cifrada com uma cifra por blocos em modo CBC tem implicitamente um MAC?
   b) Como se poderia modificar trivialmente a mensagem para resolver esse problema (isto é, passar a conter implicitamente um MAC)?
8. Indique as propriedades que distinguem as funções de síntese (*digest*) de outras funções de dispersão (*hashing*).
9. Uma cifra contínua não deve ser usada com a mesma configuração inicial (VIe chave) para cifrar mensagens diferentes. Explique porquê.
10. Explique detalhadamente (configuração e exploração) como se usam os MACpara autenticar mensagem trocadas entre dois interlocutores. (**Atenção: não descreva nenhuma função MAC em particular!**)
11. Considere o modo de cifra 3DES EDE (*Triple DES Encrypt-Decrypt-Encrypt*). Explique:
    a) Como funciona?
    b) Quais são as suas vantagens e desvantagens, face ao DES (*Data Encryption Standard*)?
12. Indique, de forma tão aproximada quanto possível, qual é o desempenho (ouseja, custo por *bit* cifrado) de uma cifra contínua que use um gerador *n-bit* OFB.
13. Considere os modos de cifra OFB e CBC (*Cipher Block Chaining*). Indique, justificando, que consequência tem, para o decifrador, a existência de um único *bit* errado num criptograma (por exemplo, devido a um erro na transmissão).
14. Nas cifras por blocos quanto maior for a dimensão do bloco (em *bits*), maior é em regra a segurança fornecida pela cifra. Explique porquê.
15. Um MAC é uma forma de proteger a integridade de uma mensagem.
    a) Dê um exemplo (explicando-o) de um MAC usando apenas uma função de cifra.
    b) Explique como funciona a construção HMAC, usada no cálculo de um MAC.
16. Considere o modo de cifra *n-bit* CTR (*Counter*).
    a) Explique como funciona.
    b) Como faria para decifrar B octetos de uma mensagem com M octetos, a partir do deslocamento b (em octetos) usando *n-bit* CTR?

17. Explique o princípio geral de operação de uma cifra assimétrica.
18. Explique o princípio geral de operação da criptanálise, usando:
    a) Texto conhecido
    b) Texto escolhido.
19. Se considerar que tem N entidades, e que entre elas pretende criar canais de comunicação secretos bidirecionais, que vantagens apresentam as cifras assimétricas face às simétricas para resolver esse problema?
20. Explique como é que uma rede de Feistel, usada em inúmeras cifras simétricas por blocos, permite realizar operações de cifra (que têm de ser invertíveis) usando internamente uma função não invertível.
21. Explique com pormenor o que significam os seguintes conceitos:
    a) Cifra monoalfabética.
    b) Cifra polialfabética.
22. Considere o uso de esteganografia em vez de criptografia para assegurar a privacidade dos dados. Explique:
    a) Qual a vantagem da esteganografia.
    b) Porque é que não é normalmente usada.
23. Considere as cifras polialfabéticas. Indique:
    a) O que é o período de uma cifra polialfabética.
    b) Uma técnica para descobrir o período (descreva a técnica com algum pormenor).
24. Explique qual o modelo geral de operação de uma cifra contínua, ilustrando-o com um diagrama.
25. Uma cifra contínua é uma cifra monoalfabética ou polialfabética? Justifique.
26. Uma cifra contínua propaga erros na decifra de um criptograma com erros?Justifique a sua resposta.
27. Uma cifra por blocos é uma cifra monoalfabética ou polialfabética? Justifique.
28. Qual é a vantagem da criptografia assimétrica, em relação à simétrica, para a comunicação confidencial de dados?

