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)**

9.1 Quais são os principais elementos de um criptossistema de chave pública ?

**Plaintext:** essa é a mensagem ou dados legíveis que são alimentados no

algoritmo como entrada.

**Algoritmo de criptografia:** o algoritmo de criptografia realiza várias

transformações no texto claro.

**Chaves pública e privada:** esse é um par de chaves que foi selecionado de modo

que, se uma for usada para criptografia, a outra será usada para decriptografia.

As transformações exatas realizadas pelo algoritmo dependem da chave pública

ou privada que é fornecida como entrada.

**Texto cifrado:** essa é a mensagem codificada produzida como saída. Ela

depende do texto claro e da chave. Para uma determinada mensagem, duas

chaves diferentes produzirão dois textos cifrados diferentes.

**Algoritmo de decriptografia:** esse algoritmo aceita o texto cifrado e a chave

correspondente e produz o texto claro original.

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

Uma chave privada de usuário é mantida privada e conhecida somente

pelo usuário. Uma chave pública de usuário é disponibilizada para que

outros a usem. A chave privada pode ser utilizada para criptografar uma

assinatura que pode ser verificada por qualquer um com a chave pública.

Ou uma chave pública pode ser usada para criptografar informação que

somente poderá ser decriptografada por quem possua uma chave privada.

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

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. **Troca de chave:** dois

lados cooperam para trocar uma chave de sessão. Várias técnicas diferentes são

possíveis, envolvendo a(s) chave(s) privada(s) de uma ou de ambas as partes.

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

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

**1.** É computocionalmente fácil para a parte B gerar um par (chave

pública *PUb*, chave privada *PRb*).

**2.** É computacionalmente fácil para um emissor A, conhecendo a chave

pública e a mensagem a ser criptografada, *M*, gerar o texto cifrado

correspondente: *C* = E(*PUb*, *M*)

**3.** É computacionalmente fácil para o receptor B decriptografar o texto

cifrado resultante usando a chave privada para recuperar a mensagem

original: *M* = D(*PRb*, C) = D(*PRb*, E(*PUb*, *M*))

**4.** É computacionalmente inviável para um adversário, conhecendo a

chave pública, *PUb*, determinar a chave privada *PRb.*

**5.** É computacionalmente inviável para um adversário, conhecendo a

chave pública, *PUb*, e um texto cifrado, *C*, recuperar a mensagem original, *M*.

9.5 O que é uma função unidirecional ?

Uma **função unidirecional** é aquela que mapeia um domínio em um

intervalo de modo que todo valor da função tem um inverso único, com a

condição de que o cálculo da função seja fácil, ao passo que o cálculo do inverso

seja inviável.

9.6 O que é uma função unidirecional com segredo ?

Uma função unidirecional com segredo é fácil de calcular em uma

direção e inviável de calcular na outra, a menos que certa informação adicional

seja conhecida. Com a informação adicional, o inverso pode ser calculado em

tempo polinomial (o tempo de execução do algoritmo segue a lei matemática de um polinômio; se fosse um função exponencial, o tempo de execução tenderia a crescer no sentido infinito e isto não é bom para a execução de um algoritmo).

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

9.7 (Problema 9.2 Stalligs)

Realize a criptografia de decriptografia usando o algoritmo RSA, seguindo o exemplo entregue em aula (Livro do Tanembaum ou Figura 9.6 Stallings) para o seguinte: p=3 ; q=11 ; e=7 ; M=5.

Resposta: *n* = 33; φ(*n*) = 20; *d* = 3; C = 26.

9.8 (Problema 9.7 Stallings)

No esquema de criptografia de chave pública RSA, cada usuário tem uma chave pública, e, e uma chave privada, d. Suponha que Bob revele acidentalmente sua chave privada. Em vez de gerar um novo módulo *n* (a criptografia depende de n), ele decide gerar uma nova chave pública e um nova chave privada. Isso é seguro ?

Não, não é seguro. Uma vez que Bob revelou sua chave privada, Alice poderá usá-la para fatorar seus módulos, n. Então ela poderá “quebrar” qualquer mensagem que Bob envie.

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

**CAPÍTULO 10 – GERENCIAMENTO DE CHAVES (Stallings)**

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

**1.** As chaves públicas de distribuição.

**2.** O uso de criptografia de chave pública para distribuir chaves secretas.

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

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

Public announcement. (Anúncio Público)

Publicly available directory. (Diretório disponível publicamente)

Public-key authority. (Autoridade de Chave Pública)

Public-key certificates (Certificados de Chave Pública)

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

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 ?

