Lista de Exercícios 1

  *Prazo de Entrega Impressa: 23-05-2014 (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, e algumas respostas, no sentido de que cada um possa pensar o mínimo sobre a disciplina e se preparar para a Prova 1.*

*Observação: Questões numeradas são do livro do CRIPTOGRAFIA E SEGURANÇA DE REDES, 4 edição, William Stallings, Peason. 2008. Questões identificadas por letras maiúsculas foram criadas pelo professor. Respostas estão em azul.

IMPORTANTE: Estdem as questões que foram colocadas já com as respostas, porque podem ser questões boas para a Prova 1.*

**CAPÍTULO 1 – INTRODUÇÃO (Stallings) - Conceitos**

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 ?

1.3 Desenhe uma matriz semelhante à Tabela 1.4 que mostre o relacionamento entre serviços e ataques. As colunas referem-se a atques e as linhas aos aspectos de segurança.

Resposta:



1.4 Desenhe uma matriz semelhante à Tabela 1.4 que mostre o relacionamento entre mecanismos e ataques à segurança. As colunas referem-se a atques e as linhas aos aspectos de segurança.

Resposta:



A tabela está partida porque a mesma foi retirada, por captura, do material do livro.

**CAPÍTULO 2 – TÉCNICAS CLÁSSICAS DE CRIPTOGRAFIA (Stallings)**

2.1 Quais são os ingredientes essenciais de uma cifra simétrica.

2.2 Quais as duas funções básicas usadas nos algoritmos de criptografia simétrica ?

2.3 Quantas chaves sáo necessárias para que duas pessoas se comuniquem através de uma cifra simétrica ?

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

2.4 Qual é a diferença básica entre uma cifra de bloco e uma cifra de fluxo ?

Uma **cifra em fluxo** é uma cifra que processa os elementos da entrada (bytes, usualmente) continuamente, produzindo a saída de um elemento de cada vez, enquanto prossegue.

Uma **cifra de bloco** processa a entrada de um bloco de elementos (bytes) de

cada vez, medido por sua quantidade de bits, produzindo um bloco de saída para cada bloco de entrada.

O processamento por fluxo é mais rápido do que por bloco.

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

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

Criptoanálise e ataque por força bruta sobre a chave.

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

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.

Um esquema de criptografia é icondicionalmente seguro, se o texto cifrado gerado pelo esquema não tiver informações suficientes para determinar exclusivamente o texto claro correspondente, não importanto quanto texto claro esteja à disposição. Ou seja, não importa quanto um oponente tenha, é impossível ele decifrar o texto cifrado, simplesmente porque a informação exigida não está lá. Procure ver (na Internet) o que é ONE-TIME PAD. Com este esquema não existe algoritmo de criptografia que seja incondicionalmente seguro. Portanto, tudo o que um projetista ou os usuários de um algoritmo de criptografia podem se esforçar para obter é um algoritmo que atenda a um ou ambos os critérios a seguir:

(a) Custo para quebrar a cifra, seja maior que o valor da informação a ser cifrada.
(b) Tempo exigido para quebrar a cifra é superior ao tempo de vida útil da informação.

Um esquema de criptografia é considerado computacionalmente seguro, se um desses dois critérios for atendido. O problema é que é muito difícil estimar a quantidade de esforço exigido para criptoanalisar o texto cifrado com sucesso.

Todas as formas de criptoanálise de esquemas de criptografia simétrica são projetados para explorar o fato de que rastros da estrutura ou do padrão de texto claro, podem sobreviver à criptografia a serem discerníveis no texto cifrado.

2.9 O que é uma cifra **monoalfabética** ? E uma cifra **polialfabética** ?

Uma **cifra por substituição monoalfabética** mapeia de um alfabeto claro

para um alfabeto cifrado, de forma que um único alfabeto é utilizado

por mensagem.

Uma **cifra de substituição polialfabética** uliliza uma cifra de substituição monoalfabética para cada letra sucessiva de texto claro, dependendo de uma chave.

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.

Esteganografia reúne um conjunto de métodos para ocultar um mensagem em texto claro, dentro de um outro arquivo. Uma mensagem pode ser apenas escondida, enquanto os métodos de criptografia tornam a mensagem innintelegível a estranhos por várias transformações do texto.

(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. Isto é usado na geração de números pseudo-aleatórios. 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. Isto corresponde ao caso ideal de números verdadeiramente aleatórios, que é o caso muito mais difícil de se conseguir. Para este caso, existem em vários fenômenos da natureza e são muito mais difíceis de se conseguir valores.

Então, nos casos práticos que usamos, são usados números pseudo-aleatórios.

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

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 e o material de texto que está na página :



**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 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, explicando cada uma delas.

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

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 ?

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

D . 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 Qual a diferença entre um MAC e uma função Hash ?

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 ?

Se você examinar a estrutura de uma simples rodada de DES, verá que a rodada inclui uma função unidirecional , f, e um XOR:

Ri = (Li – 1) ⊕ f(Ri–1, Ki).

Para o DES, a função f está descrita na figura que mosra uma iteração do DES. Ela mapeia, numa iteração, um Ri de 32 bits e um Ki (sub-chave) de 48 bits para uma saída de 32 bits. ou seja, ela mapeia uma entrada de 80 bits para uma saída de 32 bits. Essa é, claramente, uma função unidirecional. Uma função de hash que produza uma saída de 32 bits poderia ser usada para f. A demonstração, no texto, segundo o livro do Stallings, de que a decriptografia funciona, ainda é válida para qualquer função f unidirecional.

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

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 ?

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. 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.

Resposta final:

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

remanescentes 4, 5, 6.

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.

**CAPÍTULO 12 – ASSINATURA DIGITAIS**

13.1 Relacione duas disputas que podem surgir no contexto da autenticação de mensagens.

Suponha que John envie uma mensagem de autenticação a Mary. A

seguinte disputa poderia surgir:

**1.** Mary poderia forjar uma mensagem e afirmar que ela era foi enviada por John (lembre do exemplo de Ataque do Dicinário fornecido em aula, e o outro exemplo do protocolo Neumann-Stubbline descrito na aula de 25/04, mostrando o exemplo de uso do SPASS) Mary somente teria de criar a mensagem e anexar um código de autenticação usando a chave que compartilha com John.

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

13.2 Que propriedades uma assinatura digital pode ter ?

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

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.

**2.** Precisa usar alguma informação exclusiva do emissor, para

impedir tanto a falsificação quanto a retratação.

3.Deve ser relativamente fácil produzi-la.

4. Deve ser relativamente fácil reconhecê-la e verificá-la.

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.
**6.** Deve ser prático armazenar uma cópia da assinatura digital.

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 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 A.

13.5 Em que oderdem 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 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. 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.

**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.

13.7 Dê exemplos de ataques por repetição.

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

repete mais tarde.

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

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

válida.

**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.

**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.

13.8 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.

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

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

contenha o valor nonce correto.

**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.

13.9 O que é um ataque **supress-replay** ?

Quando o clock de um emissor estiver adiantado em relação ao clock do destinatário, um oponente pode interceptar uma mensagem do emissor e repeti-la mais adiante, quando o carimbo de tempo na mensagem se tornar atual na localização do destinatário. Essa repetição poderia causar resultados inesperados. Isto é causado, se os clocks do emissor e receptor não estiverem sincronizados. Veja no exemplo do Protocolo Neumann-Stubbline (aula de 25/4), onde existem nonces Na e Nb, mas existe também um rótulo de tempo (timestamp) Tb quando B envia uma determinada mensagem para o servidor confiável T.