SÉRIE PROVAS E CONCURSOS

Informática para Concursos

TEORIA E MAIS DE 180 QUESTÕES

3ª EDIÇÃO REVISTA E AMPLIADA

João Antonio

7ª Tiragem

ELSEVIER

CAMPUS
CONCURSOS

Noções de Segurança na Internet

Claro que, uma boa navegação ou troca de e-mails pela Internet está sujeita às intempéries causadas pelas pragas eletrônicas conhecidas como vírus de computador e pelos inconseqüentes bisbilhoteiros digitais autodenominados Hackers (vixi! Que texto bonito!). Pensando em minimizar os efeitos causados pelos vírus e pelas invasões de computadores, recomenda-se o uso de certos programas que ficam "na linha de frente" dos nossos sistemas como barreiras de defesa. Dentre os programas mais usados para essa finalidade, podemos destacar dois: O Antivírus e o Firewall.

Antivírus

Um programa Antivírus é usado para vasculhar o seu computador (ou a rede da empresa) à procura de vírus de computador. Esse programa funciona tanto de modo preventivo (tentando evitar a infecção por vírus) quanto de modo remediador (expulsando uma infecção existente ou excluindo os arquivos infectados).

Em tempo: um vírus de computador é um código (programa) malicioso que existe "parasitando" um arquivo qualquer (como arquivos do Word e do Excel). Um vírus é fabricado por um programador (um tremendo cretino, diga-se de passagem, mas muito competente no que faz), e é espalhado por meios de transmissão de dados variados, como disquetes ou a própria Internet.

Existem vários tipos de vírus de computador, eis alguns:

- **Vírus de programa:** Infectam arquivos de programa. Esses arquivos normalmente têm extensões como .COM, .EXE, .VBS, .PIF;
- **Vírus de Boot:** Infectam o setor de Boot de um disco rígido ou disquete - ou seja, o registro de inicialização em disquetes e discos rígidos. Os vírus de boot se copiam para esta parte do disco e são ativados quando o usuário tenta iniciar o Sistema Operacional a partir do disco infectado.
- **Vírus de Macro:** Infectam os arquivos dos programas Microsoft Office (Word, Excel, PowerPoint e Access). Esses vírus são normalmente criados com a linguagem de programação VBA (Visual Basic para Aplicações) e afetam apenas os programas que usam essa linguagem (o Office,

por exemplo). Os vírus de Macro são normalmente transmitidos em arquivos DOC e XLS (documentos do Word e planilhas do Excel)...

- **Vírus Stealth:** Este tipo de vírus é programado para se esconder e enganar o antivírus durante uma varredura deste programa.
- **Vírus Polimórficos:** Vírus que "mudam de forma". A cada nova infecção, esses vírus geram uma nova seqüência de bytes em seu código, para que o Antivírus se "confunda" na hora de executar a varredura e "não reconheça" o invasor. Os antivírus bons conseguem entender o disfarce e detectar o vírus, mesmo sendo "carne nova no pedaço".
- **Worms:** São programas parecidos com vírus, mas que na verdade apenas se copiam (não infectam outros arquivos, eles mesmos são os arquivos). Esses programas normalmente usam as redes de comunicação para infectar outros computadores (E-mails, Web, FTP, Redes das empresas etc.)
- **Cavalo de Tróia (Trojan):** não é exatamente um vírus. É um programa que atenta contra a segurança de um computador abrindo portas de comunicação para que invasores possam ter acesso ao computador. Essas portas são aquelas portas dos protocolos de aplicação da pilha TCP/IP, que, quando abertas, permitem que o computador receba pacotes direcionados a elas que, com certeza, não devem significar coisa boa!

A maioria dos programas Antivírus do mercado (gratuitos ou não) funcionam da seguinte forma: quando instalados no computador, fazem uma varredura completa procurando por vírus. Depois de verificar tudo, e limpar o que foi encontrado, eles se instalam e ficam na memória RAM do computador (e se registram para todas as vezes que o Sistema Operacional for iniciado, eles sejam abertos também), e ficam "tocaiando" a movimentação no sistema, procurando por ocorrências estranhas.

