**LISTA DE EXERCÍCIOS II - PROTOCOLOS CRIPTOGRÁFICOS**

1. Em uma reunião, sobre segurança da informação, realizada pela equipe de TI de uma grande empresa, com filiais em todo país, surgiram as seguintes situações e sugestões durante as discussões:
2. As filiais necessitam enviar, ao gerente da matriz, mensalmente seus balanços contábeis. Para garantir o sigilo dos mesmos, um dos presentes sugeriu que fosse criada uma página Web *https*, onde as filiais fariam *upload* dos balanços em texto plano e os mesmos seriam gravados no servidor da empresa em um base de dados com acesso restrito ao gerente da matriz.

*Diga se a solução proposta garante o sigilo desejado e justifique. Se não garantir, mostre como deveria ser garantido o sigilo nas comunicações.*

1. Desejava-se criar a possibilidade de gerentes trocarem e-mails sigilosos. Um dos presentes sugeriu que fosse gerado um par de chaves assimétricas para cada gerente, deixando-as gravadas em uma base de dados com acesso restrito ao gerente.

 *Mostre como dois gerentes poderiam (ou não) trocar e-mails sigilosos
 entre eles.*

1. Para garantir a integridade do cadastro de funcionários um dos presentes sugeriu que fosse acrescentado a cada registro do cadastro um campo para conter o *hash* do registro.

 *Comente a solução apontando sua alternativa, se for o caso.*

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

B) Comente as afirmativas seguintes:

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

 2 -- Ataque do homem do meio visa a captura de chaves públicas.

 3 – HASH é uma técnica de criptografia que visa ocultar o texto cifrado.

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

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

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

1. 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.

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

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

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

E) 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

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 administradores da UFSC. Sendo obrigatório o envolvimento de pelo menos 1 professor e de pelo menos 1 funcionário. Para solucionar este problema foi definido que a senha de acesso 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 – administrador UFSC, ai – i-esimo administrador

 O servidor S do BD: 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 2 professores e 1 administrador ou 1 professor e 2 adminsitradores.

 para 2 professores e 1 administrador:

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

 para 1 professores e 1 administrador:

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

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

1. O Detran de Santa Catarina descobriu que seu sistema de emissão de documentos para automóveis estava apresentando problemas de segurança.

Sabendo-se que o *login* ao sistema é realizado informando o número do CPF do funcionário e uma senha de acesso, aponte possíveis vulnerabilidades e proponha um protocolo criptográfico para solucionar o problema apresentado abaixo:

Foram detectados acessos e uso do sistema por CPFs, cujo funcionário
titular nega ter realizado.

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

H. 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.



Veja a Figura 1 e responda:

1. Para que serve o número r usado no protocolo ?
2. Para que existe o número r’ usado no protocolo ?

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

1. Considere a figura seguinte, um protocolo que mostra um procedimento de autenticação de um usuário de um terminal bancário. Suponha que um terminal bancário é uma entidade T e o sistema central (banco) uma entidade B. Considere para o terminal o par de chaves, pública e privada, (PUT, PRT) e para o sistema de autenticação em B, respectivamente, o par (PUB, PRB) de chave pública e chave privada. No protocolo da figura, a criptografia simétrica, com uma chave de sessão CS é usada no procedimento de autenticação.



Altere o protocolo acima, descrevendo formalmente suas etapas, para funcionar com criptografia de chave pública.

1. Considere que o sistema central (banco B) conheça as chaves públicas dos vários terminais *T* (*PUT*). E que esses terminais T conheçam a chave pública do sistema central.

B : *PUT  (por construção do sistema de segurança) e (PUB, PRB)*T : *PUB* e *(PUT, PRT)*
2. Alguém está querendo usar o terminal T. O protocolo se inicia quando o terminal envia sua identificação *T* para o sistema central B.

T 🡪 B : IT (aqui, o identificador de T não está criptografado, mas se fóssemos fazer assim, usaríamos *PUB(IT),* assumindo-se como acima que T conhece *PUB .*

1. Pelo protocolo, o sistema central B deve enviar uma chave de sessão *CS* para o terminal *T* poder criptografar (usando criptografia simétrica com uma chave de sessão *CS*), através da chave mestra *CT*.

