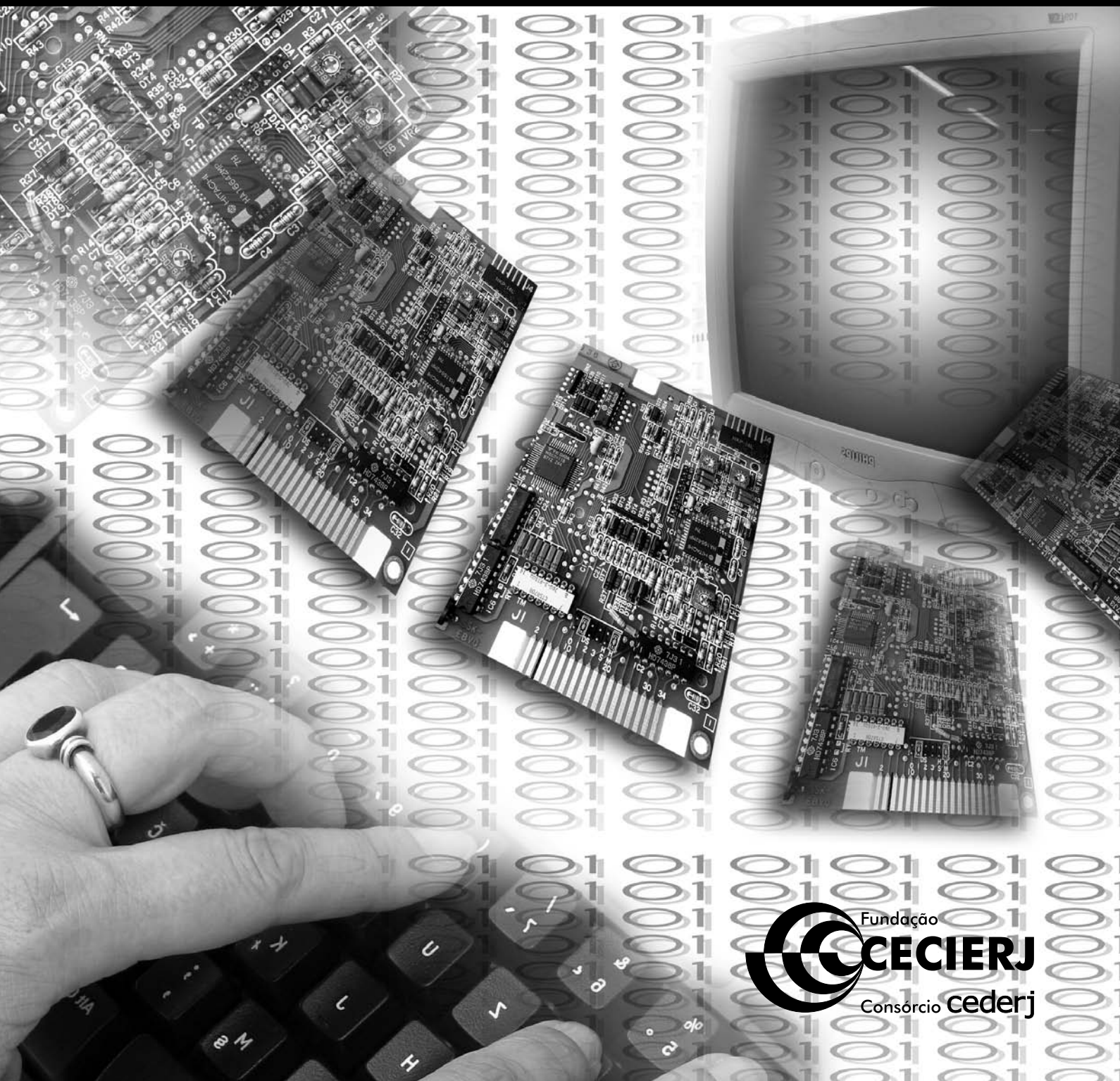
Módulo 1

Volume | 1

Celso Costa
Luiz Manoel Figueiredo

Introdução à Criptografia



Fundação CECIERJ
Consórcio cederj

Fundação CECIERJ

Consórcio cederj

Centro de Educação Superior a Distância do Estado do Rio de Janeiro

Introdução à Criptografia

Volume 1 - Módulo 1

Celso Costa
Luiz Manoel Figueiredo

UFF – Instituto de Matemática
Celso José da Costa

EB – Centro de Estudos de Pessoal
Antônio Carlos Guelfi

O material constante desta disciplina foi produzido sob o auspício de Convênio de cooperação técnico-acadêmica entre o Exército Brasileiro e a Universidade Federal Fluminense.

GOVERNO DO Rio de Janeiro
SECRETARIA DE CIÊNCIA E TECNOLOGIA

UAB UNIVERSIDADE ABERTA DO BRASIL

Ministério da Educação

BRASIL UM PAÍS DE TODOS GOVERNO FEDERAL

Apoio:

FAPERJ
Fundação Carlos Chagas Filho de Amparo à Pesquisa do Estado do Rio de Janeiro

Fundação Cecierj / Consórcio Cederj

Rua Visconde de Niterói, 1364 – Mangueira – Rio de Janeiro, RJ – CEP 20943-001
Tel.: (21) 2334-1569 Fax: (21) 2568-0725

Presidente
Masako Oya Masuda

Vice-presidente
Mirian Crapez

Coordenação do Curso de Matemática
UFF - Regina Moreth
UNIRIO - Luiz Pedro San Gil Jutuca

Material Didático

ELABORAÇÃO DE CONTEÚDO
Celso Costa
Luiz Manoel Figueiredo

EQUIPE DIDÁTICO-PEDAGÓGICA
Mônica Nogueira da Costa Figueiredo
Vanessa Maria Barbosa Queiroz

PROJETO GRÁFICO
Maria Rachel Barbosa

REVISÃO
Letícia Maria Lima Godinho
Vanessa Maria Barbosa

PROGRAMAÇÃO VISUAL
Maria Rachel Barbosa
Rafael Fontenele

CAPA
Marcelo Freitas

PRODUÇÃO GRÁFICA
Oséias Ferraz
Patricia Seabra

C837c

Costa, Celso.
Introdução à criptografia. v. 1 / Celso Costa. – Rio de Janeiro: UFF / CEP – EB, 2010.
100p.; 21 x 29,7 cm.

ISBN: 85-7648-303-3

1. Criptografia. 2. Segurança computacional. 3. História da criptografia. I. Figueiredo, Luiz Manoel II.Título.

CDD: 510

2010/1

Publicado por: Centro de Estudos de Pessoal (CEP)

Governo do Estado do Rio de Janeiro

Governador
Sérgio Cabral Filho

Secretário de Estado de Ciência e Tecnologia
Alexandre Cardoso

Universidades Consorciadas

UENF - UNIVERSIDADE ESTADUAL DO NORTE FLUMINENSE DARCY RIBEIRO
Reitor: Almy Junior Cordeiro de Carvalho

UERJ - UNIVERSIDADE DO ESTADO DO RIO DE JANEIRO
Reitor: Ricardo Vieiralves

UFF - UNIVERSIDADE FEDERAL FLUMINENSE
Reitor: Roberto de Souza Salles

UFRJ - UNIVERSIDADE FEDERAL DO RIO DE JANEIRO
Reitor: Aloísio Teixeira

UFRRJ - UNIVERSIDADE FEDERAL RURAL DO RIO DE JANEIRO
Reitor: Ricardo Motta Miranda

UNIRIO - UNIVERSIDADE FEDERAL DO ESTADO DO RIO DE JANEIRO
Reitora: Malvina Tania Tuttman

Sumário

Programa da disciplina

Ementa

Conceitos Básicos de Criptografia e Segurança em Rede: criptografia e segurança em rede, ataques a sistemas computacionais, serviços de segurança. História da Criptografia: criptografia na Antiguidade, na Idade Média e Moderna. História recente da Criptografia e atualidade.

Carga horária

30 horas

Objetivos

• Conhecer os conceitos básicos de Criptografia e Segurança em Rede, as categorias gerais de ataque e os principais meios utilizados, e os serviços básicos de segurança oferecidos por sistemas criptográficos.

• Compreender a história da Criptografia da Antiguidade à atualidade, através dos grandes marcos históricos e da mudança ocorrida com o surgimento dos computadores.

Metodologia

O conteúdo programático será apresentado na forma de textos e exemplos, com atividades a serem realizadas. Para complementar seu estudo, serão sugeridos livros, filmes e websites.

Avaliação

Trabalho ao final da disciplina e avaliação a distância (tarefas online).

Programa da disciplina

Plano de aulas - Unidade 1

- **Conceitos Básicos de Criptografia**

Conteúdo	Onde encontrar
Aula 1 - Criptografia e segurança em rede O conceito de criptografia Segurança da informação e segurança em rede Políticas de segurança Criptografia e segurança no dia-a-dia	**Textos 1 a 5**
Aula 2 - Ataques a sistemas computacionais Categorias de ataques	**Textos 6 a 8**
Aula 3 - Serviços de segurança Confidencialidade Autenticação Não-repudiação Controle de acesso	**Texto 9**
Aula 4 - Modelo de segurança em rede Exemplo de um sistema com comunicação segura	**Texto 10**

Carga horária: 14 h

Plano de aulas - Unidade 2

- **História da Criptografia**

Conteúdo	Onde encontrar
Aula 5 - Criptografia na Antiguidade O início da criptografia	**Texto 11**
Aula 6 - Criptografia na Idade Média Cifras monoalfabéticas Pré-história da criptoanálise	**Textos 12 a 14**
Aula 7 - Criptografia na Idade Moderna Cifra de Roussignol A quebra da Cifra de Vigenère	**Textos 15 a 17**
Aula 8 - História recente Criptografias mecânica e eletrônica	**Textos 18 e 19**
Aula 9 - Atualidade Computadores e representação da informação Criptografia híbrida Autenticidade, certificação e assinaturas digitais	**Textos 20 a 23**

Carga horária: 16 h

Unidade 1

Conceitos básicos de Criptografia

Introdução à Criptografia

Caro aluno, com esta disciplina você inicia seu curso de Especialização em Criptografia e Segurança em Redes, um campo de estudo que interessa a grandes empresas, bancos, militares, serviços secretos, gerentes de rede e hackers, enfim, a pessoas que desejam proteger uma informação e a outras que pretendem conhecê-la.

A necessidade de proteger uma informação, seja armazenada ou em trânsito, tem sido uma preocupação e um campo de estudo desde a Antiguidade. Com o advento dos computadores, o armazenamento e a transmissão da informação passaram a ser feitos, em grande parte, em sistemas informatizados, tornando-se imprenscindível protegê-los.

Nesta unidade 1 veremos uma introdução aos temas centrais do curso: criptografia, segurança da informação e segurança em rede. Bom estudo!

Desde a Antiguidade, a habilidade de disfarçar uma mensagem de forma que somente o destinatário possa acessá-la tem sido muito importante. Generais precisam dar ordens a seus comandados sem que essas caiam nas mãos do inimigo, o que poderia alertá-lo sobre as táticas, os movimentos de tropas etc.

Líderes políticos precisam trocar informações com seus aliados e comandados. Para eles é vital que estas informações estejam a salvo de adversários e curiosos. Enfim, a arte de disfarçar, tornar secreta, codificar uma mensagem e transmiti-la de forma que somente o destinatário possa compreendê-la, evitando que qualquer outro possa roubar esta informação, tem sido vital em várias áreas.

Irmã gêmea da antiga arte de criar códigos está a de quebrá-los, de desenvolver técnicas que permitam decifrar uma mensagem codificada com a finalidade de descobrir seu conteúdo e, até mesmo, modificá-lo antes que chegue a seu destinatário.

É uma espécie de jogo de gato e rato, presa e predador, em que cada novo avanço na técnica de codificar leva a pesquisas de novas técnicas de ataque.

Se reis, rainhas e generais dependeram, confiaram e muitas vezes foram traídos por suas técnicas de codificação, hoje, na era da internet e da comunicação instantânea, mas também de vírus, hackers, fraudes eletrônicas e total dependência de sistemas informatizados em rede, a segurança da informação é um conceito primordial para empresas e governos.

Atualmente, tanto indivíduos como organizações possuem uma grande dependência dos meios eletrônicos para armazenamento de informações. Por outro lado, existe também um alto grau de conectividade entre os sistemas informatizados, isto é, os sistemas se encontram, de maneira geral, ligados em rede.

Este fato traz algumas preocupações em relação a qualquer informação sensível armazenada em computadores:

• Como garantir a segurança? Normalmente, uma informação armazenada deve ser acessível apenas para uma pessoa ou um grupo de indivíduos que tenham direito a conhecê-la.

• Como afirmar que uma informação armazenada não terá seu conteúdo modificado por alguém? Um inimigo pode querer não só acessá-la, mas substituí-la por uma cópia modificada.

A interconexão quase universal nos sistemas informatizados leva a um maior cuidado com os ataques em rede, isto é, a tentativa de acesso indevido pode vir de pessoas fisicamente distantes dos sistemas onde a informação está armazenada.

Texto 1 - O conceito de criptografia

A primeira idéia que vem à mente quando pensamos em transmitir uma mensagem a outra pessoa, de forma que somente o receptor tenha acesso, é escondê-la em algum meio de comunicação, não é mesmo?

Técnicas para ocultar uma mensagem e transmiti-la de maneira secreta têm sido usadas há muitos anos, sendo algumas bem inventivas, quando não curiosas.

Heródoto conta a história de um grego que precisava transmitir uma mensagem secretamente. Ele então raspa o cabelo do mensageiro, tatua a mensagem na cabeça raspada e espera que o cabelo cresça novamente. Ao chegar ao destinatário, o mensageiro raspa a cabeça, revelando a mensagem.

O historiador grego Heródoto (484 a.C. - 426 a.C) é considerado o pai da História. Viajou por vários países e sua obra principal é a "História", dividida em nove livros.

O historiador conta também que uma mensagem secreta escrita em tábuas de madeira e cobertas em cera, transmitida desta maneira por um grego que vivia em solo persa, alertou os gregos sobre os preparativos do rei persa Xerxes para invadir e conquistar a Grécia. A mensagem precisou ser escondida para que passasse pelos guardas persas no caminho para a Grécia. Graças ao alerta, os gregos se prepararam adequadamente para o ataque e derrotaram a frota persa invasora.

Em ambos os relatos, uma mensagem foi escondida de uma determinada maneira. Caso fosse encontrada, seu conteúdo poderia ser lido pelo inimigo, sem nenhum esforço.

Este tipo de técnica que oculta a mensagem é chamada esteganografia. A palavra deriva do grego steganos, coberto, e graphia, escrita.

A história está repleta de episódios interessantes onde técnicas esteganográficas foram utilizadas.

Durante a Segunda Guerra Mundial, agentes alemães, que operavam na América Latina, utilizaram uma técnica de transmissão de mensagem que consistia em, usando técnicas de fotografia, microfilmar uma página de texto, reduzindo o filme ao tamanho de um ponto.

Este ponto era colocado sobre um ponto final, em uma carta de conteúdo totalmente insuspeito. O receptor, ao ter acesso à mensagem, procurava pelo ponto com a informação e ampliava-o a fim de ler a mensagem. Os aliados descobriram a técnica em 1941 e passaram a interceptar a comunicação.

A principal deficiência deste tipo de técnica é que caso a mensagem seja descoberta, ela está aberta, podendo ser lida por qualquer um.

A criptografia utiliza um outro conceito que é o de modificar a mensagem de forma que somente o destinatário possa entendê-la.

Com a criptografia, a mensagem não é compreensível por outra pessoa que não o destinatário.

Para que isso aconteça, a mensagem é embaralhada de certa maneira, usando alguma técnica combinada entre o emissor e o receptor, de forma que o segundo, e apenas ele, saiba arrumar, retornar ao texto original e à mensagem que o primeiro embaralhou.

Assim, a interceptação da mensagem em trânsito não permite, em princípio, que seu conteúdo seja revelado.

A palavra criptografia deriva do grego kryptos, secreto, e graphia, escrita, significando escrita secreta. Perceba que:

Criptografia # Esteganografia

Técnicas clássicas de embaralhamento de uma mensagem são a substituição e a transposição.

Substituição

Consiste em trocar uma letra por outra. Um exemplo simples seria um sistema em que cada letra é trocada pela letra seguinte do alfabeto. Por exemplo, a palavra casa seria transformada em dbtb.

C	—>	D
A	—>	B
S	—>	T
A	—>	B

Transposição

Tem como base trocar a posição das letras na mensagem.

Estudaremos estas técnicas mais detalhadamente no decorrer do curso.

Segundo o dicionário Houaiss, criptografar significa cifrar um texto, reproduzi-lo em código não conhecido, tornando-o, desse modo, intencionalmente ininteligível para os que não têm acesso às suas convenções.

O objetivo da criptografia não é esconder uma mensagem, mas ocultar seu conteúdo e torná-lo ininteligível para qualquer indivíduo que não conheça o procedimento, impedindo que este inverta o processo.

Algumas vezes, a criptografia e a esteganografia podem ser utilizadas juntas. Relata-se que, em alguns casos, os agentes alemães que usavam a técnica

do microponto, criptografavam a mensagem antes de enviá-la, aumentando bastante o nível de segurança.

Texto 2 - Segurança da informação e segurança em rede

Como vimos, a segurança da informação é um dos objetivos básicos da criptografia. A informação tornou-se um elemento fundamental na vida das pessoas e das empresas. Hoje, utiliza-se cada vez mais recursos computacionais para armazenar, produzir e distribuir informações. Com isso, aumenta-se também a preocupação com a segurança desta informação e com a vulnerabilidade dos sistemas computacionais que as gerenciam.

Podemos definir segurança em rede como o processo de prevenir e detectar qualquer uso não autorizado de uma rede de computadores.

Prevenir tem o sentido de tomar medidas que impeçam ou, pelo menos, dificultem ao máximo, o acesso de pessoas não autorizadas (chamadas de "intrusos") a qualquer parte de uma rede de computadores.

Detectar significa determinar se alguém tentou acessar o sistema, como foi a tentativa de acesso (o chamado "ataque"), se foi ou não bem-sucedida, e, em caso afirmativo, perceber exatamente o que o intruso fez.

Mesmo sistemas que aparentam despertar pouco interesse aos hackers, como os de uma universidade ou os domésticos ligados à internet, são constantemente alvos de ataques. Detectar estas investidas e os métodos utilizados é muito importante para uma política de segurança.

Grande parte dos indivíduos, mesmo aqueles que não lidam com informações secretas, como segredos militares e industriais, utiliza no cotidiano computadores para uma série de atividades. São feitas transações bancárias, compras pela internet, trocas de emails com amigos e de mensagens em programas de bate-papo, enfim, há uma variedade de informações pessoais nos computadores que são valiosas e que não devem ser examinadas por intrusos.

Algumas vezes, intrusos podem não ter atenção especial pela identidade, mas querem usar os sistemas para lançar ataques em outros sistemas computacionais. Ao utilizar um sistema pouco defendido, um hacker pode gerar ataques a sistemas governamentais e financeiros, ocultando sua real localização.

Assim, a segurança da informação é relevante para toda a sociedade. É importante que indivíduos e organizações adotem medidas que garantam níveis razoáveis de segurança em seus sistemas computacionais.

Podemos concluir que a área de segurança em rede tem se tornado de extrema importância, o que torna o profissional especializado nessa área em um elemento valioso e, em geral, bem remunerado nas organizações.