Quando um e-mail que está chegando ou um disquete que foi colocado no drive estiver trazendo um arquivo infectado, o antivírus avisa automaticamente e pede instruções sobre que comportamento deve tomar em relação à ameaça (limpar o vírus, apagar o arquivo, não fazer nada, etc.). Os melhores antivírus do mercado também são capazes de detectar e apagar os cavalos de tróia, para evitar invasões ao computador.

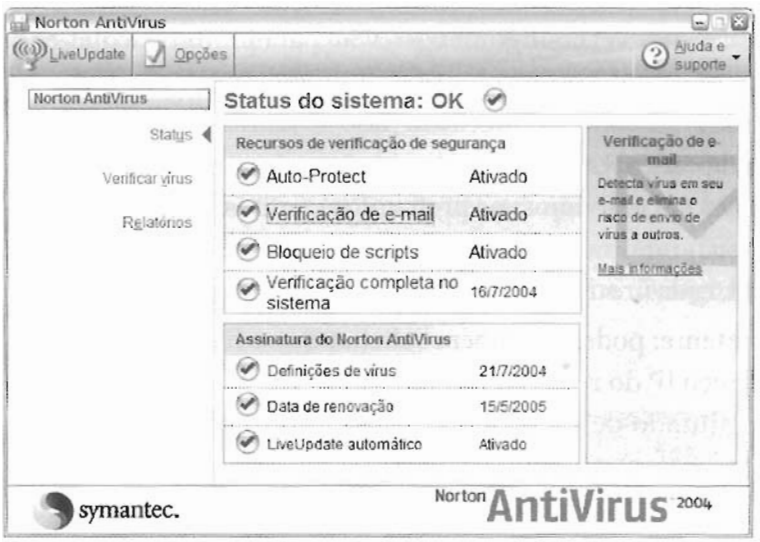

Figura 9.38 – Norton Antivírus – o mais confiável da atualidade (e mais pesado).

O programa antivírus que utilizo é o Norton Antivírus, da empresa Symantec, que é atualmente o mais confiável (em minha opinião) antivírus do mercado. O Norton Antivírus é vendido em qualquer loja de informática e, depois de comprado, permite a atualização por um ano gratuitamente na Internet.

Existem vários prós e um único contra no Norton Antivírus: ele é muito "pesado", ou seja, ele ocupa muita memória RAM e deixa o micro muito lento no momento da inicialização do Sistema Operacional (essa lentidão era mais acentuada nas versões anteriores, mas agora com a versão 2004, a Symantec parece que se "ajeitou", pois o programa está mais light).

Firewall

Um Firewall (ou "Porta Corta-Fogo", em alusão às portas que evitam a propagação de um incêndio) é um programa que analisa o tráfego de dados que entram em um computador (ou em uma rede) e filtra esses dados, permitindo a passagem de alguns e proibindo outros de acordo com regras predeterminadas.

Um firewall é capaz de filtrar os pacotes que entram na rede baseando-se em alguns critérios, como esses:

- **Porta:** é possível configurar o firewall para proibir pacotes endereçados a certas portas do protocolo TCP, limitando, assim, o tráfego de dados a certos protocolos conhecidos. Isso é particularmente interessante no caso de certos Trojans que abrem portas bem estranhas, acima do número 1024 (e, nós vimos, os protocolos comuns usam portas baixas). A filtragem por porta significa filtragem pelo protocolo de aplicação também, afinal, cada protocolo de aplicação está associado a uma porta específica.
- **Remetente:** pode-se também solicitar que o firewall filtre os pacotes pelo endereço IP do remetente. Isso é usado no caso de permitir apenas o tráfego oriundo de um determinado local (como de uma filial a outra em uma empresa). Quando se configura um firewall para filtrar pacotes pelo endereço, normalmente se cria as "zonas seguras" e as "zonas restritas". Todos os computadores cujos endereços estão listados em uma zona segura têm livre acesso à rede protegida pelo firewall, mas os endereços não contidos nesta zona serão vistos como indesejados pelo firewall.

