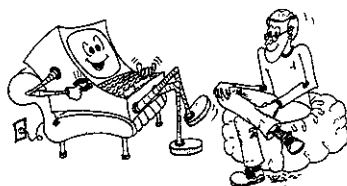

Criptografia e a importância das suas aplicações



Routo Terada
IME-USP

“A engenhosidade humana não pode arquitetar uma escrita secreta que a própria engenhosidade humana não possa resolver.”

Edgar Allan Poe

O meio de comunicação digital controlado por computadores trouxe flexibilidade e eficiência em gravação, recuperação e distribuição de informação. Várias aplicações, nesse meio, estão sendo implantadas em diversos países, com sucesso. Podemos citar, como exemplos, sistemas de transações bancárias *online*, sistemas de consulta a informações nos próprios lares (videotexto), sistemas de compras a distância (tele-shopping), sistemas de consultas a bancos de dados via satélite, correios eletrônicos, etc.

Atualmente, são comuns os chamados Caixas Automáticos ou ATMs (de Automatic Teller Machines), nos quais os clientes de bancos podem efetuar pagamentos, saques e transferência de fundos através de um simples cartão plástico, a qualquer hora do dia ou da noite.

Em futuro próximo, transferência de informações serão rápidas e baratas através de correios eletrônicos, em que será possível, por telefone, inserir uma mensagem ou carta num dispositivo e discar um número. O telefone no outro extremo, imprimirá a mensagem imediatamente. Por meio de sistemas de videotexto, uma pessoa em sua casa, poderá consultar horários de vários eventos, como espetáculos de arte, visitas a hospitais, ou reservar ingressos e passagens de algum meio de transporte, ou mesmo, movimentar sua conta bancária.

Estes são apenas alguns exemplos que ilustram como o avanço da eletrônica, nos últimos anos, está permitindo comunicações rápidas, precisas, de custos sempre decrescentes, e confortáveis, entre pessoas ou computadores distantes ou próximos.

Mas, simultaneamente, alguns problemas inerentes surgiram. Transações são agora compostas de sinais digitais que podem ser modificados facilmente, sem deixar pistas. Por exemplo, a flexibilidade, que aumenta a produtividade de um correio eletrônico, ao mesmo tempo dificulta a verificação da autenticidade de transações e documentos. Muitos usuários, em vários locais, têm acesso ao sistema e existem usuários para os quais a segurança das informações é vital, e outros para os quais ela é de pouca ou nenhuma importância. Em consequência, informações podem ser roubadas, falsificadas ou danificadas, entre dois pontos quaisquer de um sistema. A privacidade é também ameaçada, pois informações são disseminadas publicamente, em forma captável por instrumentos eletrônicos.

Segurança refere-se à proteção contra a disponibilidade, acidental ou intencional, de informações para pessoas desautorizadas, e proteção contra modificações e destruições desautorizadas.

Privacidade se refere ao direito de indivíduos, ou organizações, de determinar quando, como, e em que extensão as informações, sobre eles, podem ser transmitidas a outros.

Fraudes

Recentemente, tornam-se cada vez mais frequentes as notícias de quebra de segurança e privacidade em sistemas de informação controlados por computador. Por exemplo, em junho de 1983, o sistema VAX 115780 do Centro Hospitalar Sloan-Kettering, em Manhattan, que efetua monitoria de tratamentos de câncer por radiação, sofreu alterações feitas, via linha telefônica, por rapazes que vivem na região de Milwaukee (Estado de Wisconsin), conhecidos por "414 Gang", pois 414 é o código de área da região. Em novembro de 1984, o semanário satírico francês *Le Canard Enchaîné*, editado em Paris, contratou um "técnico mediano" que, usando um microcomputador distribuído pelo sistema postal francês, penetrou nos segredos nucleares do país, armazenados no International Company for Computer Services (CISI, na sigla em francês). O semanário diz que seu objetivo foi testar o sistema de segurança do CISI. Em 1986, um funcionário de uma corretora em Denver nos EUA, por meio, de simples mudança de algumas letras na tela do computador, foi capaz de multiplicar por dez os preços das ações da Loren Industries. Em 1987, a Volkswagen AG, na Alemanha Ocidental, sofreu uma perda de 259 milhões de dólares que tinham sido "mascarados" por alterações de programas e fitas magnéticas de computador.