Texto 3 - Políticas de segurança

O que é um sistema seguro? A resposta depende de que nível de segurança se precisa. Em termos de segurança da informação, uma empresa que lida com segredos industriais, militares ou dados bancários tem demandas distintas em relação a uma pequena empresa de prestação de serviços, por exemplo. Cada organização possui diferentes necessidades de segurança no armazenamento e na comunicação da informação em meio eletrônico.

As políticas de segurança devem ser coerentes com as necessidades das organizações.

Há muitas ferramentas disponíveis para a segurança de uma rede de computadores e também para o ataque. Elas podem ser de dois tipos: aplicativos (software) e equipamentos (hardware). As ferramentas evoluíram nas últimas décadas, da mesma que forma que as técnicas de ataque se aprimoraram.

O uso de software e de hardware adequado podem proteger sistemas computacionais em diversos níveis. No entanto, ainda que sejam elementos essenciais da segurança de qualquer rede, o simples uso de software e hardware de segurança não constitui uma política de segurança adequada. Muitas vezes o item de segurança mais óbvio é negligenciado: o acesso físico aos computadores. É muito difícil manter a segurança de uma rede se um intruso tem acesso físico às máquinas que gerenciam a rede.

Nas disciplinas de Segurança em Rede 1 e 2 você estudará detalhadamente os conceitos envolvidos em segurança em rede, software e hardware de segurança.

Texto 4 - Criptografia e segurança no dia-a-dia

Serão apresentadas neste texto as técnicas de criptografia e as ferramentas de segurança em rede que são usadas no dia-a-dia, porém nem sempre são percebidas.

Internet

O número de pessoas que acessa a internet ou que possui páginas pessoais é cada vez maior. Grande parte das organizações oferece não só informações, mas serviços pela rede mundial de computadores. Atualmente, podemos comprar vários produtos pela internet, pagar o imposto de renda e usar praticamente todos os serviços do banco.

Todas as atividades mencionadas envolvem a transmissão de informação sensível, como número de cartão de crédito, informações sobre o patrimônio da pessoa (no caso do imposto de renda) etc. É evidente que a informação precisa ser protegida.

As transações mencionadas anteriormente usam sistemas criptográficos antes do envio da informação. O programa do imposto de renda criptografa toda a informação antes de transmiti-la ao servidor da Receita Federal. Os sites que vendem produtos e serviços com uso do cartão de crédito utilizam uma forma de "navegação segura", o que consiste no uso de protocolos que criptografam a informação antes de seu envio.

Verifica-se que o navegador está em modo seguro pelo endereço da página. Endereços na internet normalmente começam por "http://", que é o nome do protocolo usado. Os endereços de sites seguros começam por "https://".

HTTP significa Hypertext Transfer Protocol. É o protocolo de transferência de arquivos hipertexto (textos com links, figuras etc.) através da internet. Necessita de um programa cliente de um lado (um navegador, por exemplo) e um servidor de web do outro. É o protocolo mais usado.

HTTPS é uma combinação de HTTP e de um protocolo de criptografia chamado SSL.

SSL significa Secure Socket Layer. É um protocolo utilizado para comunicação segura, autenticação e criptografia sobre redes.

Os navegadores apresentam um ícone visual indicando que estamos navegando em páginas seguras.

Navegador	Modo não-seguro	Modo seguro
Internet Explorer	Nenhum	
Netscape		

Na disciplina Segurança em Redes estudaremos estes e muitos outros protocolos envolvidos para uma comunicação segura na internet.

Email

A comunicação eletrônica tornou-se parte do dia-a-dia das pessoas. Atualmente, milhões de emails são enviados a cada dia, o que os tornaram também portas de entrada de vírus, que, em geral, propagam-se como arquivos anexos nas mensagens.

Hoje, emails podem conter links para a internet, o que também possibilita a transmissão de vírus. Uma mensagem pode induzir o receptor a clicar em um link ao achar que trata-se de uma informação útil, mas na verdade o liga a um download de vírus.

Porém, há outro problema de segurança relacionado aos emails: a informação trafega pela internet, passando por vários servidores, em princípio com texto aberto, no qual qualquer indivíduo pode conseguir interceptá-la e ler seu conteúdo.

Phil Zimmermann, engenheiro de software americano nascido em 1954, criou um programa de segurança para correio eletrônico, livremente disponível, chamado PGP (Pretty Good Privacy). Este programa usa uma combinação do IDEA, que é um protocolo de criptografia de chave privada (onde tanto o emissor quanto o destinatário devem conhecer uma chave), com um protocolo de chave pública, o RSA, usado essencialmente para a troca da chave que será usada no IDEA. O PGP é o software de criptografia de email mais utilizado no mundo.

A vantagem é que a criptografia de chave privada, muito mais sólida, é usada para codificar o corpo da mensagem, que pode ser muito extensa, enquanto que a criptografia de chave pública, muito mais lenta (mas com inúmeras vantagens) é usada para transmitir apenas a chave, que é uma mensagem pequena.

É comum as pessoas divulgarem suas chaves públicas de PGP para que outras possam enviar mensagens codificadas para ela.

Texto 5 - Aspecto político da criptografia: a liberdade de expressão

Há um grande debate a respeito do direito que pessoas comuns têm de usar criptografia.

Com um programa como PGP, qualquer indivíduo pode enviar mensagens que não poderão ser lidas por curiosos, nem pela polícia e sistemas de segurança. Para muitos, incluindo Zimmermann, pessoas comuns têm direi-

to à privacidade em suas comunicações. Por isso, ele criou um programa gratuito que fornece a segurança da criptografia RSA para todos.

Evidentemente, militares e grandes empresas já tinham acesso a produtos com criptografia de chave pública. A importância do PGP foi trazer esta segurança às pessoas comuns.

A questão é que com criptografia forte, também criminosos e terroristas podem se comunicar de forma absolutamente segura, mesmo que suas mensagens sejam todas lidas em trânsito. É o que podemos chamar do "lado negro" da criptografia.

Zimmermann teve problemas com o FBI por ter divulgado seu programa na internet. O governo americano incluía software de criptografia na categoria de armas e munições, junto com mísseis e metralhadoras. Por isso, o PGP não poderia ser exportado sem a permissão do departamento de defesa.

Phil foi então acusado de tráfico de armas. Porém, em 1996, após três anos de investigação, a justiça americana arquivou o caso, uma vez que o PGP já havia se espalhado por todo o mundo. Em 1997, Zimmermann vendeu o PGP para a Network Associates, mas o programa continua disponível para **download** pela internet.

Veja no endereço eletrônico: http://www.pgpi.com

Nesta aula, vimos como a criptografia e a esteganografia têm sido usadas desde a Antiguidade. Hoje, cada vez mais a segurança da informação é de grande importância para governos, empresas e indivíduos. Assim, o uso da criptografia tornou-se quase universal, especialmente quando embutido em protocolos de comunicação na rede, como https (para navegação segura na web) e PGP (comunicação segura por email).

If privacy is outlawed, then only outlaws will have privacy.

Phil Zimmermann

Tradução:
Se a privacidade tornar-se ilegal, apenas os fora-da-lei terão acesso a ela.

Atividades

1) Um serviço secreto precisa enviar uma mensagem a um agente. A mensagem é codificada, usando uma chave que o agente conhece, e enviada por um portador. Como proteção extra, o portador leva uma mensagem falsa também codificada, caso seja interceptado, e a mensagem verdadeira oculta em uma cápsula implantada sob a pele. O exemplo pode ser identificado como criptografia ou esteganografia? Explique.

2) Qual é a relação entre segurança da informação e segurança computacional?

3) Opine sobre a questão política da criptografia: todos os cidadãos devem ter acesso a ela? Explique.

Aula 2 - Ataques a sistemas computacionais

O ataque a uma organização é, de maneira geral, qualquer ação que compromete a segurança de uma informação que esta organização possui. Isso pode ocorrer de várias formas, como o acesso não autorizado a uma rede de computadores ou a uma informação codificada (quando o atacante decifra o código), por exemplo. Há vários modos de ataques e serviços utilizados para preveni-los. Nesta aula, veremos os tipos gerais e o que cada um destes ataques objetiva.

Texto 6 - Exemplos de ataques

Se o ataque é uma ação que busca acesso não autorizado de uma organização ou indivíduo, a segurança da informação possui como metas essenciais detectar e prevenir os ataques.

> Uma defesa eficiente exige conhecimento completo dos objetivos e técnicas de ataque.

A seguir, veremos alguns exemplos de ataques e condutas que comprometem a segurança da informação. Muitos deles não são "ataques" no sentido usual do termo, mas formas de "trapaça", maneiras de subverter as regras de um sistema e a confiança de outros.

Violação de segredo ou privacidade

É o acesso não autorizado à informação. Acontece, por exemplo, se alguma pessoa ler um email, tiver acesso aos arquivos pessoais de um indivíduo etc. Pode ocorrer em uma rede de computadores quando alguém se coloca e passa a "ouvir" toda a comunicação dentro dela.

Passar-se por outra pessoa

Acontece quando alguém usa documentos de outro para fins fraudulentos.

Alguém pode, por exemplo, usar um cartão de crédito e realizar compras, ou ainda roubar um talão de cheques e usá-los, falsificando a assinatura.

Negar responsabilidade por informação originada

Acontece quando alguém origina uma informação e depois nega que o fez. Um exemplo é quando uma pessoa faz uma compra com cartão e depois liga para a administradora, dizendo que este foi roubado antes que a compra tivesse sido feita. Outro exemplo é quando uma pessoa envia um email, depois arrepende-se e alega que foi outra.

Negar recebimento de informação

Ocorre quando alguém recebe uma informação e depois nega que a recebeu. Um exemplo: quando uma pessoa age incorretamente, ela é avisada, permanece no erro, e depois nega que tenha sido alertada.

Falsear informação recebida

Uma pessoa pode receber informação de alguém, mas divulgar para terceiros outra como sendo a recebida.

Troca de informação

Acontece quando um atacante intercepta uma mensagem entre duas pessoas e consegue modificá-la sem que isto seja percebido por seu receptor.

Impedir que uma informação seja disponibilizada ou transmitida entre duas pessoas.

Há vários exemplos: muitas vezes hackers atacam de forma organizada sites na internet com o objetivo de tirá-lo do ar (talvez para desacreditar a segurança do site). Outro exemplo ocorre quando uma comunicação é interrompida em trânsito, como acontece durante as guerras, em que as correspondências das pessoas são monitoradas e qualquer informação "suspeita" é impedida de continuar. Nestes casos, o receptor pode não saber que a informação foi transmitida.

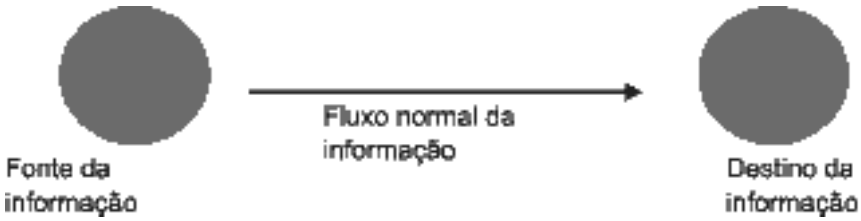
Estes são apenas alguns exemplos. Existem muitas outras formas de ataques. Como você já deve ter percebido, o tema é amplo e "onipresente" em nossas vidas.

No texto a seguir, vamos classificar os ataques em quatro categorias gerais.

Texto 7 - Categorias de ataques

Para classificar as diversas formas de ataque é necessário entender um sistema que armazena uma informação como um provedor, uma fonte desta informação. Toda informação tem seus destinatários autorizados, isto é, pessoas para as quais ela se destina.

O esquema pode ser representado pela figura a seguir.



O fluxo de informação acontece na forma de comunicação entre duas pessoas ou organizações, na transmissão de um arquivo, em uma informação divulgada em um site na internet ou no acesso de uma pessoa autorizada a um banco de dados, por exemplo.

Veremos agora as categorias gerais de ataques.

Interrupção

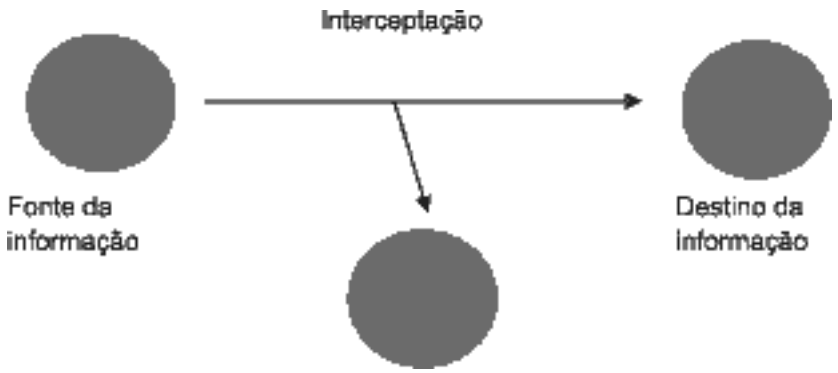
Ataque em que a informação é impedida de chegar ao destinatário, pois foi interceptada ou destruída. Este é um ataque à disponibilidade da informação.

Acontece quando, por exemplo, um servidor contendo a informação é fisicamente destruído, uma linha de comunicação (cabo de rede, linha telefônica etc.) é interrompida, um servidor de internet recebe um ataque e fica "fora do ar", entre outros.

Interceptação

É o ataque em que se consegue acesso não autorizado à informação. O atacante pode ser uma pessoa, uma organização ou um programa de computador. É uma forma de ataque muito usada para obtenção de segredos militares e industriais, pelos serviços secretos de segurança etc., em que interessa ao atacante obter a informação sem ser detectado, sem modificá-la ou interromper sua disponibilidade.

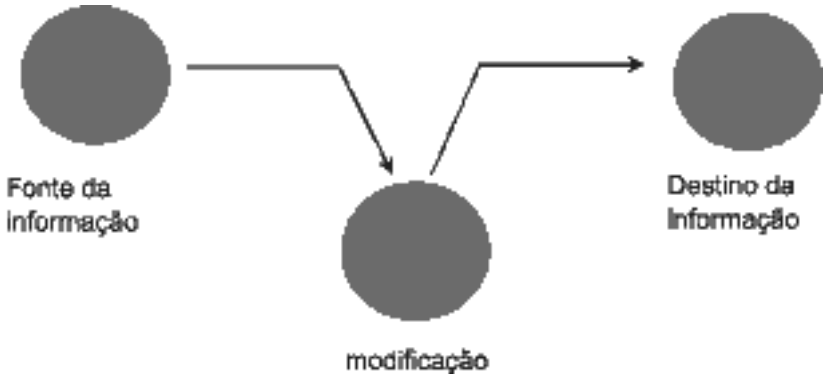
Trata-se de um ataque à confidencialidade da informação.



Um exemplo disso é a verdadeira praga moderna chamada spyware. Estes são programas que, quando colocados em um computador, passam a reunir secretamente informações sobre os hábitos dos usuários e as transmitem para outras pessoas. Normalmente são instalados sem o consentimento do usuário durante a navegação e a troca de arquivos pela internet.

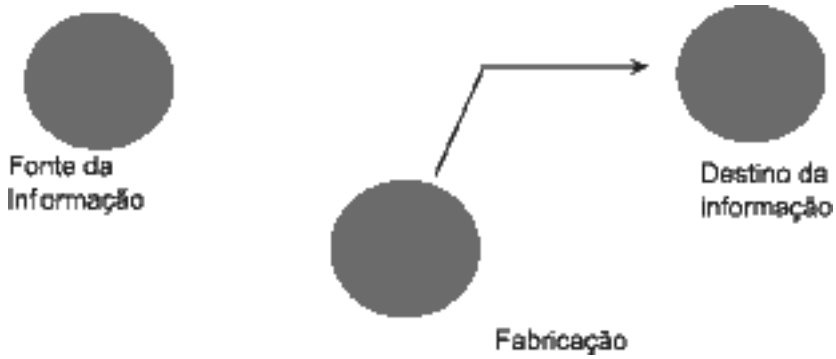
Modificação

Acontece quando uma pessoa ou organização não só ganha acesso não autorizado à informação, mas a modifica. Alguns exemplos: um hacker invade o site de um banco e modifica o saldo de sua conta bancária. Alguns vírus instalam-se nos computadores, substituindo um determinado programa ou arquivo por outro de igual nome, mas que foi alterado para realizar alguma operação fraudulenta.



Fabricação

Ataque por fabricação ocorre quando uma pessoa ou organização insere uma informação falsa no sistema. É um ataque à autenticidade da informação. Esta passa a existir e estar disponível, mas não é autêntica.



Um exemplo dessa modalidade de ataque é a adição de registro falso em um banco de dados ou de mensagens falsas em uma rede de computadores. Outra forma acontece quando, em uma guerra, um dos lados divulga

informações falsas, por canais reconhecidamente inseguros, para que estas sejam interceptadas pelo inimigo.

Texto 8 - Ataques passivos e ativos

Uma pessoa pode tentar, de várias maneiras, atacar uma rede ou um sistema de segurança de informação. Existem dois tipos principais em relação à intervenção que é feita no sistema.

Ataques passivos

O atacante pode estar simplesmente "escutando" a conversa sem ser percebido, como alguém que escuta uma conversa atrás de uma porta. Este tipo de ataque é chamado passivo. Ocorre quando alguém consegue informação através de uma escuta telefônica, consegue ler os emails de outra pessoa, mas não modifica ou impede a transmissão delas, ou seja, consegue, de alguma forma, acesso a uma informação ou comunicação, sem interferir nesta informação. O objetivo do atacante, o chamado inimigo passivo, é o de ganhar conhecimento da informação sem ser percebido. Os espiões (pessoas) e os programas spyware em nossos computadores são bons exemplos de inimigos passivos.

Uma das armas muito utilizadas por hackers são os programas "farejadores", os sniffers de rede. São programas que escutam todo o (ou parte do) tráfego de dados de uma rede, buscando informações importantes, como logins e senhas.

Os ataques passivos são, em geral, difíceis de serem detectados, uma vez que não envolvem qualquer alteração de dados. É importante que um profissional envolvido na segurança de uma rede conheça as diversas formas de ataque passivo e trabalhe com a idéia de prevenção, mais do que a de detecção.

Ataques ativos

São os ataques que envolvem algum tipo de modificação da informação, criação de informação falsa ou interrupção.

Atacantes passivos tentam ganhar conhecimento da informação. Já os atacantes ativos têm interesses diversos. Eles podem desejar modificar uma informação em trânsito, corromper informação existente, ganhar acesso não autorizado a recursos do sistema, interromper o fluxo de informação (parcial ou totalmente) etc.

Os ataques ativos podem ser divididos em três categorias:

1. Falsificação – ocorre quando uma entidade tenta passar por outra. Por exemplo, se um hacker consegue o login e a senha de alguém, pode acessar um sistema usando estas informações. Também podemos incluir nesta categoria:

•falsificação de mensagens de email;

•execução de pacotes de autenticação em uma rede.

2. Modificação da mensagem – acontece quando uma parte da mensagem é alterada. A modificação pode se dar em informação armazenada ou em trânsito.

3. Negação de serviço – é um ataque que busca impedir o uso nomal de um serviço ou meio de comunicação. O objetivo pode ser tirar um servidor do ar, por exemplo, fazendo com que a informação, neste servidor, fique indisponível.

Em geral, ataques ativos são facilmente detectados, uma vez que algo "anormal" acontece. Por isso, a segurança contra estes ataques deve enfatizar a detecção e interrupção.