Tanto na filtragem de pacotes pela porta quanto na filtragem por endereço, o administrador (pessoa responsável pela rede ou, pelo menos, pelo firewall) pode configurar o firewall de, basicamente, duas maneiras:

- **Informar os casos permitidos e proibir o restante:** significa indicar ao firewall uma listagem de dados (portas ou endereços IP) permitidos e restringir o acesso ao restante. Essa é a forma mais segura (e paranóica) de configurar um firewall. Ou seja, quando você entrega uma listagem VIP para o firewall, ele só vai permitir que passe por ele o que estiver descrito expressamente na listagem e bloquear o que não estiver na lista.
- **Informar os casos proibidos e permitir o restante:** é a configuração mais "light" de um firewall, que receberá uma lista de dados proibidos, mas não será capaz de bloquear o restante. Se você quiser sua rede (ou computador) com muita liberdade para aceitar todo tipo de conexão (por qualquer porta ou a partir que qualquer IP), configure seu firewall assim, mas depois não diga que eu não avisei!

Uma comparação interessante é a seguinte: pense num firewall como um segurança de uma boate (daqueles com 2.10 metros e 200 kg somado a uma cara de muito mau!), e você entrega a ele uma lista das pessoas que podem en-

trar na sua festa, recomendando que ninguém mais deva entrar! O que vai acontecer? Somente os convidados passarão pela barreira na porta.

Mas, se ao invés de uma lista de VIP, você entrega uma de "Personas Non Gratas", recomendando ao "armário" que deixe passar todos os que não estão na lista, o que vai acontecer? Simples, qualquer um que não for (ou não parecer) um integrante da lista vai conseguir passar. Inclusive, vão passar os integrantes da lista que se disfarçarem, demonstrando a falha de segurança nesse sistema.

Figura 9.39 – Norton Internet Security, com o Firewall Pessoal.

O Firewall que utilizo em meu computador é o Norton Personal Firewall, que acompanha o pacote Norton Internet Security (do qual o Norton Antivírus também faz parte), desenvolvido pela Symantec. É muito completo e bastante seguro!

Nas empresas, para proteger as redes, usa-se um programa firewall dentro de um equipamento, o que fez muita gente pensar que um firewall é uma máquina (tem gente que vende como sendo). Um firewall é um programa! Mas muitas empresas desenvolvem equipamentos com tal finalidade.

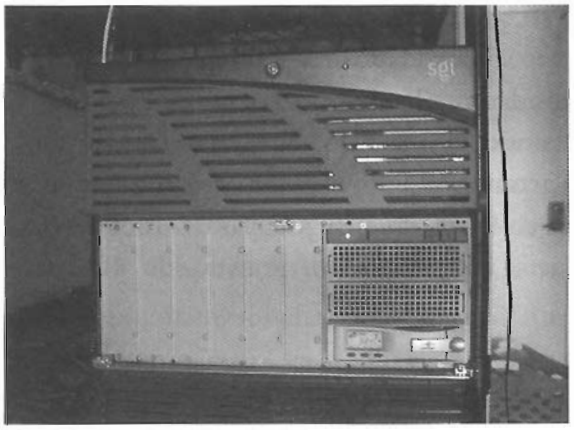

Figura 9.40 – Um firewall corporativo (equipamento).

Lembre-se bem: o tráfego dos dados maliciosos pode chegar ao firewall, mas não pode passar por ele, porque é ele justamente quem julga, de acordo com regras específicas, se aqueles dados devem passar ou não para dentro da sua rede.

Considerações Finais

Bem, acho que chegamos ao fim de mais uma etapa (por sinal, uma bem grande!). Espero que o seu interesse no assunto não fique restrito a esse material (se bem que ele está bastante completo). Existem muitos sites na Internet onde se podem buscar mais informações acerca destes assuntos!

