Lista de Exercícios 1

  *Prazo de Entrega: 04/10/2013 (data da Prova 1)*

*Criptografia Simétrica e de Chave Publica, Gerenciamento de Chaves de Sessão e Chaves Públicas. Diffie-Hellman. Função Hash, Assinatura Digital, Autenticação de Mensagens, Protocolos Criptográficos.*

A lista seguinte, contém questões de revisão da matéria, no sentido de que cada um possa pensar o mínimo sobre a disciplina e se preparar para a Prova 1.

CAPÍTULO 1 (Stallings)

-------------------------------------------------------------------------------------------------------------------1.1 Escreva sobre o que é uma ameaça e o que é um ataque. Dê 1 exemplo de cada caso.

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

1.2 Um serviço de segurança é definido como um serviço fornecido por uma camada de protocolo de comunicação, que garante a segurança adequada dos sistemas ou das transferências de dados. Um outra definição pode ser encontrada na RFC 2828, que oferece a seguinte definição: um serviço de processamento ou de comunicação que é fornecido por um sistema para prover um tipo específico de proteção aos recursos do sistema. O serviços de segurança implementam políticas (ou diretrizes) de segurança e são implementados por mecanismos de segurança. Existem definidos 5 categorias de serviço e 14 serviços específicos. Veja a Tabelas 1.2, 1.3 e 1.4 fornecidas pelo professor.

Irretratabilidade (Não-Repúdio) é um serviço ou um mecanismo de segurança ? E quais os serviços específicos desta categoria ?

Certificação digital, que usa uma terceira parte confiável é um serviço ou é um mecanismo ?

O que é autenticação ? O que é controle de acesso ?

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

CAPÍTULO 2 – TÉCNICAS CLÁSSICAS DE CRIPTOGRAFIA (Stallings)
-------------------------------------------------------------------------------------------------------------------
2.5 Quais são as duas técnicas gerais para se atacar um cifra simétrica.

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

2.6 Defina tipos de ataques criptoanalíticos com base naquilo que o atacante (ou um criptoanalista) conhece. Veja material na página sobre tipos de ataques em criptografia simétrica.

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

2.7 Qual é a diferença entre cifra incondicionalmente segura ou cifra computacionalmente segura.

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

 A. (Verdade/Falso) Cifra de Substituição é utilizada no funcionamento de um algoritmo de criptografia simétrica.

(Verdade/Falso) Cifra de Transposição não pode ser utilizada em algoritmos de criptografia simétrica. Observe como funciona o algoritmo DES.

(Verdade/Falso) Esteganografia é uma forma de criptografia. Explique.

(Verdade/Falso) Uma cifra de produto é a junção de uma cifra de substituição, mais uma cifra de transposição.

B. Qual a diferença entre aleatoriedade estatística e imprevisibilidade ?

Resposta (para conhecimento): Aleatoriedade estatística diz respeito à propriedade de uma sequência de números ou letras, como as que aparecem aleatoriamente e passam por certos testes estatísticos que indicam que a sequência tem a propriedades de aleatoriedade. Se uma sequência estatisticamente aleatória é gerada por um algoritmo, então ela é previsível por qualquer um que conheça o algoritmo e o ponto inicial dessa sequência. Uma sequência é imprevisível quando o conhecimento do método de geração dessa sequência é insuficiente para determiná-la.

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

C. A figura seguinte ilustra o caso de um protocolo entre um terminal de caixa bancário e um banco. Leia o protocolo no material na página sobre protocolos básicos.



Procure responder as seguintes questões sobre um possível ataque. Procure ver os tipos de ataque citados no material sobre Autenticação de Mensagens. O que é um *nonce* ?

1. Para que serve o número r usado no protocolo ?
2. Para que existe o número r’ usado no protocolo ?
3. Cite um ataque possível que pode ser evitado com o uso de r e r´.

Veja a Figura 1 que segue:



CAPÍTULO 9 – CRIPTOGRAFIA DE CHAVE PÚBLICA (Stallings)

9.2 Quais os papéis da chave pública e da chave privada no criptossistema de chave pública ?

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

9.3 Quais são as três categorias gerais de aplicações dos criptossistemas de chave pública ?

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

9.4 Que requistos os criptossistemas de chave pública precisam cumprir para serem um algoritmo seguro ?

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

CAPÍTULO 10 – GERENCIAMENTO DE CHAVES (Stallings)

10.1 Quais são os dois usos diferentes da criptografia de chave pública relacionados à distribuição de chaves ?

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

10.2 Liste as quatro categorias gerais de esquemas para a distribuição de chaves públicas.

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

10.3 Quais os ingredientes principais de um diretório de chaves públicas ?
Resposta:

**1.** A autoridade mantém um diretório com uma entrada {nome, chave

pública} para cada participante.

**2.** Cada participante registra uma chave pública com a autoridade de diretório.

O registro teria de ser feito

pessoalmente ou por algum modo de comunicação autenticada segura.
**3.** Um participante pode substituir a chave existente por uma nova a qualquer

momento, seja pelo desejo de substituir uma chave pública que já foi usada para

uma grande quantidade de dados, seja porque a chave privada correspondente

foi comprometida de alguma maneira.
4.Periodicamente, uma autoridade publica todo o diretório ou atualiza o diretório. 5.Os participantes também poderiamacessar o diretório eletronicamente. Para esse propósito uma comunicação

autenticada e segura da autoridade para os participantes é obrigatória.