Na Aula 2, estudamos as diversas formas de ataque a sistemas computacionais. Vimos exemplos de motivações para os ataques, as principais categorias (interrupção, interceptação, modificação e fabricação) e quais podem ser passivos ou ativos. Na próxima aula, estudaremos os principais serviços de segurança. Terminamos a aula com uma citação de Sun Tzu, em seu livro "A arte da guerra":

Há 2.500 anos, o general chinês Sun Tzu escreveu o livro "A arte da guerra" no qual apresenta conhecimentos sobre as estratégias de guerra. Hoje, o livro é uma referência para políticos, administradores, gerentes de marketing e demais profissionais. Também filósofo, Sun Tzu mostra a importância do planejamento e da motivação para se alcançar um objetivo, além da necessidade de trabalhar em conjunto, conhecer o ambiente de ação, o obstáculo a ser vencido e os próprios pontos fortes e fracos.

Se você conhece o inimigo e conhece a si mesmo, não precisa temer o resultado de cem batalhas. Se você se conhece mas não conhece o inimigo, para cada vitória ganha sofrerá também uma derrota. Se você não conhece nem o inimigo nem a si mesmo, perderá todas as batalhas.

Atividades

1) Quais categorias de ataque podem ser identificadas nos exemplos abaixo?

a) Um funcionário de uma empresa descobre a senha de um colega, que estava escrita em um papel grudado no monitor do computador deste. Usando a senha, lê todos os arquivos pessoais do colega.

b) O mesmo funcionário desonesto consegue agora entrar na conta de seu chefe. Nela, encontra uma lista de funcionários do setor que terão um aumento este mês. Rapidamente, ele coloca seu próprio nome da lista.

2) A diferença entre ataque passivo e ataque ativo está no fato de no primeiro, haver participação da pessoa e, no segundo, não? Explique.

Aula 3 - Serviços de segurança

Agora que vimos os principais ataques a sistemas, apresentaremos os serviços que um sistema deve oferecer para garantir a segurança da informação.

Texto 9 - Serviços oferecidos por sistemas criptográficos

Confidencialidade ou sigilo

É a proteção da informação, em trânsito ou armazenada, contra ataques passivos que pretendem conhecê-la. Há diversas formas de garantir a confidencialidade da informação: da proteção física da informação ao uso de sistemas criptográficos para torná-la ininteligível a quem não tenha autorização para conhecê-la.

Um outro aspecto interessante da confidencialidade é a proteção contra uma análise de tráfego. Neste caso, o atacante não tem acesso à informação diretamente (quando se encontra cifrada, por exemplo), mas consegue saber sua origem e seu destino, o tamanho da mensagem, a freqüência com que é transmitida, e outras informações que podem ser úteis.

Durante uma guerra, por exemplo, um dos lados pode não ser capaz de decifrar mensagens emitidas pelo inimigo. Porém, pode interceptar sucessivas mensagens, obter informações sobre quem está enviando, a posição exata de quem envia (triangulando emissões de rádio, por exemplo) e o movimento do grupo que emite as mensagens. Estas são, por si mesmas, informações utilíssimas em uma guerra.

Monitorando o tráfego de uma rede, mesmo se forem usados protocolos que usam criptografia, como o SSH, a informação da freqüência e duração dos pacotes pode fornecer alguma informação útil a um atacante.

Até a Segunda Guerra Mundial, a transmissão por código morse era muito utilizada, transmitindo mensagens codificadas. Os analistas da época

aprendiam a reconhecer a pessoa que enviava as mensagens pela duração de um ponto curto e um traço, funcionando como uma assinatura. Podia-se, então, afirmar quem havia enviado uma mensagem de rádio.

Por exemplo, conhecendo-se os operadores de rádio dos diversos navios, uma mensagem de rádio interceptada podia revelar o navio exato que a enviara e sua posição aproximada.

Autenticidade

Tem como objetivo assegurar que a comunicação seja autêntica.

Se é uma mensagem em uma só direção, isto é, de A para B, o serviço deve assegurar a B que a mensagem, de fato, veio de A.

Quando se trata de uma comunicação bidirecional, uma troca de mensagens entre A e B, o serviço deve assegurar que, tanto no início da comunicação quanto ao longo dela, as duas partes são quem dizem que são, e não um inimigo falsificando sua identidade.

O uso de login e senha para acessar uma rede de computadores ou um webmail, por exemplo, é um mecanismo básico para garantir autenticidade.

Alguns importantes mecanismos de controle de acesso que garantem uma comunicação autêntica são:

• uso de caixas eletrônicos. Neste caso, a autenticidade é garantida pelo uso de cartão e senhas.
• acesso remoto a redes. Em geral, utiliza-se login e senha. Para maior segurança, é comum restringir a origem da conexão a locais pré-determinados.
• acesso a bancos, com mecanismo de login e senha.
As formas de garantir a identidade de alguém podem ser apresentadas em três categorias:
• alguma característica física do usuário (exame de DNA, impressão digital, exame de retina etc.);
• algo que o usuário tem (um cartão de banco para acessar o terminal, por exemplo);
• algo que o usuário sabe (uma senha, por exemplo).
Pode-se usar, também, uma combinação destes métodos.

Hoje há uma grande preocupação com as assinaturas digitais. Ao acessar o site do banco, como garantir que a conexão foi com o site legítimo do

banco e não com uma cópia elaborada? Mesmo que a comunicação seja segura, pode estar sendo feita com o site errado.

Um ataque que ocorre é o envio de email induzindo o destinatário a clicar em certo link para acessar um banco. Ao fazer isso, o indivíduo acessa uma cópia do site, que captura as informações da conta da pessoa que será roubada.

As assinaturas digitais são mecanismos que usam sistemas criptográficos que asseguram a autenticidade nas comunicações, funcionando como uma assinatura.

Integridade

Este serviço garante que o conteúdo de uma mensagem não foi alterado.

A integridade pode ser comprometida de duas maneiras:

• alteração maliciosa – quando um atacante altera a mensagem armazenada ou em trânsito;

• alteração acidental – pode acontecer, por exemplo, por erros de transmissão ou corrupção de dados armazenados.

Em relação à alteração acidental, muitos protocolos de transmissão incluem códigos de detecção e/ou correção de erros, isto é, parte da mensagem destina-se a detectar se esta foi alterada (detecção de erro) e, em alguma medida, corrigir os erros.

No caso da alteração maliciosa, a maior preocupação, em geral, é detectar ataques ativos (alteração de dados) muito mais do que corrigir a modificação.

Quando um ataque é detectado, deve-se parar o ataque e depois retransmitir a mensagem.

Observe que há várias maneiras de se alterar uma mensagem: modificar uma parte, inserir texto novo, reordenar a mensagem, retransmissão de mensagem antiga etc.

Observe o seguinte exemplo:

Um certo funcionário possui acesso a certo recurso em um determinado momento. Uma mensagem dando-lhe esta permissão é enviada por seu chefe, mas foi capturada por ele. A mensagem pode estar cifrada, mas o empregado sabe do que se trata. Em outro momento, quando não tem mais a permissão, o funcionário pode retransmitir a mesma mensagem, a fim de conseguir um acesso para o qual não está mais autorizado. Este é um ataque por retransmissão de mensagem.

Sistemas criptográficos são ferramentas importantes e muito utilizadas para garantir a integridade da informação, como veremos em módulos posteriores.

Não-repúdio

Impede tanto o emissor quanto o receptor da mensagem de negá-la. Repúdio, neste contexto, é o ato de negar algo que foi dito, recebido ou feito.

Situações em que ocorre:

•um erro é cometido (um arquivo é apagado acidentalmente, por exemplo) e quem o cometeu nega o que fez.

•uma compra é feita e o comprador posteriormente nega que o fez (para escapar do pagamento), por exemplo, alegando que seu cartão de crédito foi roubado e usado indevidamente.

É importante que quando uma mensagem for enviada, o destinatário possa provar que, de fato, a mesma foi enviada pelo remetente e este possa provar que ela foi de fato, recebida pelo destinatário correto.

Na transmissão de mensagens pela internet, não-repúdio pode ser garantido pelo uso de assinaturas digitais e recibos de recebimento eletrônicos. No entanto, estes expedientes não são simples de serem implementados de forma segura. Mecanismos de criptografia podem ser usados para atender a estas necessidades.

Controle de acesso

É a habilidade de restringir o acesso aos sistemas informatizados, especialmente o acesso remoto. Este serviço está relacionado, de maneira mui-

to próxima, à autenticidade, uma vez que os mecanismos utilizados para restringir o acesso, com senhas, garantem também a identidade de quem emite a mensagem.

Por exemplo, ao receber o email de alguém, vindo de um sistema de email que envolve login e senha para acesso, teoricamente apenas esta pessoa poderia ter enviado a mensagem.

Este é apenas um exemplo simples. Na verdade, há maneiras de falsear o cabeçalho de um email alterando a informação de quem o enviou, por exemplo.

Disponibilidade

Algumas vezes o ataque é feito à disponibilidade da informação. Em uma guerra é comum atacar os centros de comunicação e torres de transmissão. Hackers juntam-se para atacar um servidor de web de forma a tirá-lo do ar, não necessariamente comprometendo qualquer informação. Vários ataques podem resultar na perda ou redução da disponibilidade da informação.

Há vários serviços que devem ser garantidos por sistemas de segurança. Garanti-los é um dos grandes objetivos dos profissionais e pesquisadores de área, e a criptografia tem um papel muito importante nesta área.

Na terceira aula, foram descritos os serviços que devem ser garantidos para reter a segurança na transmissão da informação: confidencialidade (ou sigilo), autenticação, integridade, não-repudiação, controle de acesso e disponibilidade. Ao longo do curso serão apresentadas as técnicas usadas para garanti-los.

Atividade 1

1) Qual é a necessidade de usar ou desenvolver os serviços descritos nesta aula?

Aula 4 - Modelo de segurança em rede

Nesta etapa, apresentaremos um modelo de um sistema de comunicação segura que reúne as características abordadas até agora. O modelo apresentado é apenas um esquema. Ainda não serão discutidos detalhes como implementações e protocolos. O exemplo apresentado pode ser realizado de diversas formas.

Texto 10 - Segurança

Segurança é um termo amplo, mesmo quando nos restringimos aos significados de segurança da informação, segurança em rede e segurança computacional.

O que é um sistema seguro?

Um computador desligado é um sistema absolutamente seguro, mas também inútil.

Segurança significa que um sistema cumpre uma função adequadamente e oferece todos os requisitos apresentados nesta aula. Há várias definições precisas. No entanto, perceba que segurança denota uma ação ativa. Um sistema deve não só ser seguro, mas manter-se seguro contra contínuos ataques.

Na "guerra" entre os que atacam e os que defendem, a situação é assimétrica: quem defende deve fazê-lo contra todos os ataques possíveis, enquanto que, para um atacante, basta encontrar uma única vulnerabilidade para invadir um sistema.

Segurança também não pode ser demonstrada. Podemos provar que um sistema foi invadido (caso tenha sido), mas não podemos provar que não foi.

Outra questão muito comum é a diferença entre a sensação de segurança e a segurança real. A maioria das pessoas sente-se muito menos segura

em uma viagem de avião do que em uma de carro. No entanto, estatisticamente, a viagem de carro é muito mais perigosa.

Uma definição razoável de segurança seria a de que um sistema seguro é aquele que faz:

• tudo o que foi projetado para fazer;

• nada que não tenha sido determinado para fazer, mesmo que alguém tente forçá-lo a se comportar de maneira diferente.

Isto se aplica a uma rede de computadores, um software, um esquema físico de proteção de uma informação, enfim, a uma variedade de sistemas.

Sendo assim, segurança de sistemas de informação é um meio termo entre segurança e funcionalidade. Para que funcionem, devemos correr riscos que não podem ser anulados. Como disse Bruce Schneier, em seu livro "Secrets and Lies" (2000), segurança da informação é, no fundo, um gerenciamento de risco.

Modelo de Segurança

O modelo consiste em uma mensagem que é transmitida entre duas partes através de algum canal de comunicação, que pode ser, por exemplo, a internet ou outra ligação por meio eletrônico.

As duas partes que se comunicam serão chamadas de principais na transação. Só é possível conseguir um canal seguro se as duas partes concordam com a adoção de mecanismos de segurança.

Veja a figura a seguir:

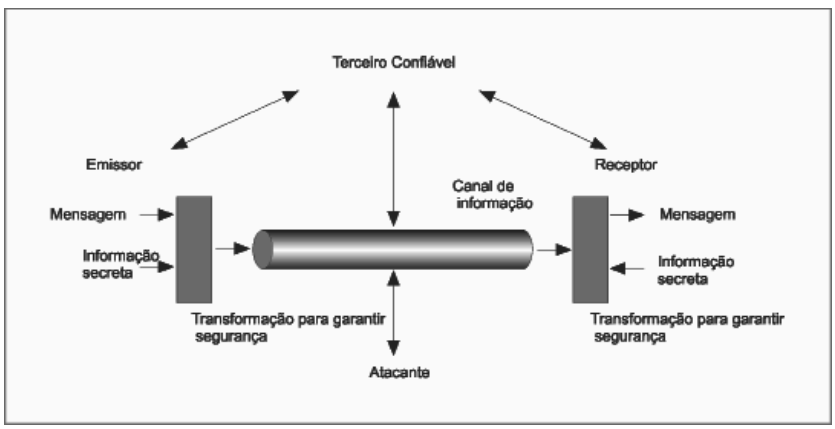


Figura 1. Modelo para Segurança de Rede

(*Fonte:* STALLINGS, 1999)

Normalmente, a informação trafega pelo canal de comunicação usando algum protocolo de transporte. Por exemplo, na comunicação pela internet, a informação é quebrada em pacotes, que passam por vários nós no caminho até o destino. Os pacotes são reunidos novamente, na ordem correta, no destino final.

Estes pacotes podem seguir caminhos distintos até o final. Portanto, o canal de comunicação deve ser entendido como um canal lógico e não como um caminho físico.

Além dos dois elementos principais da comunicação, duas outras figuras podem estar presentes:

• o oponente – este é o inimigo, aquele que ataca o sistema de maneira ativa ou passiva com o objetivo de conhecer a informação (ataque à confidencialidade), interromper seu fluxo (ataque à disponibilidade), modificar seu conteúdo (ataque à integridade) ou fabricar uma mensagem (ataque à autenticidade).

• um terceiro confiável – pessoa ou organização na qual duas partes principais confiam e que pode atuar no sistema como um árbitro, distribuidor de chaves secretas, avaliador de que o sistema é seguro etc.

Há dois elementos normalmente utilizados em comunicações:

1. Um sistema criptográfico que transforma a mensagem antes de seu envio.

A mensagem trafega cifrada, ininteligível para o oponente, caso consiga interceptá-la.

O próprio sistema criptográfico pode ser usado para assegurar a identidade do remetente da mensagem e do receptor e garantir que a mensagem não foi alterada em trânsito, isto é, o sistema criptográfico pode garantir os serviços de confidencialidade, autenticidade, integridade e não-repudiação.

2. A transmissão de uma informação (uma chave) secreta.

Esta deve ser identificada pelas duas partes que se comunicam e seu conhecimento capacitaria o oponente a decifrar a mensagem. Esta informação é, normalmente, uma chave secreta, usada por um sistema criptográfico para cifrar uma mensagem.

Posteriormente, veremos que sistemas criptográficos de chave pública não requerem a transmissão de uma chave secreta.

No caso de sistemas de chave secreta, o terceiro confiável pode ser usado para distribuir a chave entre os principais. No caso de sistemas de chave pública, o terceiro confiável pode assegurar a autenticidade das chaves.

Assim, o planejamento de um sistema seguro como este envolve um sistema criptográfico que codifica a mensagem antes de sua transmissão; informação secreta (uma chave) que deve ser trocada entre os principais, um esquema de distribuição destas chaves que pode usar um terceiro confiável. Tudo isso é reunido em protocolo, um conjunto de regras que garantem o processo.

Tipos de Ameaças

Há basicamente dois tipos de ameaças contra as quais um sistema de informação deve estar protegido:

- ameaça de acesso à informação – é a ameaça direta de interceptação ou modificação da mensagem por pessoas que não deveriam ter acesso a ela.
- ameaças por exploração de serviço – trata-se de usar falhas de segurança em serviços comuns disponibilizados por sistemas informatizados.

Programas modernos são grandes e complexos e, muitas vezes, têm comportamento inesperado em situações não previstas por seus autores.

Hackers descobrem "falhas de segurança", situações que levam o programa a um comportamento indesejado, abrindo uma brecha na segurança do sistema.

Os mecanismos de segurança são divididos em duas categorias:

- Funções de "porteiro" são mecanismos destinados a controlar o acesso ao sistema, impedindo a entrada de visitantes indesejados. Fazem parte desta categoria os sistemas de senha e login, e os sistemas de proteção contra vírus e worms, que examinam automaticamente arquivos acessados na internet e disquetes, detectando e limpando pragas diversas.

Sistemas tipo firewall são exemplos importantes, pois impedem a entrada de agentes não autorizados.

- A segunda linha de defesa são os mecanismos de controle interno, programas que monitoram a atividade de uma rede, buscando detectar a presença de intrusos.

Estas duas categorias estão representadas na figura a seguir:

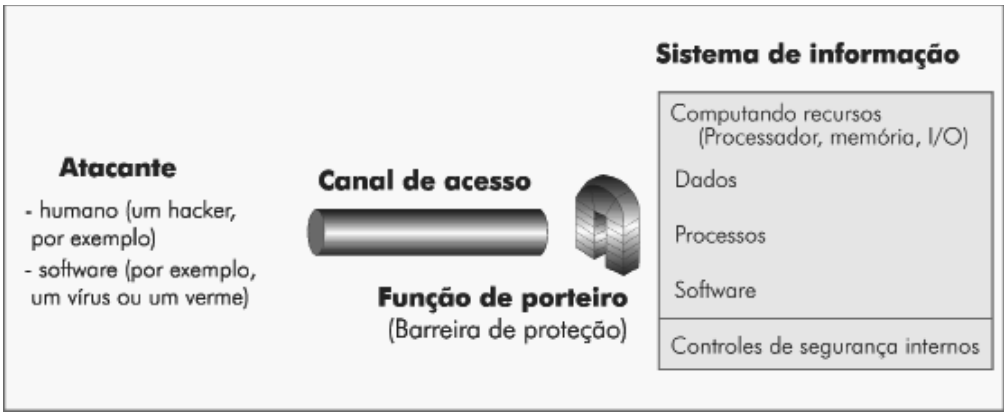


Figura 2. Modelo de segurança de acesso a rede

Nesta aula, discutimos o conceito de segurança, abordando diversos aspectos. Vimos um exemplo, descrevendo seus elementos principais, e delineamos as principais categorias de ameaças e mecanismos de defesa a sistemas de segurança.

A partir da próxima unidade e pelos próximos dois módulos deste curso, estudaremos mais especificamente a criptografia, sua história, principais mecanismos atuais e a base matemática necessária para o entendimento das técnicas mais usadas, especialmente os modernos sistemas de criptografia de chave pública.

> A garantia de nos tornarmos invencíveis está em nossas próprias mãos. Tornar o inimigo vulnerável só depende dele próprio.
>
> Sun Tzu

Atividades

1) Em uma troca de emails, sem proteção adicional, quais requisitos de segurança não são atendidos? Explique.

2) Na situação de compra via internet, com o uso do cartão de crédito, que partes do modelo de segurança proposto estão presentes?

Unidade 2

História da Criptografia

Da Antiguidade aos tempos atuais, vários acontecimentos marcaram a história da Criptografia. Na unidade 2, veremos as primeiras soluções que a humanidade criou para transmitir as mensagens secretas. Nesta segunda etapa da disciplina, apresentaremos os eventos históricos e as mudanças ocorridas com o advento dos computadores e da internet. Bom estudo!