Qualquer dúvida acerca dos assuntos vistos neste capítulo, não tenha pudor em me mandar um e-mail (agora que você já sabe como funciona na realidade o sistema). Lembre-se que contato@joaoantonio.com ou joaoacarvalho@terra.com.br são endereços das minhas caixas postais.

Encontrar-me na Web também é fácil: www.espacojuridico.com (onde sempre estou comentando algo no fórum) e www.pontodosconcursos.com.br (minha coluna de artigos).

Parte 12

Segurança da Informação

Comentários Iniciais

Bem, pessoal, começamos aqui mais um passo no aprendizado da informática para concursos: a segurança da Informação, que, apesar de ainda não ser tão cotidiana, passará a ser vista com mais freqüência em muitos concursos vindouros (inclusive porque já foi vista em concursos anteriores).

Princípios da Segurança da Informação

Por que segurança? Por que estar preocupado com o meu sistema de computação? Quais os quesitos para classificar meu sistema como sendo seguro? E mais... O que a segurança da Informação pode fazer por mim?

A Segurança da Informação é o conjunto de técnicas, processos e componentes que visa garantir um certo nível de confiabilidade às transações digitais. Os princípios básicos que definem a segurança da informação são 4, que podem ser lembrados pela sigla DICA (ou CIDA, se preferir).

Disponibilidade: é a garantia de que um sistema estará sempre disponível quando necessário (ex: ao acessar um site e ele aparecer, ele estava disponível – se ele não aparecer ou não for possível acessá-lo, o princípio da disponibilidade foi afetado). Uma forma de manter a disponibilidade de um sistema é implantar estruturas de no-breaks (para impedir que quedas de energia afetem os sistemas), espelhamento de disco (RAID 1), espelhamento de servidores (ter dois ou mais servidores fornecendo o mesmo serviço), etc.

Integridade: é a garantia de que uma informação não foi alterada durante seu trajeto do emissor para o receptor. Tendo a garantia de dados íntegros, o receptor pode se assegurar de que a mensagem que ele recebeu tem realmente aquele conteúdo (ex: se um e-mail foi alterado antes de chegar ao destino, a

Integridade foi maculada, mas o receptor não saberia disso até que tomasse alguma decisão embasada no conteúdo fajuto do e-mail).

Confidencialidade (Sigilo): é a garantia de que os dados só serão acessados por pessoas autorizadas, normalmente detentoras de login e senha que lhes concedem esses direitos de acesso. Também se refere à garantia de que um e-mail, por exemplo, não será lido por outrem a não ser o destinatário devido (ex. uma interceptação de um e-mail e a leitura deste por parte de alguém estranho à transação é um atentado à confidencialidade).

Autenticidade: é a garantia da identidade de uma pessoa (física ou jurídica) ou de um servidor (computador) com quem se estabelece uma transação (de comunicação, como um e-mail, ou comercial, como uma venda on-line). Essa garantia, normalmente, só é 100% efetiva quando há um terceiro de confiança (uma instituição com esse fim: certificar a identidade de pessoas e máquinas) atestando a autenticidade de quem se pergunta (ex: quando você se comunica, pela internet, com o site do seu banco, você tem completa certeza que é COM O SEU BANCO que você está travando aquela troca de informações?).

Quando se puder associar, de forma única e certeira, um ato ou documento digital a uma pessoa física (cidadão) ou jurídica, será possível estabelecer regras jurídicas para as transações digitais.

Ainda podemos citar um termo muito interessante, que é bastante usado nesse "assunto" de segurança: **Não-Repúdio**.

Não-Repúdio: é a garantia de que um agente não consiga negar falsamente um ato ou documento de sua autoria. Essa garantia é condição necessária para a validade jurídica de documentos e transações digitais. Só se pode garantir o não-repúdio quando houver Autenticidade e Integridade (ou seja, quando for possível determinar quem mandou a mensagem e quando for possível garantir que a mensagem não foi alterada). Novamente, entramos no mérito de que só haverá tal garantia 100% válida, se houver uma instituição que emita essas garantias.

