**LISTA DE EXECÍCIOS PARA A PROVA 2**

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, possui chaves assimétricas. O protocolo proposto é como segue:

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. Considere o seguinte cenário: suponha que você trabalha como um Home Office para uma corporação. Por questão de segurança, você estabelece uma VPN entre sua máquina e o gateway VPN de sua organização. Uma possibilidade perigosa que abre possibilidade de um ataque é a de existir na Internet um intruso e utilizar sua máquina em casa (um cliente VPN) como uma ponte entre a Internet (porque você está ligado via um modem) e a rede interna da organização. O seu equipamento passa a ter duas conexões, uma com a Internet (sujeita a ataques externos) e outra, via tunelamento VPN com a rede de sua organização, que você precisa para trabalhar de forma segura. Dessa maneira, um intruso (cracker) pode utilizar uma conexão via Internet e passar para a outra (o túnel VPN), e alcançar, assim, a rede de sua organização.

Entretanto, as considerações de segurança envolvidas no cenário acima, podem ser preocupantes, pois o cliente está disponível (mas não deve estar aberto) a todo universo na Internet.

Um dos métodos para fazer com que sua máquina (cliente VPN) atue como uma ponte entre a Internet e a rede de sua empresa, é por meio de roteamento de pacotes TCP/IP. Se a máquina-cliente VPN tiver capacidade de roteamento de pacotes, o intruso pode enviar pacotes à sua máquina, que por sua vez, rotearia esses pacotes para a rede de sua organização. Isto porque, o cliente VPN age sobre a pilha TCP/IP de sua máquina, de modo que todo pacote endereçado à rede de sua organização é transformado em um pacote VPN, que são pacotes válidos e autenticados pelo gateway VPN de sua empresa.

Escreva políticas de segurança, que sua empresa deve seguir, para evitar problemas de segurança.

Política (a): \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

 3. Suponha que você é um profissional da área de segurança, responsável por implantar os níveis apontados na política de segurança num ambiente cooperativo de uma empresa XYZ. Então, indique, visualizando a rede XYZ desprotegida na figura abaixo, como a
política de segurança pode ser implementada para se ter (desenhe ou descreva):

(a) Esquematize uma segurança de perímetro definindo uma DMZ mais externa. Ou seja, em que pode consistir a DMZ mais externa ? Considera a figura abaixo, indicando uma solução DMZ.

 (b) Uma política segura de acesso, supondo que um cliente remoto tem acesso via linha telefônica até chegar no servidor NAS (Servidor de Acesso de Rede). Ou seja, como a empresa XYZ pode aumentar a segurança de acesso remoto ? Indique na figura abaixo, a solução para esta política de segurança.



4. O CETIC da UFSC descobriu que o sistema de emissão de documentos para seus alunos, estava apresentando problemas de segurança. Sabendo que o *login* a esse sistema é realizado informando o número da matrícula do aluno e mais um senha de acesso. Aponte possíveis vulnerabilidades e proponha um protocolo criptográfico para solucionar o problema apresentado, como segue: “Foram detectados acessos e uso do sistema, por matrículas de alunos, que negam ter realizado qualquer acesso. Especifique o protocolo, usando a notação ensinada em sala de aula.