29. Qual é a desvantagem da criptografia assimétrica, em relação à simétrica,para a comunicação confidencial de dados?
30. O que é a cifra híbrida, ou mista, e por que razão é usada (por exemplo, noPGP – *Pretty Good Privacy*).
31. Considere as operações de compressão e cifra. Indique, justificadamente, asvantagens e desvantagens relativas da sua aplicação pela ordem indicada ou pela ordem inversa.
32. Um dos objetivos de usar blocos de grande dimensão (64, 128, 256 ou mais*bits*) com cifras por blocos é o de esconder padrões (um problema clássico das cifras monoalfabéticas), mas tal intento pode, mesmo assim, ser defraudado em inúmeras circunstâncias. Indique como se pode atuar para complicar a localização de padrões em criptogramas gerados com cifras por blocos.
33. As cifras por blocos atuais são cifras de substituição monoalfabéticas. Comoé que nas mesmas se escolhe o alfabeto de substituição e por que razão são muito mais robustas que as versões manuais ou mecânicas antigas face a ataques que tentem explorar estruturas linguísticas bem conhecidas (por exemplo, frequência de letras isoladas, de digramas, de trigramas, etc.).
34. Uma grande parte das cifras por blocos atuais, entre as quais o DES, usamrepetidas vezes um bloco elementar designado por rede de Feistel. Explique qual a principal vantagem operacional desse bloco, a qual impede a aplicação simultânea de difusão e confusão, através da função *f*, aos dois fluxos de informação (notar que $L_i = R_{i-1}$ é independente de *f*).
35. As cifras modernas por blocos usam unidades internas de permutação, substituição, expansão e compressão de blocos de *bits*. Explique, justificando, quais delas contribuem para a difusão apresentada pela cifra (a difusão é um dos critérios práticos de desenho de cifras indicados por Shanon, juntamente com a confusão).
36. A única cifra teoricamente segura, conhecida como *one-time pad*, não é fácil de usar. Em sua substituição usam-se cifras contínuas, que introduzem vulnerabilidades mas que são muito mais fáceis de usar. Explique porquê.
37. Considere as cifras contínuas e explique:
    a) De que maneira são uma aproximação prática da cifra *one-time pad* de Vernam.
    b) Quais são as implicações práticas dessa aproximação em relação ao volume de dados cifrados com a mesma chave.

38. Uma cifra contínua habitual (uma que não a de Vernam) deve ser usada com alguns cuidados para não ser facilmente criptanalizada. Indique dois desses cuidados.

39. A renovação de chaves simétricas deverá ser feita segundo dois critérios: (i) dados como ela cifrados e posteriormente expostos em ambientes inseguros e (ii) tempo de uso. Explique quais as vulnerabilidades que se pretende evitar com cada um dos critérios.

40. Por que razão o tempo de vida dos pares de chaves assimétricas é normalmente (muito) superior ao tempo de vida das chaves simétricas usadas em interações entre duas ou mais entidades?

41. As cifras assimétricas são cifras computacionais modernas que não são passíveis de ser aplicadas manualmente por operadores de cifra. Explique porquê.

42. A cifra assimétrica RSA é uma cifra por blocos. Indique a natureza e a dimensão dos blocos tendo em conta os valores usados pela cifra.

43. Considere a cifra assimétrica RSA. Admitindo que está a usar um módulo (n) de 1025 *bits*, qual o número mínimo de operações de cifra que é necessário fazer para cifrar completamente uma mensagem de 256 octetos (Nota: Use os arredondamentos que considerar mais ajustados).

44. A segurança da maioria dos algoritmos assimétricos atuais baseia-se na existência de problemas matemáticos complexos. Indique quais são esses problemas para o RSA e para o ElGamal.

45. O modo de cifra OFB permite transformar uma cifra por blocos numa cifracontínua. Explique como.

46. O modo de cifra OFB permite transformar uma cifra por blocos numa cifracontínua. Admitindo que a cifra por blocos usa blocos de B *bits*, qual o comprimento máximo absoluto do período, em *bits*, da cifra contínua *n-bit* OFB?

47. O modo de cifra CFB (*Cipher FeedBack*) permite transformar uma cifra por blocos numa cifra contínua. Explique como.

48. É correto dizer que o modo de cifra CBC transforma um algoritmo de cifra por blocos monoalfabético numa cifra por blocos polialfabética? Explique porquê.

49. A alteração de um criptograma cifrado como o modo de cifra CBC permite alterar deterministicamente (ou seja, de forma garantida) alguns *bits* dos dados recuperados após a sua decifra. Explique como, ilustrando de forma clara a justificação.

50. Por que razão não é aconselhável usar uma única chave de cifra e uma cifracontínua para cifrar vários conteúdos independentes (por exemplo, vários ficheiros)? Assuma que para todos eles é usado igualmente o mesmo vetor de iniciação.

51. O modo de cifra CBC permite uma melhor camuflagem de padrões no textoem claro. No entanto, a igualdade ocasional de quaisquer dois blocos do criptograma (ou seja, $C_i = C_j, i \neq j$) permite deduzir alguns padrões, ou mesmo blocos do texto em claro, sem ter que saber qual o algoritmo de cifra ou mesmo a chave concreta usada. Explique como.