B 🡪 T : *CT*(*CS*), neste caso, a chave mestra CT do terminal T criptografa a chave de sessão CS enviada pelo banco B para o terminal T.

1. Mas, para se usar criptografia de chave pública, o sistema central, agora, se utilizará da chave pública do terminal T (*PUT*), enviando a chave de sessão *CS* criptografada para *T.* Com suachave privada (*PRT)*, o terminal *T* decifra a chave de sessão *CS*.

Para usar criptografia de chave pública, o banco B, agora substitui a chave CT por uma chave pública *PUT*
O uso da criptografia de chave pública, se faz aqui na etapa 4 e poderíamos ter:

B 🡪 T : *PUT(CS)* T : *PRT(CS)* T : *CS*

1. Com *CS*, o terminal *T* pode cifrar os números *r* supostamente aleatórios gerados por *T* e enviá-los ao sistema central.

T : E*CS*(r)onde r é *nonce* gerado por T
T 🡪 B : E*CS*(r)B : D*CS*(r)
 B : r
2. De posso do número *r*, o sistema central modifica esse número *r,* adicionando 1, cifrando-o com *CS* e enviando para *T*. O banco B envia *r+1* para T. Lembrem que os números *r* e *r+1* são usados apenas uma vez, para evitar ataques de repetição no procedimento de autenticação de um usuário do terminal *T*. Daí o termo *nonce*, em inglês, para denominar esses números.

B : r+1
B: E*CS*(r+1)
B 🡪 T : E*CS*(r+1)
T : D*CS*(r+1)
T : r+1

1. O terminal envia sua identificação *iA* e a senha *sA* para o sistema central poder autenticar usando o arquivo de senhas, contendo os valores *hash* das senhas dos usuários do sistema.

O terminal T recebe o número *r+1* e assim, fica sabendo que o banco B recebeu seu número *r*, envoado anteriormente.

T 🡪 B : E*CS*(IA , SA) ,

onde IA é o identificador de um usuário A e AS é a senha do usuário, Ambos os valores são enviados criptografados para o sistema do banco B.

J) Existem três formas típicas de usar *nonces*. Suponha que Na seja um *nonce* gerado por A, A e B compartilham a chave K, e f() seja uma função como incremento. Os três casos são:

**Uso 1**(1) A 🡪 B:Na

(2) B 🡪 A: E(K,Na)

**Uso 2**
(1) A 🡪 B: E(K,Na)

(2) B 🡪 A: A:Na

**Uso 3**(1) A 🡪 B: E(K,Na)
(2) B 🡪 A: E(K,f(Na))

Todas as três casos podem ser usados. A diferença está no que é explicado como segue:

1. No Uso 1, um ataque poderia violar a segurança

através de Na e retendo uma resposta de B para um futuro ataque por

repetição. Verdade/Falso ?

2. O atacante poderia tentar prever uma possível repetição no Uso 2, mas isso não daria certo se os *nonces* forem aleatórios. Verdade/Falso ?

3. Tanto no Uso 1 como no 2, as mensagens trabalham em ambas as direções. Ou seja, se Na é enviada em uma direção, a resposta é
E[K, Na]. Verdade/Falso ?

4. No Uso 3, a mensagem é criptografada em ambas as direções; o propósito da função é assegurar que as mensagens 1 e 2 não são idênticas. Então, o Uso 3 é mais seguro. Verdade/Falso ?

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

K) Um dos pontos de fragilidade dos sistemas computacionais, reside nos cadastros de usuários e nas **restrições de controle de acesso** aos sistemas, visto que ataques a cadastros, como inclusão indevida de usuários, tem grande probabilidade de não serem detectadas. Aponte soluções para as situações abaixo e escreva o protocolo criptográfico para tentar evitar que os ataques aconteçam.

1. Um atacante, com prerrogativa de BDA, substitui do arquivo de cadastro por um arquivo vazio, simulando a condição de inicio de operação do sistema.
2. Um atacante, com prerrogativa de BDA, inclui um novo usuário no cadastro com privilégios de acesso a todo sistema.

1. Um atacante, com prerrogativa de BDA, altera os privilégios de acesso de um usuário cadastrado.
2. Um atacante, com prerrogativas de usuário privilegiado do sistema, inclui um usuário fictício no sistema.

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