Ameaças aos Sistemas de Informação

São componentes que podem prejudicar, de forma temporária ou permanente, o funcionamento de um sistema de informação. As políticas e agentes de segurança têm como principal objetivo evitar que tais componentes tenham sucesso.

Defeitos de Hardware: Aí, vai do azar de cada um... Infelizmente, não há como prever tais falhas. O que se pode fazer para evitar que tais problemas danifiquem o sistema é a realização periódica de cópias de segurança (Backups).

Vírus de Computador (Vírus Informático): programas maliciosos, criados para se replicar automaticamente e danificar o sistema. Existem vários tipos de vírus com várias características interessantes... Veremos todos adiante. Mas lembre-se de que a principal característica de um vírus é sua capacidade de se copiar sozinho e de anexar-se a arquivos (os vírus não existem sozinhos (autônomos), mas somente infectando arquivos aparentemente normais). Um bom programa **Antivírus** evitaria (ou minimizaria) o risco de tais infecções.

Worms: programas autônomos (não parasitam arquivos, pois eles são os próprios arquivos) que se replicam pela estrutura das redes, como aqueles que se copiam pela Internet, através de mensagens de e-mail.

Cavalos de Tróia (Trojan): programas que criam "canais" de comunicação para que invasores entrem num sistema. Quando um programa desses é "executado" em um computador, ele manda pacotes de informação por meio de uma porta de comunicação qualquer ao seu dono (pessoa que o enviou à vítima). Depois de enviar tal pacote, é estabelecida uma conexão naquela porta específica, permitindo a transferência de informações entre o atacante e o atacado e permitindo até mesmo que o computador da vítima seja controlado pelo invasor. Um **Firewall** bem configurado "cortaria" as relações entre os dois, evitando a comunicação por meio de portas não autorizadas.

Hackers: usuários experientes que invadem sistemas de informação. Os indivíduos denominados Hackers não são necessariamente ameaças, pois, assim como as Medidas Provisórias, existem os "Hackers do bem". Apenas são conhecidos pelos seus conhecimentos avançados em informática e, especialmente, redes de comunicação. Alguns poucos indivíduos desta categoria são capazes de peripécias antológicas, como a invasão de sistemas de segurança da NASA e do Pentágono, portanto, teoricamente, nada os pararia, mas a maioria dos que se auto-intitulam Hackers não consegue ultrapassar um firewall bem configurado e um sistema atualizado.

Programas Desatualizados: os sistemas operacionais e aplicativos apresentam falhas diversas que, com o tempo, "caem na boca do povo". Quando uma falha é descoberta, os hackers (e os quase-hackers) de plantão saem à procura de sistemas que ainda não foram atualizados e que, por isso, ainda possuem tais falhas. Manter o Windows atualizado, bem como qualquer outro programa de

comunicação com a Internet, é exigência para se ter um sistema menos suscetível a invasores.

Spam: envio de mensagens de e-mail em grande número (sem autorização dos destinatários). O SPAM não é uma ameaça à segurança em si, mas que é chato, é! Alguns programas, ditos Anti-Spam, tentam diminuir os efeitos dessa prática abusiva, mas muitas vezes sem sucesso (os programas filtram quais as mensagens que devem ser consideradas Spam e quais devem ser consideradas mensagens válidas, mas, muitas vezes, não as classificam direito!).

Usuários descontentes/leigos: podem causar problemas com/sem intenção (respectivamente). Quando um usuário não sabe o que está fazendo ou não consegue mensurar a importância de sua senha estar bem guardada, muitos problemas podem acontecer por meio de ataques ao sistema da empresa propiciados pela, digamos, "ingenuidade" do usuário. A Intenção de causar problemas ou de abrir portas para invasores pode ser também fator marcante dentre os problemas que um sistema de informação pode enfrentar.