52. Compare os modos de cifra por blocos ECB (*Electronic Code Book*) e CBC quanto aos seguintes aspetos:

    a) Paralelização (considere separadamente cifras e decifras).
    b) Propagação de erros na decifra de um criptograma com um bloco corrompido.

53. Compare os modos de cifra por blocos ECB e CBC quanto aos seguintes aspetos (considere separadamente cifras e decifras):

    a) Paralelização.
    b) Acesso aleatório rápido a qualquer bloco.

54. Compare os modos de cifra por blocos CFB e OFB quanto aos seguintes aspetos:

    a) Paralelização (considere separadamente cifras e decifras).
    b) Pré-processamento (para aumentar eficiência).

55. Compare os modos de cifra por blocos CBC e OFB quanto aos seguintes aspetos:

    a) Paralelização (considere separadamente cifras e decifras).
    b) Pré-processamento (para aumentar a eficiência).

56. Considere o modo de cifra CTR, que permite transformar uma cifra por blocosnuma cifra contínua. Explique: a) Como funciona.
    b) Como se consegue com o mesmo obter acesso aleatório rápido (ou homogéneo).

57. Inicialmente o Kerberos usava o modo de cifra PCBC (*Propagating Cipher Block Chaining*) que supostamente permitiria uma melhor propagação de erros resultantes de criptogramas errados. O PCBC é semelhante ao CBC, mas tem uma realimentação adicional na cifra e decifra:

$$C_i = E_K(P_i \oplus P_{i-1} \oplus C_{i-1})$$

$$P_i = D_K(C_i) \oplus P_{i-1} \oplus C_{i-1}$$

No entanto, se se trocarem dois blocos consecutivos do criptograma ($c_i = C_{i+1}$ e $c_{i+1} = C_i$), a decifra do bloco seguinte C_{i+2} já não evidencia qualquer erro. Demonstre esse facto.

58. Considere a técnica criptográfica designada por cifra mista. Indique:
    a) Como se usa essa técnica.
    b) Por que razão é usada.
59. Normalmente a cifra tripla é executada usando cifra-decifra-cifra (EDE – *Encrypt-Decrypt-Encrypt*), com uma, duas ou três chaves distintas. Explique qual a vantagem operacional de se usar a conjugação EDE em vez de, por exemplo, só cifras (EEE).
60. Uma das técnicas para ampliar a segurança de um algoritmo de cifra por blocos, conhecida por branqueamento (*whitening*), baseia-se na introdução de confusão antes e depois da operação de cifra/decifra. Explique como tal é feito e qual o comprimento máximo equivalente da chave de cifra que se pode usar nesta técnica.
61. Indique qual é o modelo geral de funcionamento interno de uma função de síntese.
62. Explique como é que as funções de síntese mais comuns (MD5 ou SHA-1) operam de forma a calcularem um valor de dimensão constante a partir de uma mensagem dimensão arbitrária.
63. A qualidade de uma função de síntese mede-se segundo três características: (i) resistência à descoberta de um texto, (ii) resistência à descoberta de um segundo texto e (iii) resistência à colisão. Explique em que consiste cada uma destas características.
64. Uma função de síntese deverá dificultar a descoberta de uma segunda pré-imagem, ou seja, dado uma pré-imagem M e a sua síntese $h(M)$, deverá ser computacionalmente difícil descobrir uma segunda pré-imagem M' tal que $h(M) = h(M')$. Explique a relevância desta propriedade no contexto da assinatura digital de documentos.
65. As funções de síntese devem dificultar a descoberta de colisões. Explique:
    a) Em que consiste essa descoberta.
    b) Qual o risco da descoberta de colisões no âmbito da validação de assinaturas digitais calculadas sobre valores calculados com funções de síntese.

66. Quando se afirma que uma função de síntese é não invertível, o que matematicamente é óbvio porque não é bijetiva, o que se quer dizer concretamente?

67. Uma função de síntese é muitas vezes referida como sendo uma função dedispersão unidirecional. Explique exatamente, e tão formalmente quanto souber, o que se significa neste caso o conceito de unidirecionalidade.

68. As funções de síntese devem dificultar a descoberta do texto original sintetizado e a descoberta de um segundo texto, diferente do original, que produza a mesma síntese. Dê um exemplo concreto do interesse da segunda dificuldade.

69. Um MAC pode ser calculado de várias maneiras a partir de uma mensagem e de uma chave secreta partilhada. Indique:

    a) Uma que faça uso apenas de de operações de cifra e somas módulo 2 ($\oplus$).
    b) Uma que faça uso apenas de funções de síntese.