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

10.4 O que é um certificado de chave pública ?

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

CAPÍTULO 11 – AUTENTICAÇÃO DE MENSAGENS E FUNÇÕES HASH

11.1 Que tipos de ataques são tratados pela autenticação de mensagens ?

11.3 Quais são as três abordagens para produzir autenticação de mensagens ?

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

11.5 O que é um código de autenticação de mensagens (MAC)? Quais requisitos de segurança são alcançados com o uso de códigos de autenticação de mensagens ?

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

1. Suponha que H(m) seja uma função *hash*, que mapeia uma mensagem m, de comprimento arbitrário em um valor de n bits. É, teoricamente, verdade que, para todas as mensagens x, x´, com x diferente de x´, temos sempre H(x) diferente de H(x´) ? Será que este esquema é seguro ? O que significa computacionalmente inviável ? Explique suas respostas.

Resposta: Bem, existem infinitas mensagens m, mas, existe um número finito de hashes que podem ser calculados. Suponha que H(m) tenha, por definição, um número finito de n bits. Com n bits, teremos 2 elevado a potência n, hashes únicos, e quanto mais alto o valor de n, mais alto será o resultado de hashes únicos. Assim, existem muitos hashes únicos que podem ser produzidos (de fato, esses números é quase impossível de ser compreendido), mas isto também significa, matematicamente, que existem algumas mensagens diferentes, que terão o mesmo hash. Isto não deve trazer preocupações, em termos práticos, pois é extremamente raro que duas mensagens diferentes tenham o mesmo hash. Ainda mais importante, em termos práticos, é o fato de não ser possível modificar uma mensagem e ainda assim, produzir o mesmo hash que a mensagem original. Se alterarmos um bit em uma mensagem, o hash será radicalmente diferente da mensagem original. Logo, podemos dizer que, em termos práticos, as funções Hash são seguras, e que a segurança aumenta, na medida que n aumenta.

Ou mais formalmente:

Se H(m) é *resistente à colisões (fraca)* então é computacionalmente inviável encontrar x diferente de x´, tal que H(x) = H(x´). Ou que dado o par ordenado (x, x´), onde significa que x está relacionado a x´, é *fortemente resistente a colisões*, ou seja, computacionalmente inviável encontrar H(x) = H(x´).

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

11. 6 (Questão) Qual a diferença entre um MAC e uma função Hash ?

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

11.7 Veja a Figura 11.5 fornecida no material de aula. A Figura 11.5 ilustra a variedade de modos em que o código hash pode ser usado para fornecer autenticação de mensagem. Mostre e descreva uma maneira que um valor de Hash pode ser protegido para oferecer autenticação de mensagens ? A que caso, muito usado, se refere o item 11.5 (c).

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

11.6 (Problema) É possível usar uma função Hash para construir uma cifra de bloco com o algoritmo DES ? Se uma função Hash é unidirecional e um bloco cifrado precisa ser reversível (para decriptografia), como isso é possível ?

Resposta: Não. A função Hash, por si própria, não fornece uma autenticação de mensagem. Uma chave secreta deve ser usada de alguma forma para produzir a decriptografia.

Um MAC, por definição, usa a chave secreta para calcular o código usado para autenticação. Se uma função Hash não pode, poder-se-ia utilizar uma função MAC neste sentido ? Explique.

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

E. Considere a seguinte função Hash: as mensagens estão na forma de uma sequência de números inteiros, M = (a1, a2, a3, ...., ap). O valor Hash(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(*x*) é relativamente fácil de calcular para qualquer *x ?*

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

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

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

encontrar *y* ≠ *x* tal que H(*y*) = H(*x*) ?

**6.** É computacionalmente inviável encontrar qualquer par (*x*, *y*) tal

que H(*x*) = H(*y*) ?

Mostre pelo exemplo M=(9, 6), donde Hash(M) mod 12 = 9 + 6 = 15 / 12 = 1 e resto = 3. Logo Hash(15) mod 12 = 3.

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

13.6 Quais são algumas ameaças associadas a um esquema de assinatura digital direta ?

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

1. Para acessar a base de dados de notas da UFSC com prerrogativas de administrador, devem estar envolvidos **3** membros da comunidade acadêmica, entre professores e servidores administrativos da UFSC.
Sendo obrigatório o envolvimento de pelo menos 1 professor e de pelo menos 1servidor. Para solucionar este problema foi definido que a senha de acesso KS, deveria estar cifrada de forma a garantir a regra de segurança acima definida.

Defina o protocolo criptográfico para segurança e liberação da senha de acesso, sabendo que cada membro da comunidade acadêmica possui um par de chaves assimétricas.

 p – professores, pi – i-esimo professor

 a – servidor administrativo, ai – i-esimo servidor administrativo

 S : Gera KS, senha de acesso ao banco de dados

Para **segurança** de KS, deve-se cifrar KS com todas as combinações possíveis de servidores e professores, sempre utilizando-se a KU de pelo menos 1 servidor e 1 professor.

 para 2 professores e 1 servidor:

 para 1 professor e 2 servidores:

A **liberação** da senha de acesso somente será possível com a combinação de KR’s capazes de decifrar KS, ou seja, com a presença de:

 2 professores e 1 servidor, ou

 1 professor e 2 servidores administrativos.

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. Sugestão: Ver assinaturas arbitradas.