História da Criptografia

Aula 5 - Criptografia na Antiguidade

Nesta aula, vamos tratar das primeiras e antigas soluções técnicas da criptografia, desvendando as primeiras raízes desta importante área do conhecimento.

Há mais de cem mil anos, o Homo sapiens ingressou na espiral da vida. A necessidade de viver em bandos para vencer as condições hostis do meio ambiente levou o ser humano primitivo a desenvolver uma sofisticada linguagem falada. Ao mesmo tempo, gradualmente, ele foi criando símbolos para retratar situações de seu cotidiano (as imagens pictográficas em pinturas nas paredes de cavernas).

Esta lenta evolução nas linguagens de comunicação possibilita o surgimento da escrita. É um salto extraordinário! Enquanto a linguagem falada necessita da presença física das pessoas, a escrita possibilita a comunicação remota entre dois ou mais interlocutores, através de mensagens.

Com a escrita, surge a necessidade de transmissão de mensagens confidenciais, compreendidas apenas pelo emissor e pelo receptor. Aparece também o desejo de interceptar mensagens e de decifrá-las. Motivos não faltaram: segredos militares, políticos, religiosos, questões de comércio ou motivos sentimentais.

Assim, foram lançadas as bases para o desenvolvimento da criptografia e da criptoanálise. A criptografia, como a área do conhecimento encarregada de produzir técnicas que permitam a transmissão secreta de mensagens, e a criptoanálise, cuidando da elaboração de técnicas para decifrar mensagens criptografadas.

Seja em busca de poder, vingança ou mera curiosidade, a batalha vem sendo travada desde tempos imemoriais entre aqueles que querem guardar segredos e os que querem desvendar. E um mesmo agente pode atuar em ambos os fronts da batalha.

Como foi mencionado na aula 2, criptografia tem sua origem etimológica nas raízes gregas kryptos, que significa secreto, e em graphos, que significa escrita. Portanto, criptografia é a área do conhecimento que desenvolve métodos para codificar mensagens (escrever secretamente).

Por outro lado, criptoanálise possui suas raízes em krypto mais a palavra análysis (decomposição). Portanto, é a área do conhecimento que trata do ato de decifrar ou "quebrar" o sistema criptográfico.

Na Antiguidade foram desenvolvidos dois métodos de ocultar mensagens de um possível interceptador ou espião. O primeiro consistia em esconder a mensagem propriamente dita. Nesta situação, ela não pode ser interceptada, sob pena de imediatamente ser decifrada.

O segundo método usou processos elaborados em que a mensagem mesmo tornada pública, não seria entendida pelo interceptador, uma vez que a chave era desconhecida para a leitura. Assim, vamos nesta aula 5 tratar das primeiras soluções que a humanidade criou para resolver o problema da transmissão de mensagens secretas.

Texto 11 - O início da criptografia

Traços de criptografia apareceram, por volta de 2000 a.C, no Egito e na Mesopotâmia. Os sacerdotes egípcios usaram expedientes criptográficos, ao utilizar a escrita hierática (hieroglífica), incompreensível para o resto do povo que usava língua demótica. O mesmo fenômeno é encontrado nos Babilônicos com a escrita cuneiforme.

Um modelo rústico e precursor da criptografia é a técnica de transmissão secreta de mensagens, conhecida como esteganografia: consiste em ocultar a mensagem, sem mudanças em seu estado original. A vulnerabilidade do método é muito grande, uma vez que interceptada é imediatamente decifrada. Na aula 1, relatamos alguns exemplos de esteganografia, como mensagens inscritas em cabeças raspadas e o uso de microponto na Segunda Guerra Mundial.

Se você julgar oportuno, volte ao texto 1 da aula 1 para uma revisão.

Hierática
Forma cursiva de escrita, usada pelos sacerdotes em textos sagrados. Gravada em papiro, madeira ou couro.

Demótica
Escrita cursiva, simples, usada em cartas, em registros e documentos, comum no dia-a-dia. Era gravada normalmente no papiro.

Cuneiforme
Criada pelos sumérios (povo estabelecido na Babilônia no século IV a.C.) era simultaneamente ideográfica e fonética. Cada signo correspondia a um objeto e, posteriormente, passou a representar o som respectivo deste objeto.

A esteganografia é uma técnica que permite esconder a mensagem sem transformá-la. Logo, esteganografia não é criptografia. Antes de tudo, para caracterizar criptografia, é necessário que a mensagem sofra uma transformação antes de seu envio. Esta fase de alteração é chamada "encriptar a mensagem" ou "cifrar a mensagem".

Para encriptar a mensagem, resolvida a escolha do algoritmo, é preciso selecionar uma boa chave. No caso que será apresentado na aula 5, a chave que realiza esse processo é a mesma que "decripta ou decifra a mensagem". Apenas o emissário e o destinatário podem ter acesso ao algoritmo e à chave.

Para que o interceptador tenha sucesso não basta apenas acessar a mensagem, é preciso descobrir o algoritmo e a chave.

Primeiros exemplos

Desde o surgimento, a criptografia se divide em duas técnicas fundamentais: a transposição e a substituição. Você verá o uso destas técnicas através de dois momentos relevantes da história da criptografia na Antiguidade.

Um primeiro momento, no período grego, época de freqüentes guerras entre Esparta e Atenas (século IV a.C.), e outro durante o Império Romano, com o imperador Júlio César (100 - 44 a.C.).

Método da Transposição – O Scytale

A cidade-estado grega de Esparta, por volta do século V a.C., era uma sociedade na qual a democracia não era uma prática. A retórica e a cultura, tão bem cultuadas na vizinha cidade-estado de Atenas, passavam longe das preocupações de Esparta. Dominados por uma rígida cultura da guerra, os espartanos tinham grande preocupação com a segurança das comunicações militares. Isto impulsionou várias formas de codificar mensagens, sendo o "Scytale espartano" ou "Bastão de Licurgo" o exemplo mais notável desta época. Veja a Figura 1:

Figura 1. Scytale espartano

(*Fonte*: http://www.numaboa.com.br/criptologia/cifras/transposicao/scytale.php)

A técnica do Scytale foi descrita por Plutarco, ensaísta e biógrafo grego, em 90 d.C., no livro "Vidas de Homens Ilustres". Era um bastão de madeira ao redor do qual se enrolava-se firmemente, em forma de espiral, uma tira, de couro ou papiro, longa e estreita.

O remetente escrevia a mensagem de modo vertical, em colunas, ao longo do bastão e depois desenrolava a tira, que se convertia em uma sequência de letras sem sentido. O mensageiro usava a tira como cinto, com as letras voltadas para dentro. O destinatário, ao receber o "cinto", enrolava-o em seu bastão, cujo diâmetro e comprimento eram iguais ao do bastão do remetente. Desta forma, podia ler a mensagem.

Artifícios de trocar (transpor) as letras de posição no ato de encriptar as mensagens, como o exemplo ilustrado pelo Scytale, deram o nome de "Transposição" ao método criptográfico.

Método da Substituição – O código de César

Suetônio, escritor romano que viveu no início da era cristã (69 d.C.), em seu livro "Vida dos Césares", escreveu a biografia dos imperadores romanos de Júlio César a Domiciano. Na publicação, o autor conta que Júlio César (100 – 44 a.C.) usava na sua correspondência militar uma chave de substituição muito simples, na qual cada letra da mensagem original era substituída pela letra que a seguia em três posições no alfabeto. A letra A era substituída pela D, a B pela E, e assim sucessivamente.

Figura 2. Júlio César

Veja o exemplo na Figura 3.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	J	V	X	Y	Z
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	X	Y	Z	A	B	C

Figura 3. A chave do método de Júlio César

Olhe, em detalhes, o método criptográfico de Substituição que Júlio César usava para enviar mensagens a seus generais.

Na Figura 3, na primeira linha estão representadas as letras em ordem alfabética. Na segunda linha, a seqüência alfabética começa com a letra D, a terceira letra depois da letra A. Esta é a chave. Em seguida, acrescentam-se as outras letras, terminando a segunda linha com as letras que foram esquecidas.

Outro exemplo é a mensagem "encontro confirmado sexta feira", encriptada com a chave de Júlio César, que ficaria assim:

"HQFRQXURFRQIUPDGRVHAXDIHLUD".

Em homenagem ao imperador romano, chamamos de código de César qualquer cifra em que cada letra da mensagem original seja substituída por outra deslocada em um número fixo de posições, não necessariamente três.

Como o alfabeto português possui 25 letras, são possíveis 24 códigos distintos de César. O número de casas deslocadas é a chave do código e a chave original de César tem o número 3.

Atividade 1

Decifre a mensagem a seguir, sabendo que ela está cifrada com o código de César, cuja chave é o deslocamento de dez posições.

"Z O H A G O X M G D S F S L K A K Z A B K E E K N A"

Vulnerabilidade dos códigos de César

A chave de um código de César fica totalmente determinada por um número entre 1 e 24. Este número corresponde ao deslizamento das letras do alfabeto.

Por exemplo, o número 3 define o código original de César. É evidente que uma chave baseada em apenas um número é muito vulnerável. Neste caso, um "ataque de força bruta" certamente será eficiente para quebrá-la. É preciso apenas tempo para testar 24 possibilidades e decifrar a mensagem. Na época de César, tempo era um elemento que não faltava.

Um código de César é um método onde uma chave, definida por um número, é usada para cifrar e para decifrar a mensagem. As duas partes, o emissário e o destinatário, conhecem a chave. Este sistema de comunicação coloca toda a segurança do processo sobre a chave e nenhuma sobre o algoritmo. Métodos criptográficos desta natureza são conhecidos como de chave simétrica. A chave é a mesma tanto para o emissário quanto para o destinatário.

O código de César é do tipo monoalfabético, uma vez que a chave que encripta a mensagem faz cada letra do alfabeto corresponder a, e apenas uma, letra na mensagem cifrada.

Os códigos de César se revelaram úteis em um período em que poucas pessoas sabiam ler. Uma época em que ainda não havia começado a criptoanálise. Os métodos de decifragem eram exclusivamente na base da força bruta. Na próxima aula, você verá como é possível sofisticar um código de César de modo a livrá-lo, ao menos, do ataque de força bruta.

Ainda na aula 6, serão abordados o nascimento da criptoanálise e o efetivo começo da perene e dramática luta entre criptógrafos, de um lado, na sofisticação de códigos e chaves e, de outro lado, criptoanalistas desenvolvendo, sistematicamente, métodos para quebrá-los. Esta luta será o ponto central nos estudos e discussões seguintes.

Aula 6 - Criptografia na Idade Média

A Idade Média inicia em 476, com a queda do Império Romano, e termina em 1453, com a queda de Constantinopla. Foi uma época caracterizada por relativa recessão no domínio das idéias. A criptografia não escapou desta "recessão". Grande parte do conhecimento sobre o assunto foi perdido, pois era considerado magia negra ou bruxaria. Este período, principalmente o da primeira metade da Idade Média, foi motivado por perseguições religiosas.

Nessa época, era muito perigosa a correspondência através de mensagens misteriosas e indecifráveis. A escrita secreta era interpretada como um hábito estranho, que teria ligação com forças do mal e, certamente, era usada nos tribunais civis e religiosos como peças de incriminação em processos de toda a natureza.

Os escassos sinais históricos do uso da criptografia, no início da Idade Média, referem-se a hábitos de monges utilizando-a em escritas, como forma de passatempo e diversão ou, ainda, em sociedades religiosas.

Texto 12 - Cifras monoalfabéticas

Todos os sistemas de códigos utilizados durante a Idade Média eram construídos basicamente através de cifragens monoalfabéticas.

Uma cifra monoalfabética é construída ao fazer corresponder cada letra distinta do alfabeto exatamente a um símbolo distinto.

O símbolo que representa uma letra na cifra monoalfabética pode ser definido por uma letra ou através de qualquer representação gráfica.

Na figura 4, você encontra duas possibilidades distintas de cifragem monoalfabética. Na primeira linha, aparecem as letras na seqüência alfabética e, nas duas linhas seguintes, duas cifras distintas. A primeira cifra (cifra 1) simplesmente permutou as letras do alfabeto. A segunda cifra (cifra 2) mistura símbolos e letras.

Note que, nesse tipo de cifragem, cada letra do alfabeto corresponde exatamente a um símbolo na cifra e cada símbolo da cifra corresponde a uma letra do alfabeto. Esta correspondência biunívoca é a característica fundamental da cifragem monoalfabética.

	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	x	y	z
Cifra 1	B	N	O	F	D	J	Z	R	S	C	T	L	H	A	M	G	E	Q	U	X	Y	V	K	P	U
Cifra 2	O	N	M	R	S	V	Q	Z	T	L	+	&	#	I	J	G	*	@	K	P	>	:	~	A	B

Figura 4. Duas possibilidades de cifras monoalfabéticas

Exemplo: a palavra amizade seria criptografada nas cifras 1 e 2 , respectivamente, como:

BHSUBFD ou O#T B O R S

De modo geral, o uso de código para a transmissão de mensagens secretas impõe que tanto o remetente quanto o destinatário gravem a chave que gera o código em algum meio (por exemplo escrevendo em um papel) e esconda a anotação em local seguro. Porém esta solução é perigosa, uma vez que pode cair na mão do inimigo. O ideal seria a memorização da cifra.

Observe que é muito fácil definir cifras monoalfabéticas genéricas como indicado na Figura 4. No entanto, é complicado memorizar qualquer destas cifras, se elas não possuem uma lei de composição.

Esta dificuldade não ocorre com as cifras monoalfabéticas de César, que estudamos na Aula 5. Elas correspondem a uma permutação do alfabeto, definida por uma translação das letras. Portanto, cada uma dessas cifras corresponde a um número entre 1 e 24. Este número define a cifra. E sendo apenas um número, pode ser guardado na memória.

Veja as qualidades que devem ser buscadas na definição de uma boa cifra monoalfabética:

• a cifra deve ser suficientemente complexa para dificultar sua interpretação;

• a cifra deve ser construída por um meio que permita guardar a chave de sua construção na memória.

Na próxima disciplina, "Criptografia Geral", vamos aprofundar um pouco mais o tema sobre cifragem monoalfabética. Na ocasião, mostraremos alguns tipos de cifras monoalfabéticas que satisfazem as duas qualidades acima.

Atividade 2

Construa um código de César com a palavra chave FRATERNIDADE e criptografe a mensagem: "o sol nasce para todos".

Texto 13 - Rudimentos da criptoanálise

Durante a Idade Antiga e a Idade Média, a construção de códigos era baseada em cifras monoalfabéticas. As mais populares, em virtude da fácil utilização e memorização, foram aquelas baseadas em Códigos de César, obtidos por deslizamento de letras. Este tipo de código pode ser quebrado por um método considerado como a pré-história da criptoanálise: "o método da força bruta". Vamos ver como este método primitivo da criptoanálise se aplica na quebra de códigos.

Primeiramente, o "método da força bruta" corresponde à análise de uma a uma de todas as possibilidades de chaves para quebrar o código. Uma vez com a mensagem cifrada em mãos, é feito o teste exaustivo de todas as chaves. Este método é eficiente para quebrar o Código de César.

A chave é exatamente um número entre 1 e 24 que define seu comprimento. Assim, a partir de um trecho de mensagem interceptada, a qual se supõe estar criptografada por um código de César, basta, com paciência, testar qual das 24 possibilidades decodificam o trecho da mensagem. Após definir o número que é a chave do código, toda a mensagem se revela. Como se vê, um código ingênuo deste tipo não resiste ao "método da força bruta".

Outro método importante de criptoanálise referente ao período da pré-história é o "método da palavra provável". Este método é universal e pode ser utilizado em qualquer situação na qual se tente decifrar uma mensagem. Por exemplo, considere um comunicado interceptado durante uma guerra moderna. Provavelmente, neste comunicado estarão presentes palavras como tanque, avião ou inimigo. Então tenta-se invocar qual das palavras cifradas podem corresponder à "palavra provável". Este procedimento, com sucesso, consegue decifrar algumas letras, um passo valioso para a decifragem total.

No entanto, o "método da palavra provável" teve sua origem, não propriamente na criptografia, mas na busca de revelar mensagens antigas, escritas em alfabetos desconhecidos. Embora, como foi apontado, não se trate da decifragem de um código, uma vez que os povos antigos não tinham intenção de esconder as mensagens. Do ponto de vista de quem trabalha com a decifragem de textos, é um problema equivalente. É preciso evocar a palavra certa para abrir a caverna de Ali Babá.

No século VII, al-Khalil descreve em seu livro "Kitab al Mu'amma" (o livro das mensagens criptográficas) como decifrou antigos criptogramas bizantinos. Sua solução baseou-se na suposição de que o título do criptograma seria "Em nome de Deus". Este título era comum na época em que o criptograma foi escrito e correspondeu à invocação de al-Kahlil.

Na Idade Antiga e na primeira metade da Idade Média (até o ano 800), dominavam as cifragens monoalfabéticas, das quais as mais simples são as de tipo código de César. Na mesma época eram praticados dois métodos de decifragem: o método da força bruta e o método da palavra provável. Estes métodos correspondem a ensaios rudimentares de criptoanálise.

Texto 14 - Criptoanálise: a contribuição árabe

Os primeiros sinais de ressurgimento da criptografia ocorrem com a Idade de Ouro da civilização árabe, que tem início por volta do ano 750. Pouco interessados em promover guerras de conquistas, os Califas Árabes favorecem o desenvolvimento das ciências, do comércio e da indústria, e desenvolvem uma administração eficaz, utilizando a criptografia na segurança de suas comunicações.

O nascimento da criptoanálise ocorre nesta época com a descoberta do "método da análise de freqüências". Não se sabe ao certo quem, pela primeira vez, propôs o método. O primeiro registro aparece no livro "Escritos sobre a decifração de mensagens criptográficas", do sábio árabe al-Kindy.

A "análise de freqüências" explora uma fraqueza fundamental nas mensagens codificadas através de cifras monoalfabéticas: as diferentes frequências com que aparecem os vários símbolos. Veja como funciona o método.

Em um texto longo, a freqüência de aparecimento das letras é distinta para cada letra. Na língua portuguesa, a letra que mais aparece é a letra a, a segunda é a letra e, em seguida a letra o, o r etc. A aplicação da "análise de freqüências" em um texto que se supõe criptograda por um código monoalfabético parte do princípio que o símbolo que aparece repetidamente na mensagem criptografada corresponderia à letra a, em seguida, o outro símbolo mais freqüente seria a letra e, e asssim sucessivamente. A partir deste estágio, é preciso fazer ajustes, pois algumas letras têm freqüência muito próximas. Uma dose de paciência e intuição são suficientes para completar a decifragem.

O "método da análise de freqüências" fundou a Criptoanálise em bases científicas e instalou definitivamente a eterna luta entre os criadores e decifradores de códigos.

A reação européia

A Itália foi um dos primeiros países a ver com profissionalismo e como questão de estado o uso da criptografia. Este momento da história italiana, por volta de 1300, coincidiu com as primeiras manifestações do Renascimento.

O governo italiano cria um órgão ligado diretamente ao centro do poder, dedicado exclusivamente ao estudo da criptografia, com o objetivo de decifrar as mensagens dos inimigos e aperfeiçoar os métodos de encriptação.

Era uma época em que a Europa estava perto de uma revolução no campo das idéias, que influenciou definitivamente o desenvolvimento posterior das ciências, das artes, da política e a visão estabelecida do mundo. Este movimento que abalou o sono da Idade Média foi cunhado com o nome de Renascimento, ocorrendo primeiro na Itália e depois conquistando o resto do mundo.