70. Um MAC é um meio de autenticação de dados. Explique duas formas de oscalcular usando cifras por blocos ou funções de síntese.

71. Explique como funciona o cálculo de um MAC com recurso a uma cifra por blocos e ao modo de cifra CBC.

72. Um MAC é um meio de autenticação de dados. Indique uma forma de calcular um MAC sem recorrer a funções de síntese.

73. Um MAC é um meio de autenticação de dados. Explique por que razão nãopode ser usado para provar a autoria dos dados perante terceiros (ou, por outras palavras, por que razão permite repúdio de origem).

74. Qual a diferença entre um valor de síntese e um MAC e qual a relação naturalque pode existir, e que na prática é explorada, entre as funções de síntese e as funções que geram os MAC.

75. Pensando apenas no universo dos recetores de informação, em que casos fazsentido usar os MAC ou assinaturas digitais para autenticar a informação emitida para esses recetores?

76. Um MAC é um meio de autenticação de dados de um para poucos (tipicamente de um para um) enquanto uma assinatura digital é um meio de autenticação de dados de um para muitos. Indique, justificando, qual a razão técnica para a diferença referida entre os dois métodos de autenticação de dados.

77. A função HMAC usa funções de síntese para gerar um MAC de acordo coma seguinte fórmula:

$$HMAC(m) = H(K|opad|H(K|ipad|m))$$

onde m é uma mensagem, K uma chave, $opad$ e $ipad$ excipientes de alinhamento e H uma função de síntese (MD5, SHA-1, etc.). Explique:

a) O que é um MAC.

b) O que faz com que o resultado da função HMAC seja considerado um MAC e não o simples resultado de uma função de síntese.

78. As assinaturas digitais são normalmente concretizadas sobre sínteses de documentos e não sobre os mesmos. Explique: a) Por que razão se usa essa aproximação.

b) Quais das três características de qualidade indicadas na alínea anterior são críticas para se poder usar esta aproximação.

79. Uma assinatura digital de um documento é normalmente feita cifrando umasíntese do documento com a chave privada de um par de chaves assimétricas. Essa síntese deverá ser produzida por uma boa função de síntese. Indique: a) Que propriedades deverá ter essa função para ser considerada boa.

b) Qual delas é crítica para a segurança do mecanismo de assinatura digital referido.

80. Explique qual o modelo geral de funcionamento de uma cifra contínua concretizada explorando uma cifra por blocos. Ilustre a sua resposta com um diagrama.

81. Explique, ilustrando a sua resposta com um diagrama e com provas matemáticas, por que razão uma cifra por blocos em modo CBC é comparável, em termos de resultado final, a uma cifra polialfabética.

82. Explique como opera a cifra assimétrica RSA, ilustrando a sua explicação comas expressões matemáticas da cifra (não precisa de explicar processo de geração das chaves, apenas a sua constituição).

83. Qual é relação entre o Paradoxo do Aniversário e a aferição do limite máximo da robustez de uma função de síntese à descoberta de colisões? Ilustre a sua resposta com um exemplo.

84. Um MAC é um meio de autenticação de dados. Explique como pode ser usado para garantir uma sequência correta de mensagens enviadas e recebidas (por exemplo, pacotes UDP) num fluxo de mensagens bidirecional entre duas entidades.

85. O modo de cifra CTR permite a concretização de uma cifra contínua com capacidade de acesso aleatório uniforme. Explique: a) Em que consiste esta característica?
    b) Como é que o modo CTR consegue ter essa característica?

86. As funções de síntese (*digest*) devem dificultar a descoberta de um segundo texto que produza a mesma síntese de outro texto. Explique, de forma pormenorizada, a relevância deste requisito para a segurança das assinaturas digitais.

87. Um MAC é um meio de autenticação de mensagens. Explique:
    a) Que semelhanças possui, ou não possui, com as assinaturas digitais?
    b) Como pode ser concretizado apenas com uma função de cifra em modo CBC?

88. A segurança da cifra RSA depende da dificuldade de cálculo de logaritmos discretos de números de grande dimensão. Explique porquê, recorrendo às expressões matemáticas que descrevem a operação do RSA.

89. As assinaturas digitais são normalmente acompanhadas por um ou mais certificados de chave pública. Indique: a) Que certificados são esses?
    b) Por que razão eles são enviados juntamente com a assinatura?

