**Criptografia de Chave Pública**

1. (Verdade / Falso) Uma chave pública e sua correspondente chave privada possuem uma relação matemática. Não foi provado matematicamente que é inviável calcular a chave privada a partir de sua chave pública correspondente. Mas é computacionalmente viável derivar a chave privada a partir de uma chave pública.
2. (Verdade / Falso) Devido a sua relação matemática, uma mensagem criptografada com uma chave pública pode ser decifrada com sua chave privada correspondente; e uma mensagem que foi cifrada com a chave privada pode ser decifrada com sua chave pública correspondente.
3. (Verdade / Falso) A criptografia de chave pública pode ser usada para confidencialidade, autenticação ou ambos os requisitos de segurança.
4. De que forma criptografia de chave pública pode resolver confidencialidade ?
5. De que formas criptografia de chave pública pode resolver autenticação ?
6. (Verdade / Falso) No caso da questão 5, pode uma mensagem estar segura contra alteração, mas não contra interceptação.
7. Como podemos montar um esquema usando criptografia de chave pública, para haver autenticação e sigilo ?
8. Explique a desvantagem do esquema da questão 7.
9. De que forma criptografia de chave pública pode resolver o problema da distribuição de chaves privadas de sessão?
10. O que é o procedimento do envelope digital ? Por que é utilizado ?
11. De que forma criptografia de chave pública é utilizada no esquema de envelope digital ?
12. Explicar o algoritmo de criptografia de chave pública RSA, com números pequenos. Exemplo do livro do Tanembaum.
13. A maior parte dos produtos de segurança que utilizam criptografia de chave pública para criptografia e assinaturas digitais utiliza o algoritmo RSA. Conforme já vimos, o tamanho da chave para o uso seguro do RSA tem aumentado nos últimos anos. Que desvantagem sobre o tamanho da chave, RSA tem trazido para as aplicações ?
14. Que requisitos seriam ideais para um algoritmo de criptografia de chave pública poder sobrepujar o algoritmo RSA, quanto ao tamanho da chave de criptografia ?
15. (Verdade/Falso) Assim como a criptografia simétrica, um esquma de criptografia de chave pública é vulnerável a um ataque de força bruta.

Que contramedida pode ser usada para evitar ataque de força bruta ?

1. Quais são as três categorias gerais de aplicações de criptografia de chave pública ?
2. Os algoritmos de criptografia de chave pública são seguros apenas se a autenticação da chave pública for garantida. Que esquema é bastante conhecido para oferecer a segurança necessária para chaves públicas ?
3. Requisitos que algoritmos de criptografia de chave pública devem atender (Diffie-Hellman, 1976):
4. Ser computacionalmente fácil para uma parte-destino B, gerar um par de chaves (pública PUb e privada PRb).
5. Ser computacionalmente fácil para uma parte-origem A, conhecendo a chave pública e a mensagem a ser cifrada, M, gerar o texto cifrado M’ correspondente.
6. Ser computacionalmente fácil para uma parte-destino B, decifrar o texto cifrado M’ resultante usando a chave privada.
7. Ser computacionalmente inviável para um adversário, conhecendo a chave pública PUb, determinar a chave privada PRb .
8. Ser computacionalmente inviável para um adversário, conhecendo a chave pública PUb e um texto cifrado M’, recuperar a mensagem original M.
9. As duas chaves poderem ser aplicadas em qualquer ordem:
 M = D[PUb, E(PRb,M)] = D[PRb, E(PUb, M)]
Este não é um requisito necessário para todas as aplicações.