Um certificado de chave pública contém uma chave pública e outras

informações, é criado por uma autoridade certificada e é dada aos

participantes com, chave privada correspondente. O participante converte

sua informação de chave em outra ao transmitir seu certificado. Outros

participantes podem verificar que o certificado foi criado pela autoridade.

10.5 Quais são os requisitos para usos de um esquema de certificado de chave pública ?

**1.** Cada participante pode ler o certificado para determinar o nome e a

chave pública do proprietário do certificado.

**2.** Cada participante pode

verificar que o certificado tem origem em uma autoridade certificada e

não é falsificado.

**3.** Somente a autoridade certificada pode criar e

atualizar certificados

**4.** Cada participante pode verificar a atualidade do

certificado.

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

10.6 Explique resumidamente o Acordo de Chaves Diffie-Hellman. E qual o ponto vulnerável deste algoritmo ??

As duas partes criam, cada uma, um par chave pública/chave privada (números)
e comunica a chave pública para outra parte. As chaves são projetadas de

tal modo que ambos os lados podem calcular a mesma única chave

secreta com base na chave privada de cada lado e no a chave pública do

outro lado.

O lado vulnerável é que nenhuma das duas partes se autenticam.

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

**CAPÍTULO 11 – AUTENTICAÇÃO DE MENSAGENS E FUNÇÕES HASH**

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

**Mascaramento:** Inserção de mensagens na rede a partir de uma origem

fraudulenta. Isso inclui a criação de mensagens por um oponente, que fingem

ter vindo de uma entidade autorizada. Também estão incluídas as confirmações

fraudulentas de recebimento ou não-recebimento de mensagens por alguém

que não seja o destinatário da mensagem.

**Modificação de conteúdo:** Mudanças no conteúdo de uma mensagem,

incluindo inserção, exclusão, transposição e modificação.

**Modificação de seqüência:** Qualquer modificação em uma seqüência de

mensagens entre as partes, incluindo inserção, exclusão e reordenação.

**Modificação de tempo:** Atraso ou repetição de mensagens. Em uma aplicação

orientada a conexão, uma sessão inteira ou uma seqüência de mensagens pode

ser uma repetição de alguma sessão anterior válida, ou mensagens individuais

na seqüência podem ser adiadas ou repetidas. Em uma aplicação sem conexão,

uma mensagem individual (por exemplo, datagrama) pode ser adiada ou

repetida.

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

11.2 Quais são os dois níveis de funcionalidade contidos em um mecanismo de autenticação de mensagens ou de assinaturas digitais.

No nível mais baixo, é preciso haver algum tipo de função que produza

um autenticador: um valor a ser usado para autenticar uma mensagem. Essa

função de baixo nível é então usada como uma primitiva em um protocolo de

autenticação de nível mais alto, que permite a um receptor verificar a

autenticidade de uma mensagem.

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

Criptografia de mensagem, código de autenticação de mensagem e função

de hash.

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

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 ?

Um autenticador que é uma função de criptografia dos dados a serem

autenticados e de uma chave secreta.

Autenticidade.

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

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 ?

A função de hash, por si própria, não fornece uma autenticação de

mensagem. Hash só verifica a integridade da mensagem.

Num MAC, uma chave secreta deve ser usada de alguma forma com a

função de hash para produzir autenticação. Um MAC, por definição, usa

a chave secreta para calcular o código usado para autenticação.

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

11.7 (Questão) 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).

A Figura 11.5 (material dado em auala) ilustra a variedade de modos em que o código hash pode ser usado para fornecer autenticação de mensagem como segue: **a.** A

mensagem, mais o código de hash concatenado, é criptografada usando a

criptografia simétrica. **b.** Somente o código de hash é criptografado, usando a

criptografia simétrica. **c.** Somente o código de hash é criptografado, usando a

criptografia de chave pública e a chave privada do emissor. **d.** Se forem

desejadas confidencialidade e assinatura digital, então a mensagem mais o

código de hash criptografado com a chave privada podem ser criptografados

usando a chave secreta simétrica. **e.** Essa técnica usa a função de hash, mas não

a criptografia para autenticação da mensagem. A técnica considera que as duas

partes que se comunicam compartilham um valor secreto *S* comum. A calcula o

valor de hash sobre a concatenação de *M* e *S*, e anexa o valor de hash resultante

a *M*. Como B possui *S*, ele pode recalcular o valor do hash para verificação. **f.** A

confidencialidade pode ser acrescentada à técnica de (e), criptografando a

mensagem inteira mais o código de hash.

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

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 3.5. Ela mapeia um R de 32

bits e um K 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 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 ?

**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.

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

**CAP 12 ASSINATURAS DIGITAIS E PROTOCOLOS DE AUTENTICAÇÃO**

13.1 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.** 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.** 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.

