1. 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.
2. Um atacante, com prerrogativa de BDA, substitui do arquivo de cadastro por um arquivo vazio, simulando a condição de inicio de operação do sistema.
3. 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.

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

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 alternativa se for o caso.*

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

C) Qual o somatório das afirmativas corretas abaixo?

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

2 -- Ataque do homem do meio visa a captura da chave pública.

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

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

16 – 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. 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. 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.**

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

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 alunos da UFSC. Sendo obrigatório o envolvimento de pelo menos 1 professor e de pelo menos 1 aluno. 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 – alunos, ai – i-esimo aluno

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. 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:

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