Durante toda a Idade Média, a Europa usou velhas técnicas criptográficas, embora os árabes tenham demonstrado a fragilidade destes métodos diante da análise de freqüências. O feito árabe marca o início efetivo da criptoanálise e coloca os decodificadores na frente dos codificadores.

A reação da criptografia, com a criação de novos métodos, para escapar à análise de freqüências, só ocorreria na aurora da Idade Moderna, coincidindo com o início do Renascimento. Este tempo é também marcado pelo nascimento da Imprensa e a conseqüente mecanização da escrita. Esta nova ferramenta irá influenciar fortemente o desenvolvimento posterior da criptografia, como veremos na próxima aula.

Aula 7 - Criptografia na Idade Moderna

Como você viu na aula 6, entre os anos 800 e 1200, os árabes desenvolveram um poderoso método de decifragem de códigos que foi a análise de freqüências. Apesar disso, durante toda a Idade Média, a Europa continuava firmemente presa aos códigos monoalfabéticos, ignorando a poderosa ferramenta.

A Idade Moderna é marcada pelo início do movimento renascentista na Itália, em 1450, e vai até o fim do século XIX. O renascimento abre uma era de grande desenvolvimento das ciências e das artes, causando impacto na economia e na política.

A grande novidade na criptografia ocorre em 1580, com a invenção de uma cifra aparentemente imune à análise de freqüências. Denominada cifra de Vigenère, ela fez seu reinado por quase três séculos, até 1850, quando foi quebrada por Babbage. No entanto, apesar de dispor de uma cifra poderosa como a de Vigenère, a Europa não a utilizou intensivamente. Devida a sua complexidade e a fraca mecanização da escrita, foram escolhidas alternativas como as cifras homofônicas (sobre as quais falaremos adiante) e outras soluções mistas, que acrescentaram relativa segurança às cifras monoalfabéticas.

A cifra de Vigenère seria usada com regularidade apenas 200 anos mais tarde. Esta situação determinou que as comunicações secretas na Europa, até por volta de 1750, continuassem sensíveis aos ataques da análise de freqüências, provocando grande estado de confusão, com emocionantes relatos.

Texto 15 - Início da Era Moderna

No ano de 1450, a Itália figura como palco ideal para o desenvolvimento da criptografia. Colocada no epicentro do movimento que criou a Renascença, a Itália era constituída de cidades-estados independentes, cada uma buscando sua hegemonia.

Grande parte da correspondência que tratava de política externa, economia e assuntos militares das cidades-estados era altamente sensível e necessitava de proteção.

Conscientes da fragilidade dos códigos monoalfabéticos, frente à análise de freqüências, os criptógrafos começaram a desenvolver cifras de substituição homofônicas, onde cada vogal do alfabeto era representada por vários símbolos distintos. Foi usada também a combinação de substituição homofônica com transposição de letras.

O novo tempo pedia a formação de uma estrutura organizada para tratar da proteção e interpretação da comunicação. A primeira resposta foi dada por Veneza, em 1452, criando uma secretaria dentro do governo, com o objetivo de lidar com a escrita secreta, solucionando e criando cifras. Esta secretaria foi chamada de "câmara negra".

O primeiro grande nome da criptoanálise da Europa foi Giovanni Soros, que assumiu seu posto em Veneza no ano de 1506. Sua capacidade em decifrar mensagens marcou o período. Nações aliadas de toda a Europa traziam mensagens para serem decifradas por Soros. O tratamento de Estado dado à criptografia em Veneza se espalhou, pouco a pouco, por toda a Europa.

Em Viena, a partir do ano de 1750, prosperou a mais organizada e eficiente "câmara negra" da Europa, liderada pelo Barão Ignaz von Koch. Toda correspondência nacional ou internacional que chegava ou saía de Viena passava antes pela câmara. As cartas eram violadas e entregues a um batalhão de copistas. Em seguida, o selo era reconstituído e a carta, enviada ao destinatário. A mensagem copiada era entregue a outra equipe de criptoanalistas. Viena se tornou tão eficiente neste setor que vendeu serviço às nações aliadas da Europa.

Na França, o primeiro nome ilustre foi Babou, nomeado decifrador de François I. Depois surge o matemático Viète, como o criptologista de Henri IV. Um dos feitos notáveis de Viète foi decifrar as mensagens criptografadas da corte de Filipe II da Espanha. Conhecedor do fato, o Rei queixou-se ao Vaticano, pedindo que Viète fosse julgado por um tribunal de cardeais, sob acusação de possuir ligações com o demônio. O Papa Clemente II, ciente da força dos métodos de Viète, ignorou o pleito.

No entanto, finalizando um ciclo, o mais renomado entre os franceses foi Antoine Rossignol (1600-1682), que se tornou célebre por seus trabalhos para Richelieu. Rossignol criou a Grande Cifra que só foi quebrada em 1890.

Esses fatos marcaram a Idade Moderna na Europa nos séculos XV, XVI e XVII, antes do uso mais intensivo da cifra de Vigenère. De um lado, os criptógrafos continuavam dependentes, basicamente, de cifras monoalfabéticas. Por outro lado, criptoanalistas como Babou, Soro, Viète e Rossignol destruíam as mensagens com a análise de freqüências.

Uma das situações mais trágicas da época ocorre com a quebra de um código monoalfabético que provocou a condenação da Rainha Maria da Escócia pela rainha Elisabeth I da Inglaterra. Maria era prisioneira de Elizabeth e, de seu cárcere, trocava correspondência cifrada com um grupo de católicos que tramavam a morte da rainha e a libertação de Maria para assumir o trono inglês. A correspondência de Maria foi interceptada e decifrada por Thomas Phelipes, secretário de cifras do Reino. Maria foi decapitada em 1538.

Texto 16 - A fuga desesperada da análise de freqüências

Após a tomada de consciência européia da fragilidade dos códigos monoalfabéticos, frente ao poder da análise de freqüências, ocorreu um verdadeiro vale-tudo. A primeira reação, embora insuficiente, foi de Crema, em 1452, com os "códigos de substituição homofônica".

Uma cifra homofônica é construída fazendo corresponder cada letra do alfabeto a um conjunto de símbolos diferentes (que podem ser, inclusive, as próprias letras permutadas). A quantidade de símbolos associados a cada letra corresponde ao nível de freqüência estatística com que esta letra aparece em textos longos.

> Exemplo: no caso de um texto longo em português, as vogais aparecem com mais freqüência que as consoantes. Uma boa cifra homofônica deve associar muitos símbolos distintos a uma mesma vogal e um número reduzido de símbolos a cada consoante.

Na Figura 5, você vê a chave original de substituição homofônica de Crema. Note que, na cifra, para cada uma das letras (a, e, o e u) são associados quatro símbolos diferentes.

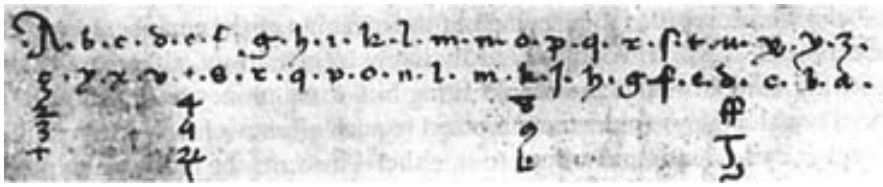


Figura 5. Tabela de substituição de Simeone de Crema
(*Fonte:* http://www.numaboa.com.br/criptologia/historia/media.php)

Você se lembra do código do Rei Felipe II da Espanha quebrado por Viète a pedido do Rei Henrique IV da França?

Era um código homófono. Naquela época, final do século XVI, o rei Felipe II tinha muitas frentes de batalha. O império espanhol dominava grande parte do mundo e os agentes espanhóis se comunicavam usando uma cifra intrincada.

A cifra espanhola era composta por mais de 500 caracteres, onde cada vogal era representada por três símbolos diferentes, cada consoante por dois símbolos, e extensas listas de símbolos para a substituição dos dígrafos e das palavras curtas mais usadas. Além disso, o código era alterado a cada três anos.

A complexidade do código não garantiu sua invulnerabilidade. Tratando-se de uma variação monoalfabética, não escapou ao arguto Viète, que utilizou com maestria a análise de freqüências. Humilhado, o rei espanhol foi reclamar com o Papa.

A criptografia estava em desvantagem perante a criptoanálise, até que surgiram duas grandes muralhas contra os quebradores de códigos: os códigos de Rossignol e de Vigenère.

A grande cifra de Rossignol

A partir do fim do século XVI, a França começa a consolidar sua liderança na criptologia. Antoine Rossignol e seu filho Bonaventure elaboraram a Grande Cifra de Luís XIV, a qual mais tarde foi usada por Napoleão em suas campanhas militares.

A Grande Cifra era homófona e tinha uma natureza original. Trabalhava com mais de 500 números. Cada grupo de números era associado a uma sílaba da língua francesa. Após a morte de Antoine e Bonaventure, caiu em desuso e suas regras foram perdidas. Muito robusta, a cifra foi quebrada em 1870 pelo militar francês Bazeries, que procurava desvendar dados históricos dos tempos de Rossignol. Bazeries trabalhou durante três anos para conseguir decifrá-la.

A cifra indecifrável

Uma alternativa à fragilidade das cifras homofônicas começou a ser desenvolvida por Leon Battista Alberti, em 1470, com a criação da primeira cifra polialfabética. Além disso, Alberti introduziu um princípio de mecanização no processo, criando um disco de cifragem, conforme demonstrado na Figura 6.

Figura 6. Discos de Alberti

Na Figura 6 aparecem duas cópias do disco de Alberti, que, conforme será apresentado, definem um código. Note que nos discos da esquerda e da direita temos, respectivamente, as correspondências, a seguir, definindo a chave do código:

A L e→ A V →

O disco externo é fixo e suas letras representam as letras da mensagem original. O disco interno pode girar sobre o eixo e suas letras servem para encriptar a mensagem.

Ao girar o disco interno, é possível definir 23 posições distintas de coincidências de letras entre o disco externo e o interno. Portanto, o disco interno é girado quantas vezes necessário, segundo a indicação da chave. No exemplo, a chave tem apenas dois estágios, definidos pelas correspondências A →L e A V→, onde A é a letra do disco externo.

A encriptação de uma mensagem é feita com a seguinte dinâmica: as letras de ordem ímpar da mensagem original são cifradas usando o disco na posição A → L, enquanto que as letras de ordem par da mensagem original são cifradas usando o disco na posição A → V.

Assim, a mensagem "volto ao amanhecer" seria codificada como "I L X Q B V B V Z V A E P A PO". O mecanismo da cifragem é semelhante se a chave é formada por mais de duas posições para os discos.

Atividade 3

Decifre a mensagem

"S E A L O F X B B X H F S R P O S Y S P A G O Z U O", que foi cifrada com três discos de Alberti nas posições S → A → V e A → L →

Apesar de representar o primeiro avanço significativo em um período de quase 800 anos, Alberti não foi capaz de aprofundar sua idéia e organizar uma cifra que pudesse resistir à análise de freqüências. Em 1523, Blaise de Vigenère publica o livro "Tratado das cifras", no qual aprofunda as idéias de Alberti, criando uma nova cifra que permaneceria indecifrável durante quase toda a Idade Moderna, até tombar sob o ataque de Babbage e Kasisk.

A cifra de Vigenère, que será detalhada nos próximos textos, consiste em usar vários discos de Alberti simultaneamente, de acordo com uma palavra chave. O número de discos para cifrar a mensagem é igual ao comprimento da palavra-chave, enquanto que as posições iniciais de cada disco são definidas por cada uma das letras da palavra. Note que, no exemplo citado anteriormente, foram usados apenas dois discos de Alberti e em duas posições iniciais bem determinadas.

Conforme já foi apresentado, a cifra de Vigenère se mostrou difícil de ser usada, em função ainda da incipiente mecanização da escrita e da comunicação. A cifragem e decifragem de uma mensagem com uma cifra de Vigenère era muito demorada, dificultando seu uso. Quando finalmente foi posta em prática, por volta de 1760, teve um curto prazo de validade. Em 1854, a cifra de Vigenère, tida como a cifra indecifrável, tombou sob o ataque de Babbage. Foi um duro golpe para os criptógrafos, deserdados de uma poderosa ferramenta.

Charles Babbage, matemático inglês, foi uma figura polêmica com uma história de vida atribulada e divertida. Filho de família nobre, foi deserdado por sua vida extravagante. Gastou parte do que ainda lhe restou de sua fortuna com implementação de máquinas e idéias nem todas muito razoáveis. No entanto, uma das máquinas desenvolvidas por Babbage é reconhecida como o primeiro protótipo de um computador.

A quebra da cifra de Vigenère foi uma realização extraordinária da criptoanálise. Foi o primeiro resultado relevante depois da criação da análise de freqüência pelos árabes há mil anos. De modo independente e nove anos depois, Friedrich Wilhelm Kasiski, um oficial da infantaria prussiana, repetiria o feito de Babbage.

Texto 17 - O umbral do século XX

Em 1844, Samuel Morse desenvolve o código que recebeu seu nome e inventa o telégrafo. A primeira mensagem telegrafada por Morse dizia: "What hath God wrought". A invenção alterou profundamente a criptografia e tornou a cifragem uma necessidade quase absoluta, mesmo para o público em geral.

Tradução: Que coisas tem feito Deus!

Por que isto aconteceu? Veja que enviar uma mensagem pelo telégrafo é essencialmente diferente de uma mensagem postada através de uma carta

comum. A mensagem será lida pelo operador de telégrafo. Portanto, mesmo assuntos domésticos eram criptografados antes de serem transmitidos em código morse pelo operador.

As cifras usadas pelo público, em geral, não teriam resistido ao ataque de um criptoanalista profissional, mas eram suficientes para proteger segredos sentimentais e comerciais de relativa importância.

Em 1894, o físico italiano Guglielmo Marconi começou a realizar experiências com circuitos elétricos. Descobriu que, sob certas condições, um circuito elétrico percorrido por uma corrente elétrica pode induzir uma corrente em outro circuito isolado a alguma distância do primeiro. O projeto dos dois circuitos é aperfeiçoado com uso de antenas. Marconi foi capaz de transmitir e receber pulsos elétricos a grande distância. Assim, foi inventado o rádio. A vantagem do sistema de Marconi era não precisar de fios.

Na aula 7, o cenário principal foi a eterna luta entre criptoanalistas e criptógrafos.

Os criptoanalistas têm vantagem graças à análise de freqüências de al-Kindy. Os criptógrafos reagem, em primeira instância, com as cifras homofônicas e uma série de expedientes diversos de dissimulação. Surge a cifra de Vigenère em 1580, a qual, no entanto, ficaria dormindo, sem uso intensivo durante quase 200 anos. Quando a cifra de Vigenère entrou em cena para valer, por volta de 1760, teve prazo de validade menor que 100 anos, sendo quebrada por Babbage em 1850.

Com a quebra da Cifra de Vigenère, a Idade Moderna termina como começou, com os criptógrafos em desvantagem, e em busca de uma nova cifra que pudesse restabelecer a comunicação secreta. É um mundo mais complexo e com importantes avanços na mecanização das comunicações. O telégrafo já é operacional e Marconi dá os primeiros passos na criação de uma nova e mais poderosa ferramenta de telecomunicação, provocando ainda maior necessidade de uma codificação segura: inicia-se a era do rádio. Um sistema de comunicação rápido, eficiente e sem fios, com o sinal viajando magicamente pelo ar a longa distância. Um sistema francamente aberto, impondo imensos desafios à proteção da informação. Tinha acabado a infância da criptografia. Nada mais seria como antes. Soam os tambores do século XX!

Aula 8 - Criptografia: História recente

O desenvolvimento da criptografia desde tempos antigos até a atualidade é marcado por três grandes fases: artesanal, mecânica e digital. Esta divisão em fases tem a vantagem de oferecer uma visão panorâmica, mas possui, de certa forma, uma relativa imprecisão, sendo impossível determinar exatamente quando uma fase começa e a outra termina.

A fase artesanal registra as primeiras manifestações históricas da criptografia e coincide com o advento da escrita, cobrindo as Idades Antiga e Média. No início da Idade Moderna, com a invenção da Imprensa, aparecem os primeiros indícios da fase mecânica da criptografia.

Com a Revolução Industrial, iniciada na Inglaterra em 1760, seguida da invenção do telégrafo e do rádio no século seguinte, a fase mecânica se desenvolve e seu apogeu ocorre com as máquinas de cifragens usadas durante a Segunda Guerra Mundial. A máquina alemã Enigma é a mais ilustre representante desta linhagem.

Texto 18 - A criptografia mecânica

A Revolução Industrial criou no homem a paixão pelas máquinas e a esperança de substituição do cansativo trabalho manual pelo mecânico.

No fim do século XIX, o telégrafo já estava consolidado com quase 50 anos de existência e a comunicação pelo rádio já era uma realidade. Os primeiros testes positivos foram realizados por Marconi em 1894. Era uma época muito difícil para a criptografia. O surgimento do rádio, uma ferramenta de comunicação poderosa e aberta, exigia uma criptografia ainda mais robusta, à prova de ataques. A cifra de Vigenère, vista como indecifrável, tinha sido quebrada por Babbage e Kasiski e nada de novo havia sido criado pelos criptógrafos, gerando um sentimento de insatisfação.

Com o rádio, pela primeira vez a criptografia enfrentava um desafio sem precedentes. A extrema facilidade da comunicação também permitia que a mensagem no caminho até o destinatário, quase sempre fosse interceptada pelo inimigo. Era a comunicação aberta e a distância lançando as primeiras sementes da globalização.

A Primeira Guerra Mundial

O século XX conviveria com o flagelo de duas grandes guerras. Nos preparativos para a Primeira Guerra Mundial, todos os países envolvidos contavam com o poder de comunicação do rádio. Porém, não tinham certeza em como garantir uma transmissão secreta. O rádio oferecia aos comandantes militares a ocasião de exercer um controle contínuo e instantâneo das forças armadas. Longe do teatro de operações, o comandante era constantemente informado da evolução das batalhas e organizava suas estratégias de forma mais consciente do que se estivesse no front. A época do general orquestrando a batalha do alto de uma colina com toques de corneta havia ficado para trás.

A Primeira Guerra Mundial iniciou com a grande ofensiva alemã em 21 de março de 1918. Neste conflito, a mais famosa cifra em uso foi a ADFGVX, obtida com uma combinação de técnicas de substituição e transposição.

Em junho de 1918, com menos de três meses de batalhas, o exército alemão estava a 100 quilômetros de Paris e preparava a ofensiva final. Era vital descobrir qual seria o ponto selecionado pelos alemães para penetrar na defesa aliada. A informação permitiria a concentração de esforços e a neutralização do efeito surpresa. A esperança da França e dos aliados era decifrar o código ADFGVX.

As forças aliadas tinham uma arma secreta: um criptoanalista chamado Georges Pavin. Pavin tinha grande reputação por ter quebrado todos os códigos alemães até aquela data. No entanto, no fim de maio de 1918, os franceses interceptam, pela primeira vez, uma mensagem em código ADFGVX que Pavin não consegue decifrar. O criptoanalista lutou contra a cifra durante dias e noites. Finalmente, em 2 de junho de 1918, conseguiu encontrar a chave que decifraria o algoritmo ADFGVX.

A partir deste momento, Pavin começa a decifrar todas as mensagens interceptadas, principalmente a que revelou o ponto escolhido pelo exército alemão para o ataque rumo a Paris. Imediatamente as tropas aliadas reforçaram o local e, uma semana depois, o ataque alemão começou. A batalha durou cinco dias. Com a perda do elemento surpresa, o exército alemão recuou.