A.3 Gestão de chaves públicas

1. Considere o problema da revogação de um certificado de chave pública. Explique:
   a) O que é uma lista de certificados revogados (CRL – *Certificate Revocation List*)?
   b) Quem a deve usar?
2. Considere o conceito de certificado de chave pública X.509. Explique:
   a) Para que servem estes certificados?
   b) Quem produz estes certificados?

3. Um certificado de chave pública é um documento com um prazo de validade.
    a) Como é definido esse prazo?
    b) Como se pode verificar se estava válido numa determinada data, diferente da atual?
4. Como se estabelece à escala mundial a confiança nas Entidades Certificadoras?
5. Considere o Cartão de Cidadão.
    a) Que importância tem o facto de os pares de chaves do seu titular serem gerados internamente?
    b) Que limitações existem pelo facto de apenas disponibilizar cifra (assinatura) com as chaves privadas, mas não decifra?
6. As assinaturas digitais realizadas sobre documentos são normalmente acompanhadas por um ou mais certificados de chave pública. a) Quais são esses certificados?
    b) Qual é o interesse em os transmitir?
7. Considere o problema da revogação de um certificado de chave pública. Explique:
    a) A diferença entre uma CRL e uma delta CRL.
    b) A relação entre uma CRL e o serviço OCSP (*Online Certificate Status Protocol*).
8. Considere a gestão de chaves públicas. Explique:
    a) O que é uma cadeia de certificação?
    b) Em que consiste exatamente uma raiz confiável de uma cadeia de certificação?
9. Explique por que razão a validação de assinaturas digitais implica a existência de certificados de chave pública.
10. Existem dois tipos de listas de revogação de certificados (CRL). Indique:
    a) Quais são estes dois tipos?
    b) Para que serve cada um deles (incluindo a relação entre ambos)?
11. Considere a norma PKCS #11 (*Public Key Cryptography Standard #11*):
    a) Em que consiste?
    b) Qual é a sua relação com o Cartão de Cidadão?

12. O Cartão de Cidadão é um elemento fundamental para suportar a atividade de assinatura digital pessoal. Que serviços presta nesse sentido? (**Sugestão: considere, para este efeito, todos os objetos criptográficos geridos pelo Cartão de Cidadão**).

13. Considere o conceito de certificação cruzada.

    a) Em que consiste?

    b) Em que situações ela pode ser vantajosa, face a outras (por exemplo, hierárquica).

14. O Cartão de Cidadão permite proteger a chave privada do seu titular.

    a) Qual é o objetivo último dessa proteção?

    b) Indique as políticas e mecanismos que são usadas(os) nessa proteção.

15. A gestão de um par de chaves assimétricas envolve a sua geração, a proteção da chave privada, a distribuição da chave pública e o tempo de vida do par. Explique os problemas que importa resolver em cada um destes quatro tópicos.

16. Considere a gestão de chaves públicas. Explique por que razão a distribuição e armazenamento de chaves públicas pelos seus utentes têm que ser fidedignas.

17. Explique em que medida, e porquê, os *smartcards* são úteis na exploração dos pares de chaves assimétricas.

18. Explique em que consiste um certificado de uma chave pública e por que razão se usam tais certificados.

19. Um certificado de uma chave pública é um documento assinado por uma ou mais entidades. A razão de ser de existirem várias assinaturas depende do modelo de certificação. Indique qual o objetivo de poderem existir várias assinaturas num dado certificado PGP e qual a relação que existe entre as mesmas.

20. Explique o que é, para que serve e como é usada uma cadeia de certificação.

21. Um certificado de chave pública Auta assinado, só por si, não tem qualquer valor prático. Explique:

    a) Em que é que consiste tal certificado.

    b) Em que circunstâncias é usado.

    c) O que faz com que o mesmo tenha, de facto, alguma utilidade.

22. Considere a gestão de chaves públicas. Explique:

a) O que é um certificado de uma chave pública.

b) Como se pode limitar o tempo de vida dos certificados emitidos por uma Entidade Certificadora.

23. Um *smartcard* não é um mero circuito de memória, mas possui um processador e até capacidades de execução de funções criptográficas complexas e de geração de valores aleatórios. Explique a utilidade destas duas últimas capacidades.

24. O Cartão de Cidadão é um *smartcard* que permite efetuar assinaturas digitais qualificadas. Por omissão, essa funcionalidade está desativada no ato de entrega do cartão, podendo ser solicitada a sua ativação pelo titular. Explique como, tecnicamente, essa ativação é concretizada.

