**INE 5680 - TAREFA DE RECUPERAÇÃO   
  
Nome: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

1. Qual o somatório das afirmativas corretas abaixo?

1 - Em termos de chaves assimétricas, autenticidade somente é garantida com uso da chave privada.

2 - Ataque do homem do meio visa a captura da chave pública.

4 - HASH é uma técnica de criptografia que visa ocultar o texto cifrado.

8 - A dependência do texto assinado está expressa pelo uso da chave privada.

16 - Qualquer chave do par pode ser usada para criptografia, independente da tecnologia do par de chaves assimétricas.

Resposta:

1. Algumas ameaças associadas a um esquema de assinatura digital direta ?

**1. (Verdade/Falso)** A validade do esquema depende da segurança da chave privada do emissor. Se um emissor, mais tarde, quiser negar o envio de uma determinada mensagem, ele poderá reivindicar que a chave privada foi perdida ou roubada, e que um outro falsificou sua assinatura.

**2. (Verdade/Falso)** Outra ameaça é que alguma chave privada possa realmente ser roubada de X no momento T. O oponente pode, então, enviar uma mensagem assinada com a assinatura de X e ‘carimbada’ com uma hora antes ou igual a T.

1. Diferença entre uma assinatura digital direta e uma arbitrada ?

(Verdade/Falso) A **assinatura digital direta** envolve apenas as partes em comunicação (origem, destino). Considera-se que o destino conhece a chave pública da origem. Uma assinatura digital pode ser formada criptografando-se a

mensagem inteira com a chave privada do emissor ou criptografando-se um

código de hash da mensagem com a chave privada do emissor.   
  
(Verdade/Falso) A **assinatura digital arbitrada** opera da seguinte forma: cada mensagem assinada de umemissor X para um receptor Y vai primeiro para um árbitro A, o qual submete a mensagem e sua assinatura a uma série de testes para verificar sua origem e conteúdo.A mensagem, então, é datada e enviada a Y com uma indicação de que foi verificada e aceita pelo árbitro.

1. Ordem a função de assinatura e a função de confidencialidade deveriam ser aplicadas a uma mensagem e por quê ?  
     
   (Verdade/Falso) É importante realizar a função de assinatura primeiro e, depois, uma função de confidencialidade externa. No caso de disputa, algum terceiro deverá ver a mensagem e sua assinatura. Se a assinatura for calculada sobre uma mensagem criptografada, então o terceiro também precisará acessar a chave de decriptografia para ler a mensagem original. Porém, se a assinatura for a operação interna, então o destinatário poderá armazenar a mensagem em texto

claro e sua assinatura para uso posterior na solução da disputa.

----------------------------------------------------------------------------------------------------------

E. Considere a seguinte função Hash H: as mensagens estão na forma de uma sequência de números inteiros, M = (a1, a2, a3, ...., ap). O valor H(M) é calculado como (a1 + a2 + a3 + ....+ ap) mod n, para algum valor predefinido n. Esta função Hash satisfaz a qualquer um dos requisitos para uma função Hash ? Ou seja, para qual dos itens abaixo, esta função é satisfeita?

**1.** H pode ser aplicado a um bloco de dados de qualquer tamanho ?

**2.** H produz uma saída de comprimento fixo ?

**3.** H(*M*) é relativamente fácil de calcular para qualquer *M ?*

**4.** Para qualquer valor *h* dado, é computacionalmente inviável

encontrar *M,* tal que H(*M*) = *h ?*

**5.** Para qualquer bloco dado *M*, é computacionalmente inviável

encontrar *M´* ≠ *M* tal que H(*M´*) = H(*M*) ?

**6.** É computacionalmente inviável encontrar qualquer par (*M*, *M´*) tal

que H(*M*) = H(*M´*) ?

Sugestão: Veja arimética modular.  
 **ADIÇÃO MODULAR**  **(Aritmética modular)**

Qual o resultado da adição **5 + 10** na **Aritmética Módulo 12** ?

Na aritmética usual seria igual 15, mas para respondermos corretamente à nossa pergunta temos que saber qual é o resto que 15 tem quando é dividido por 12. Uma vez que este resto é igual a 3, dizemos que:  
  
**5 + 12 = 3 mod 12**http://www.atractor.pt/mat/alg_controlo/arit_modular/adicao/graphics/som__1%20copy.gif http://www.atractor.pt/mat/alg_controlo/arit_modular/adicao/graphics/som__1%20copy.gifhttp://www.atractor.pt/mat/alg_controlo/arit_modular/adicao/graphics/som__2%20copy.gifhttp://www.atractor.pt/mat/alg_controlo/arit_modular/adicao/graphics/som__2%20copy.gif

**9 + 6 = 3 mod 12**E se considerássemos agora o módulo 9 em vez de 12? Procedíamos de maneira análoga, mas neste caso a divisão considerada seria por 9 e não por 12. Uma vez que 15 = 1 x 9 + 6, dizemos que

1. **+ 10 = 6 mod 9**
2. Relacione duas disputas que podem surgir no contexto da autenticação de mensagem.

Suponha que Bob envie uma mensagem de autenticação a Alice. A

seguinte disputa poderia surgir:   
  
**1. (Verdade/Falso)** Alice poderia forjar uma mensagem e afirmar que ela era foi enviada por Bob.   
Alice somente teria de criar a mensagem e anexar um código de autenticação usando a chave que compartilha com Bob.   
  
**2. (Verdade/Falso)** Bob pode negar ter enviado a mensagem. Como é possível para Alice forjar a mensagem, não há como provar que Bob, de fato, não a enviou.

1. Que requisitos um esquema de assinatura digital deve satisfazer ?
2. Para que serve o Acordo de Chave de Diffie-Helman ?
3. Quais são os requisitos para usos de um esquema de certificado de chave pública ?

**1. (Verdade/Falso)** Cada participante pode ler o certificado para determinar o nome e a chave pública do proprietário do certificado.

**2. (Verdade/Falso)** Cada participante pode verificar que o certificado tem origem em uma autoridade certificada e não é falsificado.  
  
**3. (Verdade/Falso)** Somente a autoridade certificada pode criar e

atualizar certificados   
  
**4. (Verdade/Falso)** Cada participante pode verificar a atualidade do

certificado.

1. Três amigos residentes em cidades distantes desejam trocar informações pela Internet de forma segura. Somente um deles, B possui KR/KU. Proponha um protocolo para que os amigos possam trocar uma KS (chave simétrica) para ser utilizada pelos três na troca de mensagens sigilosas.

A : Gera KSa

A 🡪 B : E**KUb** ( KSa)

B : D**KRb** [ E**KUb** (KSa)]

C : Gera KSc

C 🡪 B : E**KUb** ( KSc)

B : D**KRb** [ E**KUb** (KSc)]

B : Gera KSB 🡪 A : E**KSa** (KS)   
 B 🡪 C : E**KSc** (KS)

A,B,C 🡨 E**KS** ( M ) 🡪 A,B,C

Indique onde está o erro deste protocolo, caso exista.