Os ingleses também possuíam um grupo de criptoanalistas trabalhando na Primeira Guerra Mundial. Este grupo foi responsável direto pela entrada dos Estados Unidos no conflito em março de 1920. Em janeiro de 1917, a Inglaterra intercepta uma mensagem alemã para o embaixador alemão em Washington. Foi o famoso telegrama Zimmermann, como ficaria conhecido mais tarde.

Um ponto essencial na estratégia alemã era isolar a Inglaterra, com o uso de submarinos, e impedir a chegada de suprimento pelo mar. Em 7 de maio de 1915, submarinos alemães que patrulhavam a costa da Irlanda afundaram o navio Lusitânia, matando mais de mil passageiros civis, sendo 128 americanos. Foi uma afronta terrível à nação americana e quase levou os americanos à guerra, se não fosse a garantia dada pelos alemães de que seus submarinos não mais atacariam estando submersos. A precaução era evitar ataques acidentais a navios mercantes que transportavam civis. Esta promessa de conduta acalmou os americanos.

Porém, em 9 de janeiro de 1917, o Alto Comando Alemão resolve partir para uma guerra naval irrestrita. Os alemães sabiam que, uma vez quebrada a promessa, com os submarinos atacando abaixo da linha d'água, era inevitável a entrada dos americanos na guerra. Portanto, a estratégia seria desenvolver uma operação relâmpago, isolando a Inglaterra e forçando sua capitulação em seis meses. Era preciso também cuidar da reação americana. O plano desenvolvido foi convencer o México a se unir em aliança com a Alemanha, atacando os Estados Unidos. O objetivo era dividir as forças americanas, entre a defesa de seu território e a participação no teatro principal de operações na Europa.

Esse era o teor do telegrama Zimmermann, endereçado ao embaixador alemão em Washington, que seria transmitido ao seu colega no México, para ser decodificado e transmitido ao presidente mexicano.

A proposta incentivava os mexicanos para a reconquista dos territórios do Novo México, Texas e Arizona, com a ajuda da Alemanha, que ofereceria apoio militar e financeiro. Além disso, solicitava o empenho do México para convencer os japoneses a atacar os Estados Unidos. Veja a íntegra do telegrama Zimmermann decodificado:

> Pretendemos iniciar a guerra submarina irrestrita no dia 1 de fevereiro. Apesar disso, devemos tentar manter a neutralidade dos Estados Unidos. No caso de não termos sucesso, faremos ao México uma proposta de aliança na seguinte base: faremos a guerra juntos e a paz juntos, apoio financeiro generoso e a compreensão, de nossa parte, de que o México deve reconquistar seus territórios perdidos no Texas, Novo México e Arizona. Os detalhes do acordo ficam por sua conta. Deve informar ao presidente (do México) do que se encontra resumido acima, assim que o início da guerra contra os Estados Unidos esteja certo e acrescentar a sugestão de que ele deve, por sua própria iniciativa, convidar o Japão para se unir a nós e ao mesmo tempo servir como mediador entre nós e o Japão. Chame a atenção do presidente para o fato de que o emprego irrestrito de nossos submarinos agora oferece uma perspectiva de levar a Inglaterra a assinar a paz dentro de alguns meses. Acuse recebimento. Zimmermann. (SINGH, 2001)

O telegrama Zimmermann impõe reflexões, pois representa a cifragem de uma mensagem longa, o que significa um presente para o criptoanalista. Por que o risco foi assumido? A hipótese mais provável foi a excessiva autoconfiança alemã, subestimando a capacidade aliada.

A Segunda Guerra Mundial

Foi marcante a entrada em cena da máquina de cifras alemã denominada Enigma, durante a Segunda Guerra Mundial. A primeira foi desenvolvida em 1918 pelo engenheiro alemão Arthur Scherbius. O objetivo era facilitar a troca de documentos secretos entre comerciantes e homens de negócios.

No entanto, a máquina não conseguiu empolgar o setor. Mais tarde, a invenção de Scherbius se torna interessante para uso militar. O governo alemão adquire o direito de utilização da Enigma e o exército redesenha a

máquina, começando a usá-la em junho de 1930 com o nome de Enigma I. Durante a guerra, o modelo inicial é aperfeiçoado e todos os níveis do governo alemão, incluindo o exército e a diplomacia, utilizam a máquina para se comunicar.

O filme Enigma (2001), do diretor Michael Apted, mostra a equipe de decodificadores ingleses que precisam decifrar, durante a Segunda Guerra Mundial, um código ultra-seguro – o Enigma – usado pelos nazistas para mandar mensagens aos seus submarinos. Vale a pena assisitir e entender como funcionava a máquina alemã.

Veja alguns detalhes da estrutura da Enigma (figura 6):

• a mensagem era cifrada e decifrada usando o mesmo tipo de máquina. A Enigma lembrava uma máquina de escrever.

• era constituída de um teclado, um painel luminoso, uma câmara com três misturadores, um refletor e um painel frontal com cabos elétricos.

• a chave para utilização da Enigma dependia de uma configuração de montagem, que compreendia a ordem e posição dos misturadores, conexão dos cabos emparelhando duas letras no painel frontal e a posição do refletor.

• para cifrar uma mensagem, o operador teclava uma letra e o comando estimulava o circuito elétrico e as letras cifradas apareciam, uma a uma, no painel luminoso. Eram anotadas para compor a mensagem secreta.

Figura 6. A máquina Enigma

(Fonte: http://www.temakel.com/histenigma.htm)

A máquina Enigma foi a ferramenta criptográfica mais importante da Alemanha nazista e os alemães apostavam em sua eficiência para vencer a guerra. Ela trabalhava com um processo de cifragem complexo e de chave simétrica e, por questões de segurança, a cada mensagem a chave era trocada.

A cifra começou a ser quebrada pelo matemático polonês Marian Rejewski, cujo esforço inicial foi baseado em textos cifrados interceptados e em uma lista de três meses de chaves diárias obtidas através de um espião.

O trabalho de quebra da cifra Enigma foi concluído pela equipe inglesa liderada por Alain Turin, Gordon Welchman e outros pesquisadores, em Bletchley Park, Inglaterra.

Na próxima disciplina, Criptografia Geral, você verá a descrição em detalhes das partes constituintes e do funcionamento da máquina Enigma.

Texto 19 - A Criptografia eletrônica: a cifra DES

Na criptografia mecânica é fundamental a ocultação pública da chave e também desejável manter segredo sobre a estrutura da máquina que produz a cifragem. Com o desenvolvimento e aperfeiçoamento dos computadores e a incrível capacidade de realizar mais de um milhão de operações por segundo e a necessidade de uso da criptografia pelo comércio e bancos, os algoritmos criptográficos passam a ser de conhecimento público e o segredo a residir exclusivamente na chave.

Em 1974, a IBM apresenta à agência oficial americana NBS (National Bureau of Standards) uma cifra que alguns pesquisadores vinham desenvolvendo desde 1960. A NBS, após avaliar o algoritmo com a ajuda da NSA (National Security Agency), introduz algumas modificações, principalmente a redução na dimensão do espaço de chaves, e adota o código como padrão de cifragem de dados para os Estados Unidos. O código passou a ser conhecido como DES (Data Encryption Standard).

No DES, apesar da exigência de redução imposta pela NBS, a quantidade de chaves distintas que pode ser definida atinge 2^{56}, um número muito elevado.

NSA é o órgão oficial de segurança em comunicações do governo norte-americano. Fundada no início dos anos 50 do século XX pelo presidente Truman, é até hoje responsável oficial pela segurança em termos de criptografia nos Estados Unidos.

A experiência acumulada pela NSA coloca-a anos à frente dos esforços públicos em criptografia. No entanto, é interessante observar o contexto da intervenção da National Security Agency, solicitando a diminuição da dimensão do espaço de chaves do DES. A NSA forçou a IBM a enfraquecer o sistema de tal forma que o governo americano pudesse eventualmente quebrar mensagens. Naturalmente, a NSA, ainda hoje, nega o ocorrido.

Inicialmente projetado pelos pesquisadores da IBM para atender a demanda dos bancos, o DES foi concebido para implementação em um computador. O processo de cifragem é realizado em 19 etapas de aplicação de um algoritmo definido pela chave. Cada fase necessita de milhões de operações por segundo, portanto, só factíveis em um computador.

O DES é o algoritmo criptográfico mais usado atualmente no mundo. Sua utilidade atende aos bancos, aos órgãos de defesa, às grandes companhias e ainda ao comércio eletrônico na internet. Funciona com chave simétrica (chave privada) de 56 bits, sendo extremamente difícil de ser quebrado.

Nos Estados Unidos, além da utilidade comercial, o DES é usado pelo Ministério da Defesa, órgão que controla também sua exportação. Ainda que seja muito seguro, certas empresas e bancos preferem usar o duplo-DES ou o triplo-DES, que é exatamente um código no qual a rotina do algoritmo é aplicada duas ou três vezes.

A aula 8 abordou o desenvolvimento da criptografia no século XX, cobrindo toda a fase definida como mecânica e avançando até o surgimento dos computadores de grande porte. Nesta parte, foi apresentado o primeiro código desenvolvido para operar em um computador de grande porte, a cifra DES. É o primórdio da fase digital.

Durante toda esta etapa, que cobriu a fase mecânica até o princípio da fase digital com o algoritmo DES, um aspecto permaneceu inalterado: a utilização de chaves privadas, caracterizando uma criptografia simétrica. A chave que produz a mensagem cifrada é a mesma para decifrá-la. Assim, como você já viu, esta é a principal fragilidade destes códigos. O problema de distribuição de chaves torna-se difícil para o caso de compras através da internet ou troca de mensagens entre as pessoas que estão ligadas no ciberespaço.

Qual é a saída para a situação? Ela existe?

Na próxima aula, você terá contato com a revolução provocada na criptografia pela invenção das chaves públicas. Neste momento também será a época dos computadores pessoais e da internet - poderosa ferramenta que chegou para revolucionar a comunicação e, em sentido mais profundo, a própria organização da sociedade mundial.

Nos jogos de infância tivemos a oportunidade de nos divertirmos com brincadeiras de comunicação secreta. Quem se lembra de ter praticado o código do espelho? A brincadeira funcionava mais ou menos assim: a mensagem original era escrita no papel e o lado escrito era virado para um espelho. O texto cifrado aparecia refletido e era copiado. O amigo ou amiga da brincadeira receberia uma mensagem com letras ao avesso. Para ter acesso ao conteúdo, deveria refletir o texto cifrado de novo no espelho, onde leria a mensagem. Este era o código.

A chave simétrica consistia em refletir a mensagem no espelho, tanto para cifrar como para decifrar a mensagem. É saudoso lembrar estes tempos descompromissados e de ingênuos jogos de criptografia. Atualmente, no mundo globalizado, computadores ligados em rede e a internet determinam a evolução da comunicação, do mercado e, mais profundamente, da organização da sociedade.

O sistema globalizado e aberto proporcionado pela rede mundial de computadores necessita de ferramentas capazes de:

- garantir a segurança do sistema na troca de mensagens confidencias;
- controlar a adulteração de mensagens e dados;
- garantir credibilidade para o comércio eletrônico;
- autenticar assinaturas digitais e outros tantos desafios.

A criptografia se firma como uma importante ferramenta em auxílio à necessidade de troca de informações com segurança, em um mundo cada vez mais globalizado.

Ao revisar todos os algoritmos criptográficos que você já estudou até aqui, começando na antiguidade com o código de César, passando pela cifra ADFGVX usada na Primeira Guerra Mundial, pela máquina Enigma na Se-

gunda Guerra Mundial, chegando na poderosa cifra DES, absorvida pela NSA americana, há uma característica comum: todas as chaves eram privadas.

Um processo de comunicação secreta com chave privada necessita de um canal especial de comunicação em paralelo, seguro suficiente para a prévia troca de chaves entre o remetente e o destinatário. Este momento é muito delicado e nele reside a maior fraqueza destes sistemas criptográficos de chave simétrica.

A principal fragilidade dos algoritmos criptográficos de chave simétrica reside na necessidade prévia da troca de chaves.

Quais são as alternativas para o segredo da chave? O remetente e o destinatário, por exemplo, poderiam se encontrar uma vez por mês para combinarem as chaves. Mas se um deles adoece e não pode comparecer ao encontro? É preciso colocar uma terceira pessoa no circuito para viabilizar a passagem da chave. Surge então o perigo de corrupção. Poderia se pensar no telefone, mas o aparellho pode estar grampeado.

A longa convivência da criptografia com a chave simétrica e a aparente impossibilidade de alternativas pareciam ter estabelecido a chave simétrica como um axioma para a criptografia, impossível de ser contrariado. É justamente neste cenário conformista que, na segunda metade do século XX, alguns pesquisadores começam a pensar na utopia da chave pública. Uma chave que fosse de conhecimento de todos, mas, como "um pulo de gato", garantisse a comunicação secreta entre duas ou mais pessoas.

Texto 20 - Computadores e representação da informação

Durante a Segunda Guerra Mundial, os britânicos superaram os alemães, pois decifraram todos os códigos nazistas. Para fazer face ao processo mecânico e rápido da Enigma, os quebradores de códigos de Bletchey inventaram dois tipos de máquinas: as bombas de Alan Turing e a Colossus, projetada por Max Newman e primeiramente construída por Tommy Flowers.

A Colossus era uma máquina mais elaborada, potente e flexível que as bombas. Possuía a característica fundamental de ser programável, o que a referenciou como a primeira e mais primitiva de uma linha de máquinas que evoluíram para os modernos computadores.

Era evidente a superioridade da Colossus sobre os engenhos mecânicos. Em um moderno computador, a informação é representada através de uma seqüência de zeros e uns: são os dígitos binários, mais adequadamente referidos por bits. Portanto, para começar uma cifragem de uma mensagem através do computador, a primeira operação consiste na tradução da mensagem original, em números binários. Existem vários protocolos que fazem a transformação.

Um exemplo é o ASC II (Código padrão americano para a troca de informações), que destina a cada letra do alfabeto um número binário de sete dígitos - o que representa uma seqüência de zeros e uns.

No caso de 1011110, trata-se de um número binário de sete dígitos. Como há a possibilidade de $2^7 = 128$ números binários distintos com sete dígitos, então é possível representar todas as letras do alfabelto, maiúsculas e minúsculas, e ainda todos os sinais da linguagem escrita, pontos de interrogação, exclamação, vírgula e outros símbolos.

Veja a Tabela 1, que mostra a relação entre números binários e as letras maiúsculas do alfabeto, segundo o Protocolo ASC II.

A 1000001	B 1000010	C 1000011
D 1000100	E 1000101	F 1000110
G 1000111	H 1001000	I 1001001
J 1001010	K 1001011	L 1001100
M 1001101	N 1001110	O 1001111
P 1010000	Q 1010001	R 1010010
S 1010011	T 1010100	U 1010101
V 1010010	X 1011000	Z 1011010

Tabela 1. Alfabeto representado no ASC II

Para representar a palavra FELIZ, por exemplo, em linguagem binária, usando o protocolo ASC II, usamos a Tabela 1 para encontrar:

1000110 1000101 1001100 1001001 1011010

A seqüência de números anterior representa a palavra FELIZ na linguagem do computador.

Atividade 4

Traduza a palavra a seguir representada em linguagem ASC II:

1000011 1010010 1001001 1010000 1010100 1001111 1000111
1010010 1000001 1000110 1001001 1000001

Texto 21 - No caminho da chave pública

Vamos voltar ao problema fundamental que preocupou os criptógrafos de todos os tempos: a distribuição das chaves. Para pensar a questão, você pode escolher Alice, Bob e Eva, personagens fictícios da literatura da criptografia para animar a discussão.

A situação típica a ser analisada ocorre quando Bob quer mandar mensagens para Alice, sob o risco de Eva interceptar a comunicação. Bob e Alice precisam combinar as chaves que serão usadas ao longo da troca das mensagens.

Na criptografia simétrica, uma mesma chave será usada por Bob para codificar uma mensagem e por Alice para decodificá-la. Neste momento é que ocorre o problema. No processo de comunicação da chave, Eva pode ter acesso. Em uma situação mais simples, Bob e Alice podem marcar um encontro mensal, onde combinam as chaves. Mas se Bob e Alice estão distantes, qual seria o meio seguro para trocar a chave? Esta é a fragilidade principal dos algoritmos de chave simétrica.

A chave que cifra a mensagem é a mesma que a decifra. A necessidade de uma chave simétrica foi considerada uma verdade necessária durante quase dois mil anos, até que foi contrariada em 1976, com a criação do conceito de chave pública/chave privada.

Mas voltando à pergunta: será possível a troca secreta de mensagens entre Bob e Alice sem que haja previamente uma combinação das chaves? Vamos imaginar a seguinte situação que poderia ter ocorrido na época do Imperador Júlio César.

Veja como Alice e Bob podem trocar mensagens secretas sem nenhuma combinação prévia de chaves. Alice deseja comunicar, em segredo para Bob a mensagem:

" encontro"

E assim escolhe para cifrar um código de César, que avança duas casas do alfabeto. Isto é, a letra a será cifrada como C, a letra b será cifrada como D e assim por diante. Desta forma, a mensagem "encontro", cifrada por Alice, chegaria para Bob como:

" G P E Q P V T Q"

Bob, ao receber a mensagem cifrada, escolhe a sua cifra pessoal, do tipo César, que corresponde a avançar cinco casas no alfabeto, aplica nova cifragem na mensagem e reenvia para Alice. Veja como fica a mensagem duplamente cifrada ao chegar até Alice:

"L U J V U C A V"

Agora é o momento de Alice retirar da mensagem sua cifra usando sua chave pessoal, e retornar a mensagem para Bob. Decifrar para Alice é recuar duas

casas no alfabeto. Veja como chega para Bob a mensagem, após a atuação de Alice:

"J S H T S A X T"

Bob recebe uma mensagem que tem apenas a intervenção de sua cifra. A cifra de Alice foi retirada. Portanto, Bob pode agora decifrar a mensagem utilizando sua chave pessoal, que no caso de decifragem corresponde a recuar cinco casas no alfabeto. Ao final deste processo, Bob pode finalmente ler a mensagem que Alice passou secretamente:

" e n c o n t r o"

O que aconteceu no processo? Houve uma troca secreta de mensagens entre Bob e Alice sem necessidade prévia de combinar chaves. Bob tem uma chave e Alice, outra chave. Ambas são chaves simétricas. Este exemplo simples mostra a possibilidade da troca de mensagens secretas entre duas pessoas sem necessidade da troca prévia da chave. É evidente que nem sempre a situação é simples, como o código de César. Pela primeira vez, você viu, através de um exemplo, que a troca prévia de chaves não é uma parte intrínseca, inevitável da criptografia.

Mas será que este método de dupla cifragem funciona sempre e resolve, de uma vez por todas, o problema da distribuição das chaves? Infelizmente não. Na troca de mensagem entre Bob e Alice ocorreu a seguinte ordem de intervenção: Alice cifra, Bob cifra, Alice decifra e Bob decifra. Ocorreram duas cifragens para, em seguida, ocorrer em duas decifragens. Em geral, duas cifragens consecutivas podem introduzir uma confusão na estrutura da mensagem, tornando-a irrecuperável.

A situação do exemplo anterior funcionou porque o código de César é muito simples, linear e uma dupla cifragem não altera a natureza do processo. Mesmo com cifras monoalfabéticas, em geral, não é possível recuperar as mensagens. A ordem ideal na ocorrência de dupla cifragem seria: cifragem, decifragem, cifragem, decifragem. Ou seja, o último que cifra é o primeiro a decifrar. Mas esta regra não atende à natureza de nosso problema.