25. Os certificados de revogação de chaves públicas são, muitas vezes, críticos para uma correta utilização dos certificados de chaves públicas. Explique: a) O que são.

    b) Como e quando são gerados.

    c) Como são usados.

26. Considere a revogação de certificados de chaves públicas. Explique:

    a) Em que consiste um certificado de revogação.

    b) Por que razão é preciso manter e consultar listas de certificados de revogação.

27. Explique para que serve o protocolo OCSP e em que circunstância deve serusado.

28. Qual a vantagem de cada entidade, pessoa ou serviço, usar dois pares de chaves assimétricas independentes para suportar cifra de conteúdos e autenticação de conteúdos com assinatura digital (um par para cada fim)?

29. Considere os repositórios pessoais de certificados confiáveis. Explique:

    a) Por que razão este repositório tem de ser convenientemente protegido.

    b) Conceba e descreva sucintamente um ataque onde esse repositório seja usado.

30. Considere os certificados digitais de chaves públicas. No caso do PGP as chaves públicas são certificadas por múltiplas entidades, enquanto na maioria dos outros casos as chaves públicas são certificadas apenas por uma entidade. Explique:

    a) Qual a razão filosófica subjacente a esta diferença.

    b) Quais as dificuldades operacionais que se colocam ao PGP para tornar útil a certificação múltipla.

31. Uma das funções de uma infraestrutura de apoio ao uso de chaves públicas(PKI – *Public Key Infrastructure*) é a definição de cadeias de certificação. Na prática, o que é que tal definição acarreta?

32. Uma das funções de uma infraestrutura de apoio ao uso de chaves públicas(PKI) é a publicação de listas de certificados de chaves públicas revogadas. Explique:

    a) O que é um certificado de uma chave pública revogada.
    b) Qual a razão para a publicação das listas referidas.
    c) O que pode levar a revogar uma chave pública certificada.

33. Muitas vezes envia-se, juntamente com um documento e com uma sua assinatura digital, toda uma hierarquia de certificados de chaves públicas que podem ser úteis ao(s) recetor(es). A que hierarquia nos estamos a referir e como é que ela pode ser útil.

34. Considere a gestão de chaves públicas. Explique:

    a) O que é uma cadeia de certificação de chaves públicas?
    b) Em que consiste, tecnicamente, o conceito de certificação cruzada.

35. O PGP não requer para o seu funcionamento quaisquer infraestruturas centrais de apoio. No entanto, atualmente usam-se servidores centrais públicos e de uso aberto para facilitar a utilização do PGP. Explique com que propósito foram criados esses servidores.

36. No PGP existem dois atributos para classificar uma chave pública alheia: validade e confiança. Explique o que significa cada um deles e quais as combinatórias possíveis dos mesmos (de entre as quatro possíveis).

37. Considere o conceito de certificação *ad hoc*. Explique:

    a) Em que consiste.
    b) Quais são as suas vantagens políticas (ou seja, não técnicas).

38. O PGP usa uma certificação de chaves públicas *ad hoc* (*web of trust*) que obriga cada utilizador da ferramenta a gerir dois tipos de confiança em relação a chaves públicas alheias. Explique:

    a) Quais são esses tipos de confiança.
    b) Qual a relação entre os mesmos.

39. O PGP usa uma certificação de chaves públicas *ad hoc* (*web of trust*) que obriga cada utilizador da ferramenta a gerir dois tipos de confiança em relação a chaves públicas alheias: correção e confiança no seu dono. Explique: a) Qual a relação entre esses dois tipos de confiança.
    b) Quais deles podem ser transmitidos a terceiros através da *web of trust*.

40. Explique, exemplificando com o Cartão de Cidadão, por que razão os *smartcards* são úteis para a implantação de infraestruturas de chave pública (PKI).

41. Considere o problema da validação de um certificado de chave pública. Explique, com pormenor, quais as vantagens e desvantagens de usar listas de certificados revogados (CRL) ou serviços OCSP pela entidade validadora.

42. Um certificado de chave pública X.509 certifica, para além de uma chave pública, o fim a que a mesma se destina.

    a) Qual é, de entre vários existentes, o interesse primordial da certificação de uma chave pública?
    b) Indique três tipos de fins a que se pode destinar uma chave pública certificada (lembre-se do Cartão de Cidadão).

43. As cadeias de certificação terminam quando se atingem certificados declarados como confiáveis. Explique:

    a) Porque terminam nestes certificados?
    b) Quem define quem são estes certificados?