No Brasil, as fraudes com computadores talvez já se tenham tornado uma rotina. As vítimas é que não gostam de divulgar, embora procurem informar-se sobre todos os métodos de proteção e segurança modernos. Aqueles que ainda não sofreram acidentes acham que não existem no país indivíduos tão sofisticados que possam furtrar, alterar ou inserir informações falsas em redes de computadores. É enganoso supor, no entanto, que tais eventos só ocorrem na ficção, como no filme *War Games*, em que um rapaz acidentalmente, se intromete num sistema computacional, quase provocando a eclosão de uma guerra mundial. Em maio de 1986, por exemplo, um banco sofreu uma perda de dois milhões e meio de cruzados provocada por indivíduos em uma microcentral telefônica, instalada em uma perua em Guarulhos, SP. Eles descobriram os códigos e interferiram no sistema de computação do Banco, conseguindo gerar ordens de pagamento falsas.

Portanto, à medida que se intensificam as transmissões de numerosas informações (como transferência de fundos, registros financeiros, médicos, militares, etc.) através de meios eletrônicos (satélites, linhas telefônicas, fitas magnéticas, etc.), as possibilidades de quebra de segurança ou de privacidade crescem dramaticamente. Desejamos que as informações possam ser trancadas em computadores, de uma maneira tão segura quanto documentos em cofres bancários. No entanto, os dados em muitos sistemas eletrônicos não podem ser considerados em alto nível de segurança porque, infelizmente, não se tem desenvolvido nenhum mecanismo eficiente de proteção física em meios eletrônicos.

Uma maneira fraca de limitar o acesso físico às informações, ou recursos valiosos, tem sido o uso de palavras-senha, juntamente com perguntas sobre características exclusivas do usuário autorizado (além de outros meios físicos de proteção). Em 1983 e 1984, propusemos métodos para restringir acessos a informações, nos artigos "Senhas Criptografadas, com Assinatura Eletrônica" e "Um Esquema Criptográfico para Autenticação de Usuários", no Congresso Nacional de Informática.

Afirmamos, porém, que os problemas de segurança e privacidade não são inteiramente solucionados desta maneira pois, após obter o acesso físico das informações (uma simples cópia de fita magnética ou detecção de linha telefônica ou radiofônica, para citar alguns exemplos), um indivíduo desautorizado atinge integralmente os seus objetivos. Ademais, possivelmente, este crime não deixará vestígios ou pistas!

Criptografia

No Brasil, só recentemente tem havido interesse por uma maneira complementar de evitar tais violações dos sistemas eletrônicos e proteger informações sigilosas: o uso de *Criptografia e cripto-sistemas*.

A maneira mais segura de ter uma garantia de que informações transmitidas não serão copiadas, modificadas ou falsificadas é o uso de Criptografia.

Criptografia consiste em codificar informações, usando-se uma chave, antes que estas sejam transmitidas, e em decodificá-las, após a recepção.

O *processo de codificação* nada mais é do que uma transformação completa dos dados, de tal modo que uma pessoa desautorizada (que não conheça a chave usada na transformação) não possa obter a informação original a partir do código. Desta maneira, mesmo que uma pessoa desautorizada consiga obter uma cópia das informações, elas estarão codificadas e serão ininteligíveis e, portanto, inúteis para esta pessoa.

Atualmente, a Criptografia é aplicada em várias áreas. Podemos citar, por exemplo:

- Recursos humanos: auditoria eletrônica e lacre de arquivos de pessoal e pagamentos;
- Compras e vendas: autenticação de ordens eletrônicas de pagamento;
- Jurídico: transmissão digital e custódia de contratos;
- Automação de escritórios: autenticação e privacidade de informação.

Cifras one-time pad

A Criptografia tem sido usada, desde a época dos antigos chineses, por espões, amantes e manipuladores políticos. Há uma literatura variada a respeito, principalmente após o advento do rádio, e têm havido investimentos significativos neste assunto, nas áreas militares, diplomáticas e de serviços secretos. Edgar Allan Poe, que se considerava um cripto-hábil, estava convencido de que nenhum esquema criptográfico “inquebrável” poderia ser inventado.

