Lista de Exercícios 1 2014-2

  *Prazo de Entrega: 10/10/2014 (data final da Prova 1)*

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

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 segunda parte da Prova 1.

**CAPÍTULO 1 (Stallings)**

-------------------------------------------------------------------------------------------------------------------1.1 Escreva sobre o que são vulnerabilidades, o que é uma ameaça, o que é um risco e o que é um ataque. Dê um exemplo de cada caso.

* Vulnerabilidades: Os pontos de um sistema por onde se pode atacar. Uma falha de segurança em um sistema de software que pode ser explorada para permitir a efetivação de uma invasão.

Exemplo: Os *bugs* (erros de uso de linguagens) existentes nas implementações.
 Portas que tem serviços de processamento ou de comunicação sendo
 executados.
* Ameaça: Potencial (possível perigo) para violação da segurança quando há uma circunstância que pode quebrar a segurança e causar danos. É a tentativa de um ataque a um sistema, explorando suas vulnerabilidades.

 Exemplos: Um *link* suspeito num email que você recebeu.

* Risco: É a probabilidade da ocorrência de uma ameaça.

Exemplo: Sua empresa tem a probabilidade 0,6 de ser atacada pelo *worm* “XYZ”.
* Ataque: É uma tentativa (pode ser bem sucedida ou não no objetivo do atacante) deliberada de burlar os serviços de segurança e violar a política de segurança de uma sistema ou corporação. O ato de tentar desviar dos mecanismos de segurança de um sistema. Qualquer ação que comprometa a segurança da informação.

 Exemplos:

1. A quebra de chave ou de um algoritmo criptográfico.
2. Você clica no link suspeito, concretiza a ameaça e sofre as consequências pelos danos causados.
3. A elevação de privilégio de um usuário comum para um
administrador de um sistema.
* Mecanismos de segurança: Processos projetados para detectar ou impedir ataques.

(Padrão X.800) Cifragem, Assinatura Digital, Controle de Acesso, Integridade de Dados, Troca de informações de autenticação, Preenchimento de tráfego, Controle de roteamento, Certificados digitais, Rótulos de segurança, Detecção de eventos, Registros de auditoria de segurança, Recuperação de segurança.
* Serviços de segurança: (RFC 2828) São serviços de processamento ou comunicação fornecidos por um sistema para prover um tipo específico de proteção aos recursos do sistema.

Serviços de segurança (Padrão X.800): Autenticação, Controle de acesso, Confidencialidade, Integridade e Irretratabilidade.

Os serviços utilizam uma ou mais mecanismos de segurança.

* O grau do dano de um ataque chama-se severidade .

A consequência para uma organização da perda de confidencialidade, disponibilidade e/ou integridade de uma informação é chamado impacto.

 Conceitos relacionados:

* Intrusão: Se a tentativa de desviar os controles de segurança é bem sucedida.

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

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 utilizam um ou mais mecanismos de segurança para prover os serviços. Existem definidos 5 categorias de serviço e 14 serviços específicos. Veja a Tabelas 1.2, 1.3 e 1.4 fornecidas.

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)

2.4 Indique Verdade/Falso:

(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.

(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.

2.5 Quais são as duas técnicas gerais para se atacar um cifra simétrica.

2.6 Defina alguns 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 ?

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

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.

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 ?

**Criptografia/decriptografia:** o emissor criptografa uma mensagem com a chave pública do destinatário.

**Assinatura digital:** o emissor ‘assina’ uma mensagem com sua chave privada. A assinatura é feita por um algoritmo criptográfico aplicado à mensagem ou a um pequeno bloco de dados que é uma função da mensagem, que é a função Hash.

**Distribuição de chave (troca de chave):** dois lados cooperam para trocar uma chave de sessão. Várias técnicas diferentes são possíveis.

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

9.4 Que requisitos 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. (VERDADE/FALSO)

**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. (VERDADE/FALSO)
 **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. (VERDADE/FALSO)

4.Periodicamente, uma autoridade publica todo o diretório ou atualiza o diretório. (VERDADE/FALSO)
5.Os participantes também poderiamacessar o diretório eletronicamente. Para esse propósito uma comunicaçãoautenticada e segura da autoridade para os participantes é obrigatória. (VERDADE/FALSO)

**-------------------------------------------------------------------------------------------------------------------**

10.4 Indique a afirmação correta.

Para que serve um acordo de chave Diffie-Hellman ?