Exploits: programas que exploram falhas em sistemas de informação. São programas prontos que os Hackers constroem para os que "estão na escolinha de Hacker". Esses programas são criados para utilizar as falhas previamente descobertas nos sistemas.

Sniffers: programas que espionam a comunicação em uma rede ("escutam" o que os outros falam). São chamados de "programas farejadores". Quando instalados em servidores proxy ou gateways de uma rede, podem armazenar ou enviar (para o espião) todos os pacotes que trafegam pela rede e ele, o bisbilhoteiro, poderá ler os pacotes (pois a maioria deles é de texto, simplesmente). As comunicações criptografadas não são compreendidas por quem está "farejando" a rede. O uso de switches, ao invés de hubs, pode minimizar esses tipos de ataques, especialmente se o programa farejador está instalado apenas no computador do atacante.

Port Scanners: programas que vasculham um computador à procura de portas de comunicação abertas. Esses programas ficam analisando, seqüencialmente, as diversas portas de um computador, enviando vários pacotes seguidos para esse computador com números de portas diferentes, apenas para receber a resposta de uma delas e, com isso, constatar a presença de portas abertas. Um programa **Firewall** pode fechar todas as portas desejadas, evitando maiores riscos com essa técnica. Um programa **IDS** (Sistema Detector de Intrusos) pode analisar o comportamento suspeito de mandar pacotes seguidos a várias portas e diagnosticar aquilo como sendo uma tentativa de **port scan**.

Backdoor: "Porta dos fundos" – é uma brecha, normalmente colocada de forma intencional pelo programador do sistema, que permite a invasão do sistema por quem conhece a falha (o programador, normalmente). Acredita-se que sistemas comerciais famosos, como o Windows, possuam Backdoors para que a Microsoft possa obter informações do micro sem que o usuário invadido saiba.

Spyware: programas, instalados no computador da vítima, que "filmam" tudo o que ela faz. São programas pequenos que "copiam" tudo o que se digita no micro afetado e/ou armazenam uma lista das páginas visitadas e enviam esses dados para o computador do bisbilhoteiro. Existem diversos programas **Anti-Spyware**, mas um bom antivírus já detectaria essa presença desagradável e tomaria as providências cabíveis.

Adware: programas que, instalados no computador do usuário, realizam constantemente a abertura de janelas (popus) de anúncios de propaganda. Normalmente, esses programas são confundidos com vírus, mas não são classificados desta maneira.

Malware: é apenas um termo genérico, usado muito recentemente pela ESAF, para designar todo programa de computador construído com intenções maldosas (ou seja, os programas que estamos vendo aqui nesta lista!).

Engenharia Social: técnica muito utilizada pelos hackers para obter, graças à ingenuidade das pessoas, informações necessárias e relevantes sobre o sistema a ser invadido. Exemplo: Um invasor liga para uma secretária de uma empresa se fazendo passar por um funcionário da manutenção da companhia telefônica, e, para realizar testes, precisa que ela forneça a senha de acesso à rede da empresa... Coisas desse tipo...

Tipos de Vírus de Computador

Vírus de Boot: afetam o setor de boot e o Sistema Operacional. Normalmente se copiam para o MBR do HD, apagando seu conteúdo ou permanecendo lá, para serem carregados sempre que o Sistema Operacional for executado (na inicialização da máquina).

Vírus de Macro: afetam os programas da Microsoft que são baseados em VBA (Visual Basic for Applications). As instruções destes vírus são, na verdade, macros existentes em arquivos .DOC ou .XLS (.MDB do Access também), que, quando executadas, dão origem a várias operações inconvenientes no micro (incluindo o apagamento de arquivos).

Agentes da Segurança

Antivírus: programa residente na memória (fica sempre na memória RAM) que protege o sistema contra infecções de vírus de computador (vírus "informático" é um nome atualmente usado).