Poe certamente estava errado; criptografias, chamadas simplesmente “cifras”, que são inquebráveis têm sido usadas por mais de meio século. São as chamadas cifras “one-time pad”, que são usadas apenas uma vez para cada mensagem. Um exemplo simples é a chamada “Cifra de César”, porque o famoso Júlio César a utilizava.

A “*Cifra de César*” consiste no seguinte: Fixa-se um número t , entre 0 e 26, como chave. Estabelece-se uma correspondência entre símbolos (letras e espaços) e números, pela tabela:

espaço □	A	B	...	J	K	L	...	Y	Z
00	01	02	...	10	11	12	...	25	26

Substitui-se um símbolo na mensagem recebida, correspondente ao número m por esta tabela, pelo símbolo correspondente ao número c , também entre 0 e 26, dado por

$$c \equiv m + t \pmod{27} \quad (1)$$

Assim, por exemplo, para $t = 12$,

a mensagem cifrada X G H C O T O V F T V C
deve ser lida como I S T O É G R E G O .

A cifra “one-time pad” consiste em escolher, ao acaso, uma chave t para cada símbolo na mensagem. Mesmo intuitivamente, não é difícil compreender que o “one-time pad” é inquebrável pois, como qualquer chave t escolhida ao acaso é válida, em consequência qualquer símbolo pode substituir um símbolo na mensagem. Quando o agente secreto russo Rudolf Abel foi capturado em Nova York, em 1975, possuía uma seqüência de chaves “one-time pad”, do tamanho de um selo postal, no seu bolso. E o famoso telefone “vermelho” entre Washington e Moscou utiliza “one-time pad” através de seqüências de chaves trocadas periodicamente entre as embaixadas.

O único inconveniente prático do “one-time pad” é exatamente o fato de ser necessária a comunicação secreta e prévia de longas seqüências de chaves. Existem histórias espetaculares ocorridas na Segunda Guerra Mundial sobre “quebra” de códigos inimigos. Recomendamos, entre outros, o livro *The Codebreakers, the Story of Secret Writing*, escrito por D. Kahn em 1967 (Macmillan New York).

A Criptografia é uma “luta” entre a pessoa que codifica e a pessoa desautorizada, que tenta “quebrar” o código. Nesse sentido, a pessoa desautorizada é um “inimigo” a ser combatido com as melhores “armas” disponíveis. Este tópico tem se desenvolvido substancialmente com o advento dos computadores pois a Criptografia é uma forma especial de computação.

Os métodos clássicos de Criptografia, como a de César, são todos simétricos, isto é, a chave usada pela transmissora para codificar mensagens é igual à chave usada pela receptora para decodificar as mensagens recebidas. Mesmo a tecnologia mais moderna — como o sistema Data Encryption Standard, de janeiro de 1977, da National Bureau of Standards, ou o sistema Lúcifer da IBM — faz uso de métodos simétricos.

Chaves públicas

Recentemente, houve um verdadeiro salto no avanço da Criptografia, provocado pela definição de um conceito teórico, denominado *cripto-sistemas com chaves públicas*, por Diffie e Helman.

Denominaremos este conceito modelo *CP*. Como o próprio nome indica, no modelo *CP* existem chaves de conhecimento público; mais precisamente, a chave da transmissora é pública, e é, naturalmente, *diferente* da chave (secreta) da receptora. Portanto, o modelo *CP* possui estrutura *assimétrica*. Mais recentemente, a definição do modelo *CP* foi integralmente fundamentada pela apresentação de várias realizações do modelo.

Estas realizações foram inventadas num intervalo de tempo relativamente curto, de 1976 a 1980, e os seus autores foram, em parte, inspirados pela extrema elegância do modelo *CP* (*).

Um exemplo de realização do modelo *CP* é o chamado Sistema *RSA*, iniciais dos nomes dos autores *Rivest*, *Shamir* e *Adleman*, professores de Ciência da Computação no Massachusetts Institute of Technology(**). Considerando-se o processo mais rápido que se conhece para “quebrar” o sistema *RSA* e, utilizando-se os computadores mais rápidos existentes, seriam necessários 74 anos de cálculos ininterruptos para deduzir a chave constituída por apenas 50 algarismos decimais.