( ) Criptografar uma função Hash.

( ) Gerar uma chave compartilhada entre duas partes que se desejam se comunicar
 de forma segura.

( ) Diffie-Hellman é seguro porque os dois lados na comunicação se autenticam.

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

10.4 O que é um certificado de chave pública ? Para que serve ?

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

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 ?

Respsota: A função de hash, por si própria, garante integridade, mas não fornece uma autenticação de mensagem. Uma chave secreta deve ser usada de alguma forma com a função de hash para produzir autenticação. E neste caso, um MAC, por definição, usa

a chave secreta para calcular o código usado para autenticação, como pode ser usado na HMAC, que é um MAC bastante conhecido e usado.

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

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? Consulte o link sobre aritmética modular na página da disciplina.

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

Sim. P é fixo, mas pode ser estabelecido a um valor relativamente grande no conjuntos dos números naturais.

1. H produz uma saída de comprimento fixo ?

Sim, H(M) tem como entrada um bloco de tamanho p, mas dá como saída um valor fixo, que é sempre um valor do tipo de número natural, soma dos valores da mensagem M = (a1, a2, a3, ...., ap).
2. H(*x*) é relativamente fácil de calcular para qualquer *x ?*

Sim, basta somar os componentes da mensagem M. A operação de soma de números naturais é bem conhecida ...

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

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

Falso. Contra-exemplo: Seja h = 3. Se x = (6,9), onde a mensagem M(6,9) é diferente de M(9,6), pois os componentes de M são indexados de 1 a p, e neste caso, existe uma ordem sobre os componentes. Ambas proporcionam H(9,6)=H(6,9)=(9+6) mod 12 = (6+9) mod 12 = 3, como pode ser visto nas operações mostradas em (7).

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

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

Falso. Para a propriedade 5, tome qualquer mensagem *M* e adicione o dígito decimal 0 para a sequência, onde H(9+6+0) mod 12 = H(15) mod 12 = H(9+6) = 3 ; ela terá o mesmo valor de hash. Ou considere x = (9,6) que é diferente de y = (6,9), mas os H(M) são iguais, como mostrado acima e nas operações mostradas em (7).

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

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

Falso. Seja o par x=(9,6) e y=(6,9). Então, (x, y) = ( (9,6), (6,9) ), mas H(x) mod 12 = 3 e H(y) mod 12 = 3

7. Seja M(9,6). Então, H(M) = (9+6) mod 12 = (15 / 12) = 1 e resto = 3. O resto é, pela aritmética modular, por definição, o resultado da operação.

Resposta final:

**Assim,** Ela satisfaz as propriedades 1 a 3, mas não as propriedades

remanescentes 4, 5, 6.

8. Mostre pelo exemplo que se M=(9, 6) e n=12, então H(M)=3.

Seja M(9,6). Então, H(M) = (9+6) mod 12 = (15 / 12) = 1 e resto = 3. O resto é, pela aritmética modular, por definição, o resultado da operação.

Comentário: Ela satisfaz as propriedades 1 a 3, mas não as propriedades remanescentes. Por exemplo, para a propriedade 4, a mensagem que consiste do valor *h* satisfaz H(*h*) = *h*. Para a propriedade 5, tome qualquer mensagem *M* e adicione o dígito decimal 0 para a sequência; ela terá o mesmo valor de hash.

CAPÍTULO 13 – ASSINATURAS DIGITAIS

13.2 Que propriedades uma assinatura digital pode ter ?

1. Ela deve verificar o autor, a data e a hora da assinatura. (VERDADE/FALSO)
2. Ela deve autenticar o conteúdo no momento da assinatura. (VERDADE/FALSO)
3. Deve ser verificável por terceiros, para resolver disputas. (VERDADE/FALSO)

13.3 Que requisitos um esquema de assinatura digital deve satisfazer ?

**1.** Ela precisa ser um padrão de bits que dependa da mensagem que será

assinada. (VERDADE/FALSO)

**2.** Precisa usar alguma informação exclusiva do emissor, para impedir tanto a falsificação quanto a retratação. (VERDADE/FALSO)

3. Deve ser relativamente fácil produzi-la. (VERDADE/FALSO)

4. Deve ser relativamente fácil reconhecê-la e verificá-la. (VERDADE/FALSO)

5. Deve ser computacionalmente inviável falsificá-la, seja construindo uma nova

mensagem para uma assinatura digital existente seja construindo uma assinatura digital fraudulenta para determinada mensagem. (VERDADE/FALSO)
**6.** Deve ser prático armazenar uma cópia da assinatura digital. (VERDADE/FALSO)

13.4 Qual é a diferença entre uma assinatura digital direta e a arbitrada. Consulte os exemplos nos slides do professor.

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.