Do ponto de vista matemático, a cifra de César é uma simples função matemática denominada translação. Foi exatamente a extrema simplicidade dessa função associada ao código de César que tornou possível o exemplo

A construção dos primeiros computadores abriu novos horizontes para a criptografia e marca o início do uso de métodos matemáticos relevantes para a construção de códigos.

anterior: uma troca secreta de mensagem sem combinação prévia de chaves.

Vamos modificar a pergunta, sem alterar a natureza do objetivo que perseguimos. É possível Bob e Alice combinarem uma chave, através de uma troca de mensagens no sistema aberto de comunicação, e que, no final do processo, termine como conhecimento exclusivo deles? Existem funções na matemática que podem cumprir esta missão?

A resposta a este problema foi encontrada pela dupla de pesquisadores Whitfield Diffie e Martin Hellman em 1976, que publicaram o livro "New Directions in Cryptography". A função usada por Diffie e Hellman para resolver o problema, uma combinação de função exponencial com aritmética modular, é denominada, no jargão da criptografia, função de mão única. No entanto, a construção era teórica, aparentemente, sem apontar possibilidades de realização prática.

O resultado obtido pelos pesquisadores, em 1976, introduzia a possibilidade do conceito de chave pública. Apesar de ser um resultado no plano teórico, representou um passo gigantesco, arranhando o dogma da criptografia, o qual estabelecia a necessidade de uma troca prévia de chave.

Porém, entre o resultado teórico e a tradução em algo aplicável, existe um longo caminho. Felizmente este trajeto se revelou virtuoso e conduziu a um dos resultados mais impressionantes da criptografia: a invenção da chave pública/privada, através da famosa cifra RSA, em 1977.

Criptografia de chave pública - a Cifra RSA

O monopólio da agência governamental americana NSA (National Security Agency), em questões ligadas à criptografia, manteve-se permanente até o grande salto dado por Diffie e Hellman, em 1976, ao introduzirem teoricamente o conceito de chave pública.

O conceito revolucionário foi criado inteiramente longe da influência da NSA e teve impressionante impacto no ambiente acadêmico. Imediatamente foi estabelecido um movimento independente, com a realização de conferências regulares e lançamento de jornais científicos dedicados à área de pesquisa.

Após a publicação, em 1976, do conceito de chave pública pelos pesquisadores, houve uma verdadeira corrida ao ouro na tentativa de traduzir na prática as idéias reveladas.

A corrida foi vencida em 1977, por Rivest, Shamir e Adleman, três brilhantes pesquisadores do MIT (Massachussetts Institute of Technology). Baseados nas idéias de Diffie e Hellman, eles construíram um dos mais poderosos algoritmos criptográficos que o mundo conheceu. O algoritmo foi batizado como RSA (iniciais dos nomes Rivest, Shamir e Adleman). Em 1983 foi aceita a patente do RSA, o que representou o primeiro algoritmo criptográfico da história a receber um registro desta natureza.

Durante o intervalo de tempo entre o anúncio da descoberta em 1977 e o recebimento da patente em 1983, Rivest, Shamir e Adleman não publicaram detalhes da cifra RSA. No entanto, em setembro de 1977, no calor da descoberta, os três pesquisadores entregaram um texto relatando a pesquisa para Martin Gadner, com o objetivo de ser publicado na revista Scientific American.

O artigo apareceu na edição de setembro de 1977 e incluía a oferta de enviar o relatório técnico completo para qualquer um que enviasse um envelope selado com o próprio endereço. Foram recebidos milhares de pedidos vindos de todo o mundo.

A NSA contestou a distribuição deste relatório para estrangeiros e os relatórios não foram enviados. Esta foi uma situação ideal para os pesquisadores, que perceberam a necessidade de não dar maior divulgação ao algoritmo antes de conseguir a patente.

Após a aceitação da patente e não tendo a NSA informado a base legal da proibição, apesar da solicitação dos pesquisadores, os relatórios foram enviados. Também neste tempo, logo após esta tentativa de censura por parte da NSA, a comunidade acadêmica reagiu em defesa de sua indepedência. Estava instaurada a luta entre o controle do estado sobre a criptografia e a pressão da sociedade exigindo o uso irrestrito da ferramenta.

O algoritmo RSA tem sua base matemática na teoria dos números primos e a aritmética modular. Trabalha com duas chaves matematicamente ligadas, uma para cifrar (chave pública) e outra para decifrar (chave secreta, particular). A chave privada, usada para decifrar, consiste de dois números primos muito grandes (digamos P e Q). A chave pública, usada para cifrar, é definida por N , onde N é obtido pelo produto N = P x Q. A chave pública N pode ser comunicada a todo mundo e figurar, por exemplo, em uma espécie de lista pública de chaves.

Porém, em um sistema de chave pública, como funciona a troca de mensagens secretas entre Bob e Alice sob os olhos espertos de Eva?

Para mandar uma mensagem para Alice, Bob deve antes procurar a chave pública de Alice na lista pública que está à disposição de quem quiser. Ele encontra o número N, cifra a mensagem com esta chave pública e envia a Alice. A mensagem codificada chega a Alice, que usará sua chave secreta composta pelos números primos P e Q para decifrar e ler a mensagem.

A espiã Eva conhece a chave pública N de Alice, e pode mesmo interceptar a mensagem cifrada de Bob. No entanto, Eva não poderá decifrá-la, pois não conhece os números primos P e Q, que são de conhecimento exclusivo de Alice. E esses números compõem exatamente a chave privada.

O fundamento que sustenta a impossibilidade virtual de Eva, a partir do conhecimento do número N, de encontrar seus fatores primos P e Q é a teoria de fatoração dos números inteiros.

A teoria estabelece que se um número N tem mais do que 10^{160} dígitos e é obtido como produto de dois números primos, cada qual com mais de 10^{70} dígitos, então o tempo computacional para encontrar estes fatores é maior que a idade do universo. Você leu corretamente! No estágio de desenvolvimento tecnológico em que vivemos, mesmo com todos os computadores do mundo trabalhando em rede e usando os melhores algoritmos de fatoração, o tempo para encontrar os fatores primos P e Q do número N, com as características especificadas, seria maior do que a idade do universo!

No mundo da criptografia RSA, cada usuário possui duas chaves, uma secreta e outra pública, com finalidades distintas e complementares.

A chave secreta jamais deverá ser revelada a ninguém, ao passo que a chave pública é difundida sem restrição. A regra de segurança número um da cifra RSA garante que é impossível, virtualmente, deduzir a chave secreta a partir da chave pública.

O algoritmo RSA é classificado como chave assimétrica, uma vez que a chave que cifra a mensagem é diferente da chave que decifra a mensagem.

Todo algoritmo de chave assimétrica, como o RSA, resolve dois problemas importantes da criptografia de todos os tempos: primeiro elimina a necessidade de troca preliminar de chaves e, em segundo lugar, fornece um método para autenticação de mensagens.

Texto 22 - Popularização da criptografia: criptografia híbrida

Os algoritmos de chave assimétrica (como o RSA) têm a desvantagem de serem pesados e muito mais lentos que os algoritmos de chave simétrica (como o DES). Portanto, algoritmos de chave simétrica não são indicados para cifrar mensagens muito longas. Também não são recomendados para uma política de popularização da criptografia, como para o uso em computadores pessoais.

Um meio de atenuar esta dificuldade é combinar os dois tipos de algoritmos: o de chave simétrica com o de chave assimétrica. Esta combinação é denominada de criptografia híbrida ou "envelope digital".

A solução mais famosa foi o PGP (Pretty Good Privacy), inventado por Philip R. Zimmermann, que representou um marco na popularização da criptografia e incomodou o governo americano.

Inquieto politicamente desde a época de estudante, Philip Zimmermann fazia parte de grupos ativistas anti-nucleares nos EUA. Philip foi muitas vezes ao deserto, aos locais programados para explosões atômicas, sentar no chão com uma pequena multidão de manifestantes. Como conseqüência de suas atividades de protesto, esteve duas vezes preso.

Porém, Philip tinha outras duas paixões: a informática e a criptografia. Ele se empenhou para encontrar uma saída na implementação do algoritmo RSA, ou uma modificação dele, em computadores pessoais. Trabalhou intensamente no projeto em 1984. Em junho de 1991, Zimmermann liberou a primeira versão do programa que iria se tornar o cavalo de batalha do ideal da criptografia para as massas. Denominou seu sistema de PGP (Pretty Good Privacy).

Inicialmente, Zimmermann pensou em comercializar seu produto. No entanto, o PGP usava em rotinas internas o RSA, um produto patenteado. Diante do dilema de uma demorada negociação com os dententores da patente do RSA e temeroso de que o uso popular de programas de criptografia por chave pública terminasse sendo proibido por imposição da NSA, Philip liberou gratuitamente o código-fonte do PGP para uso do público em geral. O PGP espalhou-se, de forma incrivelmente rápida, por todo o planeta.

A reação da NSA foi imediata, processando Philip por usar nas rotinas internas do PGP o algoritmo patenteado RSA. A argumentação de Philip se baseou no fato de não haver cobrado pelo PGP e que a distribuição seguiu a tradição acadêmica de divulgação dos resultados de um projeto de pesquisa científica.

Em um primeiro momento, a disputa judicial resultou na ilegalidade de uso do PGP nos EUA. A situação de Zimmermann complicou ainda mais, uma vez que o algoritmo RSA sofria restrições de exportação. O ITAR (International Traffic in Arms Regulations) proibiu a exportação de software criptográfico sem prévia licença do Departamento de Estado dos EUA, uma licença difícil de ser obtida para algoritmos criptográficos de alta performance, como o RSA, que são considerados armas de guerra. Zimmermann estava sendo acusado de contrabandear armas.

Foi um embate memorável, longo e emocionante entre Philip Zimmermann e o Governo americano. Neste episódio estava em discussão a liberdade das pessoas de possuir privacidade e a pressuposição da autoridade estatal que invocava direitos de invadir sem barreiras esta privacidade em favor da segurança nacional. O caso foi arquivado após três anos.

Como funciona a comunicação protegida através de um algoritmo híbrido como o PGP? Alice prepara o envio de uma mensagem para Bob. Em um primeiro momento, Alice cifra o texto destinado a Bob com um algoritmo simétrico rápido (por exemplo, o DES, que, neste caso, emprega uma chave

secreta). Em uma segunda etapa, Alice irá cifrar a chave secreta (do DES) com a chave pública de Bob. O algoritmo assimétrico (por exemplo o RSA) vai cifrar um texto muito curto, apenas a chave secreta que Alice usou para cifrar a mensagem e não a própria mensagem. A comunicação é enviada a Bob. Este exemplo mostra que usando uma chave híbrida é possível cifrar rapidamente mensagens tirando benefícios dos dois sistemas. No entanto, tudo foi possível graças à chave pública.

Texto 23 - Autenticidade, certificação e assinaturas digitais

Você viu anteriormente como o conceito de chave pública elimina a necessidade da troca preliminar de chaves. Vamos agora nos concentrar no problema de autenticidade de mensagens, certificação e assinaturas digitais.

Autenticidade e assinatura digital

Alice acaba de receber uma mensagem de Bob. Como garantir a autenticidade? Como Alice, ao receber a mensagem de Bob, pode ter certeza de que a mensagem não foi interceptada e adulterada por Eva no meio do caminho? Agora, será mostrado a você como este problema geral de autenticidade de documentos é resolvido com algoritmos de chave pública. Como devem Bob e Alice proceder?

Antes de enviar a mensagem a Alice, Bob deve tomar precaução de modo a garantir que, ao receber a mensagem, Alice possa reconhecer que esta veio dele e não foi adulterada. Em primeiro lugar, Bob cifra a mensagem usando sua chave privada (é a autenticação da mensagem), gerando o que significaria uma assinatura digital.

Veja o esquema representado na figura 7.

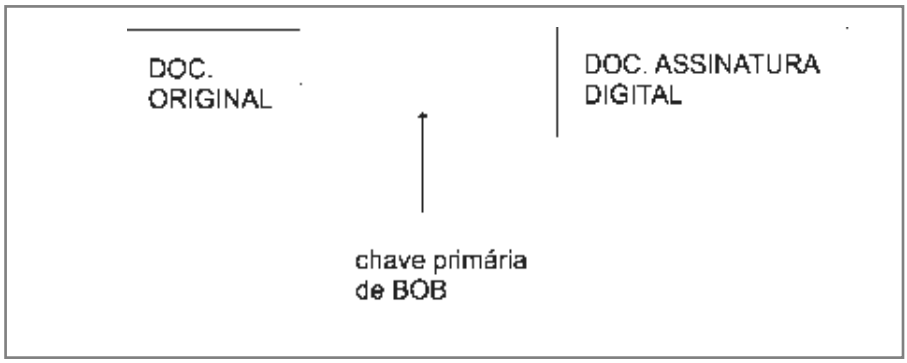


Figura 7. Assinatura digital de Bob com chave privada

A única chave que pode decifrar esta mensagem é a chave pública de Bob. Desta maneira, quando Alice ao receber a mensagem cifrada e decifrá-la com a chave pública de Bob, todos terão certeza de que foi Bob e ninguém mais o autor da mensagem, uma vez que só Bob possui a chave secreta ligada matematicamente à sua chave pública.

Em resumo, é impossível qualquer um forjar a assinatura de Bob. Da mesma forma, tendo assinado a mensagem, Bob jamais poderá alegar no futuro que outra pessoa falsificou sua assinatura.

Porém, Bob pode enviar uma mensagem autêntica (assinada) e privada para Alice. De que forma? Em primeiro lugar, Bob cifra a mensagem com sua chave privada e, em seguida, promove uma nova cifragem com a chave pública de Alice.

Assim, ao receber a mensagem, Alice usa sua chave privada para a primeira decodificação da mensagem e depois aplica a chave pública de Bob para finalmente ter acesso à mensagem. Neste procedimento, somente Alice pode abrir e ter certeza de que a mensagem partiu de Bob.

Certificação de chaves públicas - cartórios digitais

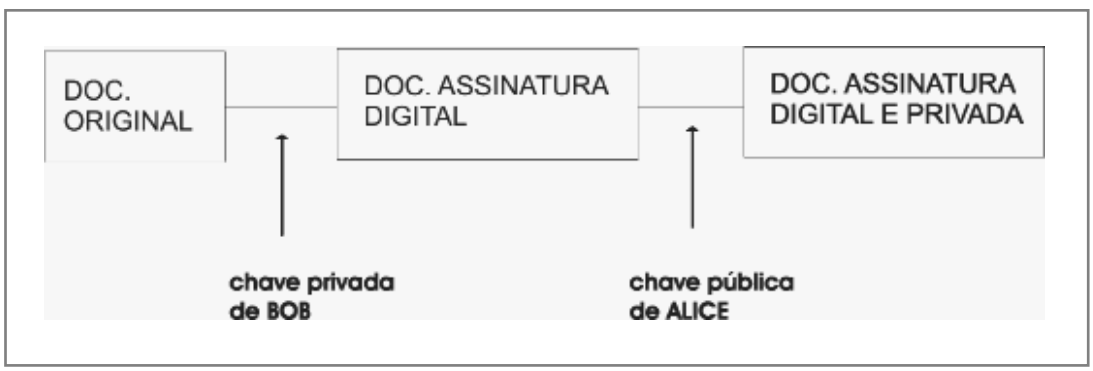


Figura 8. Dupla cifragem: autenticação e privacidade

Será que não existe um ponto fraco no conceito de chave pública? Suponha que Alice consulte, em uma lista pública de chaves, a chave pública de Bob. Como garantir que a chave é realmente de Bob? Eva poderia ter registrado na lista uma chave pública em nome de Bob. Nesta situação, Eva teria a chave privada complementar e decodificaria toda mensagem que fosse dirigida a Bob, enquanto que Bob não saberia o que aconteceu.

Uma das saídas para esta possibilidade de fraude é a certificação de chaves públicas. Empresas idôneas, como cartórios digitais e sob supervisão de autoridades, têm como função receber as chaves públicas de pessoas ou empresas e certificar estas chaves. Assim, quando Alice quer a chave pública de Bob, deve buscar na lista de chaves mantida pela autoridade certificadora. O organismo certificador deve tomar todas as precauções no processo de autenticação, em função do grau de importância que a chave pública implica. O cartório digital, por exemplo, pode marcar um encontro pessoal com Bob para o recebimento da chave.

Comércio eletrônico

O emprego popular da extraordinária rede possibilitada pela internet é, antes de tudo, uma revolução em matéria de expressão humana em escala planetária. É um espaço gigantesco de comunicação que permite a criação de novos tipos de empresas, explorando novos potenciais da economia e, sobretudo, melhorando os canais de distribuição da informação.

A internet é um espaço mundial descentralizado onde cada um pode agir, se expressar e trabalhar sem ser controlado, até o presente, por nenhum estado ou empresa. Sobre esta infra-estrutura promissora, o comércio eletrônico tem um espetacular potencial econômico e, futuramente, vai representar um papel essencial na organização da sociedade.

Este desenvolvimento não está ocorrendo sem ameaças. Neste novo espaço revolucionário de comunicação, os riscos de fraudes, falsificações e espionagens, autorizadas pelo estado ou não, são imensos.

Portanto, pelo caráter de abertura irrestrita, a internet se torna o meio ambiente adequado a todas as formas de delitos ligados à informática. As mensagens, desejadas como sendo confidenciais, podem ser facilmente interceptadas, lidas, copiadas, adulteradas. Documentos ou informações sensíveis em circulação podem ser contestados em sua identidade. Informações sensíveis podem cair em mãos de concorrentes (no caso de empresas),

de agentes estrangeiros (para mensagens secretas diplomáticas ou militares secretas) ou em mãos criminosas, que buscam oportunidade para ganhos desonestos.

Estas ameaças contribuem para minar a confiança dos usuários desta nova plataforma de comunicação e dificulta o desenvolvimento de uma cultura digital que favoreça o uso da web de modo amplo, compreendendo o comércio eletrônico e os serviços bancários. A criptografia é a guardiã deste tesouro de comunicação sem fronteiras e tem a estratégica tarefa de garantir a segurança do sistema.

Invasão de privacidade - controle do Estado

Quando você usa seu telefone ou passa uma mensagem eletrônica por um computador, pode estar sendo gravado pelo dispositivo titânico denominado ECHELON. Todas as atividades mundiais de telecomunicações (telefone, fax e correio eletrônico) são vigiadas pelo ECHELON.

Os serviços secretos americanos estão à frente desta rede de escuta e são apoiados por diversos países aliados. Este é um grande conflito popular que discute o direito dos governos de controlar a intimidade das pessoas. O argumento do Estado é centrado na necessidade de vigiar ações terroristas, contrabando, venda de drogas etc. A discussão é boa. Será que a argumentação estatal é suficiente para justificar a existência do ECHELON? De que lado você fica:com a necessidade do estado ou com a política de Phill Zimmermann, que criou o PGP para permitir a qualquer cidadão comum, se o assim o desejar, guardar segredo sobre suas comunicações privadas?

De qualquer maneira e qualquer que seja a resposta, a criptografia é componente essencial para qualquer política sustentada de segurança.

O Computador Quântico

A partir do início de 1990, começa o trabalho de pesquisa para a construção de computadores quânticos e o desenvolvimento de uma criptografia quântica. Os primeiros ensaios experimentais são publicados por Charles H. Bennett, Gilles Brassard e colaboradores, relatando o uso de fótons para transmitir um fluxo de bits.