Um antivírus tanto evita novas infecções como limpa o sistema de infecções já estabelecidas. Um antivírus normalmente degrada o desempenho do computador por estar sempre executando na memória RAM e, na maioria dos casos, ser muito "pesado". Antivírus não são sistemas efetivos contra tentativas de invasão.

Firewall: programa que cria uma "barreira" de proteção contra invasores (na verdade, contra, especificamente, as tentativas de comunicação com o computador protegido). Um firewall pode bloquear as comunicações por diversos critérios, como os **filtros de pacotes** (o tipo mais comum de firewall) que pode proibir ou permitir a passagem de um pacote de acordo com a porta de comunicação utilizada.

Existem Firewalls muito mais inteligentes que conseguem detectar tentativas de invasão em pacotes cujas portas são consideradas lícitas, por exemplo, quando a tentativa de invasão é feita por uma página da web (todos os pacotes daquela página serão, por padrão, transmitidos pela porta 80), um firewall filtro de pacotes não encontraria nada malicioso nesses pacotes e iria permitir sua passagem completa. Mas, se nesses pacotes "lícitos" houver uma tentativa de invasão escondida, um **Firewall de Aplicação** poderá detectá-la e impedi-la.

IDS: Sistema Detector de Intrusos (IDS) é um conjunto de tecnologias (programas, hardware) que objetiva descobrir, em uma rede, os acessos não autorizados a ela que podem indicar a ação de invasores. Os scanners de portas, os cavalos de tróia, os pacotes endereçados a portas estranhas são indícios de possíveis ações maliciosas de invasores.

Anti-Spam: programas que podem classificar as mensagens de e-mail recebidas como sendo aceitáveis ou como sendo spam (indesejadas). Esse programa permite que os usuários não sejam incomodados com essa prática desagradável. Como um spam pode trazer outras coisinhas chatas consigo (vírus, worms, trojans), o anti-spam é um recurso bastante interessante para que nossas caixas postais sejam usadas para armazenar apenas o necessário.

Criptografia: processo matemático para embaralhar uma mensagem digital, tornando sua leitura incompreensível por pessoas que não possuam a chave (código) para desembaralhar a mensagem. A criptografia pode ser usada,

atualmente, para manter os dados sigilosos (privacidade) e para garantir a identidade do remetente de uma mensagem (autenticidade).

É a criptografia a "alma" dos processos de certificação digital e assinatura digital, que começaremos a estudar agora...

Criptografia

Como já foi dito, a criptografia (Cripto=enigma, grafia=escrever – "A arte de escrever por enigmas") é um processo matemático usado para embaralhar os dados de uma mensagem que deve ser secreta (confidencial).

Entendendo a Criptografia

A principal finalidade da criptografia é, sem dúvida, reescrever uma mensagem original de uma forma que seja incompreensível, para que ela não seja lida por pessoas não autorizadas. Veja um exemplo:

Mensagem Original		Mensagem Embaralhada
Olá, pode pagar ao cliente!	→	J#%9(aAs##1!2)%"&&sDoPPoghklQw

A idéia só funciona, claro, se a pessoa autorizada a ler a mensagem (o receptor, destinatário, interlocutor, etc.) puder transformar a mensagem embaralhada de volta em mensagem legível.

Então, temos que entender que os dois envolvidos oficiais na comunicação precisam acordar em algo ("acordar" não de "despertar", claro, mas de "entrar em acordo" – essa explicação é somente para você, aluno, "acordar" dessa leitura chata!).

Pense nisso:

– João e José vão trocar números (senhas) pessoalmente, durante uma reunião na empresa, mas ninguém pode saber das senhas. Eles ainda não possuem tais números, mas, antes da reunião, cada um vai saber qual é a sua senha (aí você me pergunta: "Ei João, que estória é essa?" – Calma! Seja criativo: imagine que João e José são espiões, sei lá!)

– Eles decidem (previamente, claro) que não vão passar-se mutuamente os números em voz alta, em vez disso, vão dividi-los por 43 e passar o resultado