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 amensagem 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 A.

Qual o caso mais utilizado ?

13.5 Em que ordem a função de assinatura digital e a função de criptografia para obter confidencialidade devem ser aplicada a uma mensagem e por quê ?

É importante realizar a função de assinatura primeiro e, depois, uma

função de confidencialidade externa.

Veja figura 9.4 de CRIPTOGRAFIA DE CHAVE PÚBLICA.

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.

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

**1.** A validade do esquema depende da segurança da chave privada doemissor. 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. Por isso, se pode dizer, que NÃO-REPÚDIO, vale para situações “ingênuas”. Mas, pode haver malícia por parte de quem envia uma mensagem, como o caso referido acima. (VERDADE/FALSO)

**2.** Outra ameaça é que alguma chave privada possa realmente ser roubada de X

no momento T. Um oponente Y, de posse da chave privada furtada pode, então, enviar uma mensagem assinada como se fosse a assinatura de X e ‘carimbada’ com uma hora antes ou igual a T. (VERDADE/FALSO)

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

13.7 Relacione duas disputas que podem surgir no contexto da autenticação de mensagem.

Resposta: A autenticação de mensagem protege duas partes que trocam mensagens contra uma terceira parte. Mas, não protege as duas partes uma da outra e diferentes formas de disputa são possíveis entre as duas.

Suponha que João envie uma mensagem de autenticação à Maria. A

seguinte disputa poderia surgir:

**1.** Maria poderia forjar uma mensagem e afirmar que ela foi enviada por João. Maria somente teria de criar a mensagem e anexar um código de autenticação usando a chave que compartilha com João.

**2.** João pode negar ter enviado a mensagem. Como é possível para Maria forjar a mensagem, não há como provar que João, de fato, não a enviou.

Em situações em que não existe confiança mútua e completa entre emissor e receptor, é necessário algo mais do que autenticação. A solução mais adequada para esse problema é a assinatura digital, que é semelhante à assinatura escrita a mão. Uma assinatura precisa ter as seguintes características:

* Deve verificar o autor, a data e hora da assinatura.
* Deve autenticar o conteúdo no momento da assinatura.
* Deve ser verificável por terceiros, para resolver disputas.

13.8 Dê exemplos de ataques por repetição.

**Repetição simples:** o oponente simplesmente copia uma mensagem e a

repete mais tarde. (VERDADE/FALSO)

**Repetição simples:** o oponente simplesmente copia uma mensagem e a

repete mais tarde. (VERDADE/FALSO)

**Repetição que pode ser registrada em log:** um oponente

pode repetir uma mensagem com carimbo de tempo dentro da janela de tempo

válida. (VERDADE/FALSO)

**Repetição que não pode ser detectada:** esta situação poderia surgir

porque a mensagem original poderia ter sido suprimida e, assim, não ter

chegado ao seu destino; somente a mensagem por repetição chega. (VERDADE/FALSO)

**Repetição inversa sem modificação:** esta é uma repetição de volta ao emissor da

mensagem. Esse ataque é possível se a criptografia simétrica for usada e o

emissor, com base no conteúdo, não puder reconhecer facilmente a diferença

entre mensagens enviadas e mensagens recebidas. (VERDADE/FALSO)

13.9 Liste três técnicas gerais para lidar com **ataques de repetição** entre dois participantes, A e B que se comunicam.

**1.** Anexar um número de seqüência a cada mensagem usada em uma

troca de autenticação entre A e B. Uma nova mensagem é aceita somente se seu número de seqüência estiver na ordem correta. Muitos protocolos usam este fato.

(VERDADE/FALSO)

**2.** A parte A, esperando uma mensagem nova de B, primeiro envia a B um

*nonce* e exige que a mensagem subseqüente (resposta) recebida de B

contenha o valor *nonce* correto.

(VERDADE/FALSO)

**3.** A parte A aceita uma mensagem de B, como sendo nova, somente, se esta tiver um

carimbo de tempo que, no julgamento de A, é próxima o suficiente do

conhecimento de A da hora atual. Essa técnica exige que os relógios entre os

diversos participantes estejam sincronizados.

(VERDADE/FALSO)