Em um computador quântico será extraordinária a velocidade. No momento, existem ainda dificuldades técnicas importantes até que possamos

ter à disposição estas máquinas. No entanto, o caminho é promissor e, em pouco tempo, o computador quântico pode ser realidade, oferecendo novos desafios à criptografia.

Depois de tudo que você caminhou e após esta visão panorâmica da proteção dada por métodos criptográficos, veja uma definição mais abrangente do que seja criptografia:

A criptografia é a área do conhecimento que trata do desenvolvimento de meios e métodos de transformação de dados destinados a cifrar o conteúdo, estabelecer a autenticidade e implementar técnicas de detecção de qualquer modificação não autorizada.

Caro(a) aluno(a), chegamos ao fim de nossa primeira disciplina. A idéia central foi dar uma visão histórica da Criptografia, partindo dos primeiros sinais registrados na pré-história até a atualidade. Neste caminho, percebemos a importância crescente que a Criptografia vem tendo ao longo dos tempos até se transformar, com o surgimento dos computadores e da internet, em uma área estratégica para a sociedade.

O objetivo foi relatar os fatos e motivar o assunto, uma vez que na próxima disciplina, Criptografia Geral, retomaremos os temas com ênfase nos aspectos técnicos da Criptografia e da Criptoanálise. Até a próxima jornada!

Resumo da Unidade 1

- Criptografia Esteganografia

Um dos objetivos básicos da criptografia é a segurança da informação.

Criptografia - modifica a mensagem de forma que somente o destinatário possa entendê-la.

Esteganografia - técnica que oculta a mensagem sem mudar seu estado original.

A criptografia e a esteganografia podem ser utilizadas juntas em certos casos.

- Com a criptografia, a mensagem não é compreensível por outra pessoa que não o destinatário. Para isso, esta é embaralhada com o uso de alguma técnica combinada entre o emissor e o receptor. Técnicas clássicas de embaralhamento: substituição e transposição.

- A utilização de recursos computacionais para armazenar, produzir e distribuir informações aumentou a preocupação com a segurança e com a vulnerabilidade dos sistemas computacionais que gerenciam estas informações.

- Segurança em rede - processo que previne e detecta qualquer uso não-autorizado de uma rede de computadores. Há ferramentas disponíveis para a segurança de uma rede e também para o ataque. Elas podem ser de dois tipos: aplicativos (software) e equipamentos (hardware).

- Técnicas de criptografia e ferramentas de segurança em rede são usadas no dia-a-dia, porém nem sempre são percebidas: na internet - verifica-se que o navegador está em modo seguro pelo endereço da página. HTTPS é uma combinação de HTTP (protocolo de transferência de arquivos hipertexto através da web) e de um protocolo de criptografia chamado SSL.

no email – Phil Zimmermann, engenheiro de software americano, criou o PGP (Pretty Good Privacy), programa de segurança para correio eletrônico, livremente disponível. O programa combina IDEA, protocolo de criptografia de chave privada, com o RSA, protocolo de chave pública. O PGP é o software de criptografia de email mais utilizado no mundo.

- Ataques e condutas que comprometem a segurança da informação:

• violação de segredo ou privacidade

• passar-se por outra pessoa

• negar responsabilidade por informação originada

• negar recebimento de informação

• falsear informação recebida

• troca de informação

• impedir que uma informação seja disponibilizada ou transmitida entre duas pessoas

- Categorias de ataques:

Interrupção - a informação não chega ao destinatário, pois é interceptada ou destruída.

Interceptação - acesso não autorizado à informação.

Modificação - ocorre acesso não-autorizado com modificação da informação.

Fabricação - inserção de uma informação falsa no sistema.

- Ataques passivos e ativos: dois tipos de atacar uma rede ou um sistema de segurança de informação em relação à intervenção que é feita.

- Serviços oferecidos por sistemas criptográficos:

confidencialidade ou sigilo, autenticidade, integridade, não-repúdio, controle de acesso e disponibilidade.

- Sistema seguro é aquele que faz tudo o que foi projetado para fazer e nada que não tenha sido determinado para efetuar, mesmo que seja forçado.

- Modelo de Segurança consiste em uma mensagem que é transmitida entre duas partes através de um canal de comunicação. Só é possível obter um canal seguro se ambas as partes concordam com a adoção de mecanismos de segurança.

Resumo da Unidade 2

Criptografia:

Na Antiguidade: foram desenvolvidos dois métodos para ocultar mensagens: a transposição – o Scytale – e a substituição – o Código de César.

Na Idade Média: todos os sistemas de códigos utilizados neste período eram construídos através de cifragens monoalfabéticas. Uma cifra monoalfabética é construída ao fazer corresponder cada letra distinta do alfabeto exatamente a um símbolo distinto.

- Na Idade Antiga e na primeira metade da Idade Média dominam as cifragens monoalfabéticas. Nesta época eram praticados dois métodos de decifragem: o método da força bruta e o da palavra provável.

- A Itália foi um dos primeiros países a ver, com profissionalismo e como questão de estado, o uso da criptografia. Este momento da história italiana coincidiu com as primeiras manifestações do Renascimento.

Na Idade Moderna: a grande novidade na criptografia ocorre em 1580, com a invenção da cifra de Vigenère. A partir do fim do século XVI, a França consolida sua liderança na criptologia.

- Em 1470, Leon Battista Alberti cria a primeira cifra polialfabética. Ele também introduz um princípio de mecanização no processo ao criar um disco de cifragem. Apesar de representar o primeiro avanço significativo em um período de quase 800 anos, Alberti não foi capaz de organizar uma cifra que resistisse à análise de freqüências.

- Em 1523, Blaise de Vigenère publica o livro "Tratado das cifras", no qual aprofunda as idéias de Alberti, criando uma nova cifra que permaneceria indecifrável durante quase toda a Idade Moderna, até tombar sob o ataque de Babbage e Kasisk, em 1854.

- A quebra da cifra de Vigenère foi uma realização extraordinária da criptoanálise e o primeiro resultado relevante depois da criação da análise de freqüência pelos árabes.

- Em 1844, Samuel Morse desenvolve o código que recebeu seu nome e inventa o telégrafo. A invenção altera profundamente a criptografia e torna a cifragem uma necessidade quase absoluta.

- O físico italiano Guglielmo Marconi, em 1894, realiza experiências com circuitos elétricos e inventa o rádio. Pela primeira vez, a criptografia enfrenta um desafio sem precedentes: a facilidade da comunicação permite que a mensagem até o destinatário seja quase sempre interceptada pelo inimigo. Era a comunicação aberta e a distância lançando as primeiras sementes da globalização.

- Na História recente: o desenvolvimento da criptografia desde a antiguidade até a atualidade é marcado por três grandes fases: artesanal, mecânica e digital.

- A fase artesanal registra as primeiras manifestações históricas da criptografia e coincide com o advento da escrita, cobrindo as Idades Antiga e Média. No início da Idade Moderna, com a invenção da Imprensa, aparecem os primeiros indícios da fase mecânica da criptografia.

- Com a Revolução Industrial, a invenção do telégrafo e do rádio, a fase mecânica se desenvolve e seu apogeu ocorre com as máquinas de cifragens usadas durante a Segunda Guerra Mundial: a máquina alemã Enigma é a mais ilustre representante e marca um ponto de inflexão entre a criptografia antiga e a moderna.

- A construção dos primeiros computadores abriu novos horizontes para a criptografia e marca o início do uso de métodos matemáticos relevantes para a construção de códigos.

- Em 1974, a IBM apresenta à agência oficial americana NBS (National Bureau of Standards) uma cifra que alguns pesquisadores vinham desenvolvendo desde 1960. A NBS avalia o algoritmo com a ajuda da NSA (National Security Agency), introduz algumas modificações e adota o código como padrão de cifragem de dados para os Estados Unidos. O código passou a ser conhecido como DES (Data Encryption Standard).

- O DES é o algoritmo criptográfico mais usado atualmente no mundo. Atende a bancos, órgãos de defesa, grandes companhias e ao comércio eletrônico. Funciona com chave simétrica (chave privada) de 56 bits, sendo extremamente difícil de ser quebrado. Ainda que seja muito seguro, certas empresas

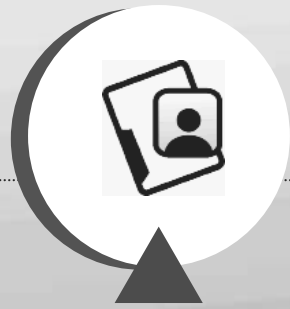
e bancos preferem usar o duplo-DES ou o triplo-DES, que é exatamente um código no qual a rotina do algoritmo é aplicada duas ou três vezes.

- Na atualidade: a criptografia se firma como uma importante ferramenta em auxílio à necessidade de troca de informações com segurança, em um mundo cada vez mais globalizado.

- Em 1991, Philip R. Zimmermann apresenta o PGP (Pretty Good Privacy), sistema criado por ele, que se torna um marco na popularização da criptografia e incomoda o governo americano.

- A partir de 1990 começa o trabalho de pesquisa para a construção de computadores quânticos e o desenvolvimento de uma criptografia quântica. Atualmente, existem dificuldades técnicas, porém o caminho é promissor e o computador quântico pode ser realidade em pouco tempo, oferecendo novos desafios à criptografia.

Autores



Celso José da Costa

Professor titular do Departamento de Geometria do Instituto de Matemática da Universidade Federal Fluminense (UFF), onde trabalha desde 1981. Bacharel em Matemática pela Universidade Federal do Rio de Janeiro (UFRJ), o prof. Celso Costa é Mestre e Doutor em Matemática pelo Instituto de Matemática Pura e Aplicada (IMPA). É coordenador do Núcleo de Educação Assistida por Meios Interativos (NEAMI), órgão responsável pela Educação a Distância na UFF, e vice-presidente do Consórcio CEDERJ. Professor responsável pelo conteúdo da Unidade 2 desta disciplina.

Luiz Manoel Silva de Figueiredo

Professor adjunto da Universidade Federal Fluminense (UFF), onde leciona desde 1992. Bacharel em Física pela Universidade Federal do Rio de Janeiro (UFRJ), o prof. Luiz Manoel Figueiredo é Mestre em Matemática pelo Instituto de Matemática Pura e Aplicada (IMPA) e Doutor em Matemática pela University of Cambridge (Reino Unido). Sua área de doutorado é em teoria dos números e atualmente trabalha com Criptografia. Professor responsável pelo conteúdo da Unidade 1 desta disciplina.

Referências bibliográficas

CARVALHO, Daniel Balparda de. **Segurança de dados com criptografia**: métodos e algoritmos. Rio de Janeiro: Book Express, 2001.

MENEZES, A. J. et al. **Handbook of applied cryptography**. Boca Raton, FL.: CRC Press, 1997.

SINGH, Simon. **O livro dos códigos**. Rio de Janeiro: Record, 2001.

STALLINGS, William. **Cryptography and network security**: principles and practice. 2.ed. Prentice Hall, 1999.

TERADA, Routo. **Segurança de dados**: criptografia em redes de computador. São Paulo: Edgard Blücher, 2000.

TZU, Sun. **A arte da guerra**. São Paulo: Paz e Terra, 1996.

Sites consultados

http://adorocinema.cidadeinternet.com.br/filmes/enigma/enigma.htm

http://www.numaboa.com.br/criptologia/cifras/transposicao/scytale.php

http://www.numaboa.com.br/criptologia/historia/media.php

http://www.temakel.com/histenigma.htm

Complemente seu estudo

Leituras

KAHN, David. The Codebreakers. Nova York: Macmillan, 1967.

PAINE, Stephen; BURNETT, Steven. Criptografia e Segurança: o guia oficial RSA. Rio de Janeiro: Editora Campus, 2002.

SINGH, Simon. O livro dos códigos. Rio de Janeiro: Record, 2001.

Websites

http://www.ajc.pt/cienciaj/n32/escrita.php

http://fma.if.usp.br/convite/coloquios/Criptografia.html

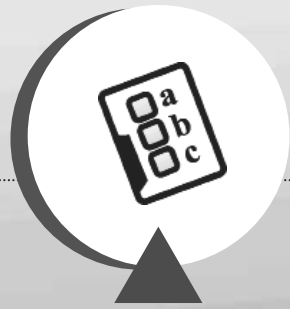
http://www.numaboa.com.br/criptologia/historia/media.php

http://www.swimmer.org/morton/enigma.html

http://www.temakel.com/histenigma.htm

Complemente seu estudo

Glossário



Criptoanálise - é a área do conhecimento que trata do ato de decifrar ou "quebrar" o sistema criptográfico.

Criptografia - é a arte de disfarçar uma informação de forma que apenas a pessoa certa possa entendê-la. Este tem sido um dos grandes instrumentos de proteção da informação.

HTTP (Hypertext Transfer Protocol) - é o protocolo de transferência de arquivos hipertexto (textos com links, figuras etc.) através da internet.

HTTPS - é uma combinação de HTTP e de um protocolo de criptografia chamado SSL.

Escrita cuneiforme – criada pelos sumérios (povo estabelecido na Babilônia no século IV a.C.), era simultaneamente ideográfica e fonética. Cada signo correspondia a um objeto e, posteriormente, passou a representar o som respectivo deste objeto.

Escrita demótica – trata-se de uma escrita cursiva, simples, usada em cartas, em registros e documentos, comum no dia-a-dia. Era gravada normalmente no papiro.

Escrita hierática - forma cursiva de escrita, usada pelos sacerdotes em textos sagrados. Era gravada em papiro, madeira ou couro.

Esteganografia – técnica de transmissão secreta que oculta a mensagem, sem mudar seu estado original. Trata-se de um modelo rústico e precursor da Criptografia.

Segurança da informação – é a proteção da informação contra o acesso não autorizado, evitando assim sua modificação ou destruição.

Segurança em rede - é o conjunto de instrumentos usados para proteger um sistema computacional. Proteger um computador e uma rede não são duas tarefas distintas, com ferramentas próprias. Hoje as redes estão em todo lugar e não existem fronteiras bem definidas entre esses dois objetivos.

Sniffers - são programas que escutam todo ou parte do tráfego de dados de uma rede, buscando informações importantes, como logins e senhas.

Spyware - programas que, quando colocados em um computador, passam a reunir secretamente informações sobre os hábitos dos usuários e as transmitem para outras pessoas.

SSL (Secure Socket Layer) - é o protocolo utilizado para comunicação segura, autenticação e criptografia sobre redes.

Umbral – local de entrada

Gabarito das atividades

Unidades 1 e 2

Unidade 1

Aula 1

1) As duas formas de proteção da mensagem estão claramente presentes. O fato da mensagem ser codificada, isto é, criptografada, indica que foi usada criptografia. Como a mensagem foi oculta em uma cápsula sob a pele do portador, houve uso de esteganografia.

2) Há várias maneiras de responder a esta pergunta. Em linhas gerais, podemos dizer que atualmente a informação tende a ser guardada em meio eletrônico, com o uso de computadores, e disponibilizada por meio de processos de comunicação através de redes de computadores. A proteção desta informação contra o acesso não autorizado implica na proteção destas redes de computadores. Assim, podemos dizer que a área de segurança computacional está diretamente envolvida na segurança da informação.

3) Esta é uma questão de opinião pessoal. Há pessoas que acham que todos devem ter direito a comunicar-se com garantia de sigilo. Estas pessoas acham que nem mesmo os órgãos de segurança deveriam ter acesso irrestrito aos nossos emails, telefonemas etc.

Outras pessoas acham que, em um mundo sob constante ameaça de terroristas, em uma sociedade que sofre enormemente com a corrupção e o tráfico de drogas, os serviços de segurança de governo podem acessar todas as comunicações dos cidadãos. A per-

da potencial de privacidade é compensada pela maior segurança que o governo pode dar a seus cidadãos.

Bem, há quem defenda enfaticamente cada uma das duas opiniões expressas acima.

Aula 2

1) a) É um ataque de interceptação. Foi violada a confidencialidade dos emails do colega.

b) Foi um ataque de modificação. A informação foi acessada e alterada pelo invasor.

2) Nos dois tipos de ataque há participação de um atacante. A diferença está em que um atacante passivo apenas ganha acesso à informação, não a modifica ou interrompe seu fluxo normal. Um atacante ativo, além de acessar a informação, modifica-a ou interrompe seu fluxo, ou ainda fabrica informação indevidamente.

Aula 3

1) Os serviços descritos nesta aula – confidencialidade, autenticidade, integridade, não-repúdio, controle de acesso e disponibilidade – são serviços normalmente requeridos por sistemas que armazenam informação e devem permitir seu acesso a agentes autorizados, ou ainda por sistemas destinados à comunicação de informações.

A necessidade dos serviços descritos ocorre em maior ou menor grau, dependendo da aplicação.

Aula 4

1) Na verdade, a troca de emails com mensagem não criptografada provê de pouca segurança. Há confidencialidade e integridade (ninguém deve poder ler ou alterar os emails) com o controle de acesso por senha ao servidor de emails, mas se este servidor for atacado, por exemplo, as mensagens podem ser lidas no servidor.

Não há garantia de autenticidade, uma vez que é relativamente fácil forjar um remetente em uma mensagem de email. Também não há garantia de que o destinatário de fato leu a mensagem.

O uso de um sistema de criptografia de emails, como o PGP, aumenta consideravelmente a segurança no uso de emails.

2) A compra em um site seguro usa um protocolo de criptografia na transmissão de dados, como o número do cartão de crédito. Isto aumenta bastante a confidencialidade e integridade da informação, visto que caso a mensagem seja interceptada em trânsito, não haverá como decifrá-la.

Unidade 2

Aula 5

1) Nevou em Curitiba o ano passado.

Aula 6

2) "L Q L H K F Q E M F P F S L T L Q"

Aula 7

3) "Após a Tempestade vem a bonança.

Aula 9

4) "CRIPTOGRAFIA"

Créditos

UNIVERSIDADE FEDERAL FLUMINENSE - UFF
EXÉRCITO BRASILEIRO - EB

Coordenação Geral
Antônio Carlos Guelfi
Paulo Gil Teixeira

Coordenação do Curso
Luiz Manoel Silva de Figueiredo

Coordenação Pedagógica
Caubi de Alcântara
Rogério Guimarães de Gusmão

Administração e Logística
Centro de Estudos de Pessoal - CEP

Equipe didático-pedagógica
Mônica Nogueira da Costa Figueiredo
Vanessa Maria Barbosa

Edição-Livro didático

Professores autores
Celso José da Costa
Luiz Manoel Silva de Figueiredo

Capa
Maria Rachel Barbosa

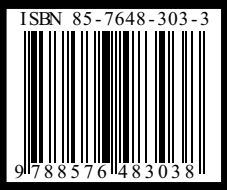
Projeto Gráfico
Maria Rachel Barbosa

Diagramação
Maria Rachel Barbosa
Rafael Fontenele

Revisão
Letícia Maria Lima Godinho
Vanessa Maria Barbosa

Impressão
Armazém das Letras
Gráfica e Editora
Tel: 3860-1903

ISBN 85-7648-303-3



UENF
Universidade Estadual
do Norte Fluminense

UERJ
UNIVERSIDADE DO ESTADO DO RIO DE JANEIRO

Universidade Federal Fluminense
uff

Universidade Federal Rural
do Rio de Janeiro

UNIRIO

FAPERJ
Fundação Carlos Chagas Filho de Amparo
à Pesquisa do Estado do Rio de Janeiro

GOVERNO DO
Rio de Janeiro
SECRETARIA DE
CIÊNCIA E TECNOLOGIA

UAB
UNIVERSIDADE
ABERTA DO BRASIL

Ministério
da Educação

BRASIL
UM PAÍS DE TODOS
GOVERNO FEDERAL