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

13.2 Que propriedade uma assinatura digital de 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.

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

13.5 Qual a diferença entre uma assinatura digital direta e arbitrada ?

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.

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

13. 5 Em que ordem a função de assinatura e a função de confidencialidade deveriam ser aplicadas a uma mensagem e por quê ?

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.

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

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.

 **2.** 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.

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

**PROTOCOLOS CRIPTOGRÁFICOS**

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.

 Solução:

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

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

 para 2 professores e 1 aluno:

 S : E**KUpi** { E**KUpi+1** [ E**KUai** ( **KS** ) ] } e

 S : E**KUpi** { E**KUpi+2** [ E**KUai** ( **KS** ) ] } e

 . . . . . . . . . . . . . . . . . . . .

 S : E**KUpi** { E**KUp+n**  [ E**KUai** ( **KS** ) ] }

 para 2 alunos e 1 professor:

 S : E**KUpi** { E**KUai**  [ E**KUai+1** ( **KS** ) ] } e

 . . . . . . . . . . . . . . . . . . . .

 S : E**KUpi** { E**KUai**  [ E**KUai+n** ( **KS** ) ] }

A **liberação** da senha de acesso somente será possível com a combinação de KR’s capaz de descifrar KS, ou seja com a presença de 2Prof e 1Aluno ou 1Prof e 2Alunos.

 S : D**KRpi** { D**KRpi+1** [ D**KRai** ( **KS** ) ] } ou

 S : D**KRpi** { D**KRai+1** [ D**KRai** ( **KS** ) ] } ou

 . . . . . . . . . . . . . . . . . . . .

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 KS

B 🡪 A : E**KSa** (KS)

B 🡪 C : E**KSc** (KS)

 A,B,C 🡨 E**KS** ( M ) 🡪 A,B,C

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

H. Três amigos residentes em cidades distantes desejam trocar informações pela Internet de forma segura. Um deles propôs o seguinte protocolo para troca da chave simétrica. Somente um deles, C, possue KR/KU.

A : Gera **N** randômico

A 🡪 B : **N**

A 🡪 C : **N**

 C : Gera **X** = **N** ⊕ **R, R** randômico

C 🡪 B : E**N** ( **X** )

C 🡪 A : E**N** ( **X** ) || E**KR** ( **N** )

 A : **N ==** D**KU** [ E**KR** ( **N** ) **] ?**

 A : Gera **Ks,** calcula **R** = **X** ⊕ **N**

A 🡪 B : E**R** ( **Ks** )

A 🡪 C : E**R** ( **Ks** )

Pergunta-se: **A**, **B** e **C** podem, ou não, trocar mensagens seguras cifradas com **Ks?**

Justifique mostrando o erro no protocolo caso exista.

**Resposta: NÃO PODEM,**

**Ainda conceitualmente, não existe solução para troca de chave segura utilizando somente chaves simétricas e o protocolo somente utiliza chaves simétricas para troca da chave Ks.**

**Erro no protocolo proposto: N trafega em texto plano.**

**N pode ser utilizado para decifrar X.**

**R pode ser calculado para decifrar Ks.**

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

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

Em um sistema B2B web, com as seguintes características e requisitos:

- Empresas vendedoras acessam o sistema e oferecem seus produtos.

- Empresas compradoras acessam o sistema para consulta a preços.

- Empresas compradoras acessam o sistema e realizam pedidos.

Identifique pontos de ataque para empresas compradoras ou vendedoras, mostre como os ataques podem ocorrer e apresente um protocolo criptográfico comentado para solucionar os ataques.

 ***Ataques empresas vendedoras:***

1. Autenticação, um quer se faz passar pela empresa fazendo ofertas falsas.
2. Integridade, um quer modifica a oferta da empresa.

 ***Ataques empresas compradoras:***

1. Autenticação, um quer se faz passar pela empresa fazendo compras falsas.
2. Integridade, um quer modifica a compra da empresa.

V : Empresa Vendedora C : Empresa Compradora

 V : Gera Oferta

V 🡪 B2B : S**KRv** ( Oferta) || KUv // assina oferta

 B2B : KUv ??? // verifica se empresa cadastrada

 B2B : V**KRv** ( Oferta ) // verifica originalidade da oferta

 B2B : Armazena Oferta

C 🡪 B2B : Consulta Oferta

 C : Gera Pedido

C 🡪 B2B : S**KRc** ( Pedido) || KUc // assina pedido

 B2B : KUc ??? // verifica se empresa cadastrada

 B2B : V**KRc** ( Pedido ) // verifica originalidade do pedido

 B2B : Armazena Pedido