No sistema *RSA*, as chaves do transmissor (t) e do receptor (r) são diferentes e as expressões que substituem a função em (1) são mais complicadas. Aqui, elas envolvem blocos de símbolos, ao invés de tradução símbolo por símbolo, e potência ao invés da soma.

A chave t é pública, bem como um número n . A chave secreta r e os números n e t devem satisfazer:

- (i) $n = p \cdot q$, com p e q números primos;
- (ii) $t \cdot r \equiv 1 \pmod{[(p-1)(q-1)]}$;
- (iii) r e $(p-1)(q-1)$ são primos entre si.

Ilustremos o sistema *RSA* com um exemplo fictício (fictício, porque, na prática, o número n deve ser muito grande):

O transmissor tem a chave pública $t = 7$ e o número $n = 22$.

O receptor tem a chave secreta $r = 3$ e o número $n = 22$.

O leitor deve se certificar de que as condições (i), (ii) e (iii) estão satisfeitas.

Suponhamos que a mensagem a ser transmitida seja apenas a letra I . Esta é a 9ª letra do alfabeto, portanto a ela corresponde o número 9.

O transmissor, usando $t = 7$ e $n = 22$, transforma 9 em “ $9^7 \pmod{22}$ ”. Existem algoritmos simples que fazem este cálculo:

$$9^7 \equiv 15 \pmod{22}.$$

Portanto, o transmissor envia “15”.

O receptor, usando a chave secreta $r = 3$, calcula “ $15^3 \pmod{22}$ ”, o que dá 9, e fica sabendo que a letra transmitida foi I .

Em geral, o transmissor transforma o número α a ser transmitido em $\beta \equiv \alpha^t \pmod{n}$. O receptor calcula $\gamma \equiv \beta^r \pmod{n}$. Um dos teoremas de Fermat garante que, nas condições (i), (ii) e (iii), $\gamma = \alpha$.

Como, após o cálculo da chave secreta r , os números p e q são apagados no computador, o leitor pode verificar que um modo de “quebrar” o sistema (isto é, de calcular a chave r , secreta, a partir do conhecimento da chave pública t e do valor de n) é fatorar n em primos e depois procurar r que

(*) Publicado, em 1976, com o título *New Directions in Cryptography*, em IEE Transactions in Information Theory, novembro de 1976.

(**) *On Digital Signatures and Publickey Cryptosystems*, MIT Technical Memo 82, abril, 1977.

satisfaça (ii), o que pode ser feito através de uma modificação do Algoritmo de Euclides.

O ponto importante nesse procedimento é que, até hoje, não se conhece um algoritmo rápido para a decomposição de n em fatores primos. Por meio do algoritmo de Schroeppel, o mais rápido conhecido hoje, usando-se um computador capaz de efetuar uma multiplicação em um microssegundo (10^{-6} seg), o tempo para “quebrar” o sistema, em termos do número de algarismos de n , é dado na tabela abaixo:

nº de algarismos de n	tempo necessário para “quebrar” o <i>RSA</i>
50	3,9 horas
75	104 dias
100	74 anos
200	$3,8 \times 10^7$ séculos
300	$4,9 \times 10^{13}$ séculos
500	$4,2 \times 10^{23}$ séculos

O comprimento recomendado para se obter uma boa margem de segurança é o de 200 algarismos para n .

Para o professor de Matemática, é oportuno salientar que resultados sobre números primos e congruências, que, durante tanto tempo, tinham sua importância restrita à Teoria dos Números, passaram a representar um instrumento precioso para o cálculo destas chaves e para a verificação das propriedades de um modelo *CP*. Técnicas, outrora desenvolvidas na busca de provas do Teorema de Fermat, têm hoje valor prático na construção de algoritmos.

Assim é que a Criptografia, ao mesmo tempo que se serve da Teoria dos Números, propiciou um novo impulso ao seu desenvolvimento, acrescentando-lhe, ainda, novas técnicas de abordagem.

A Criptografia está vivendo um período bastante frutífero e útil, em conexão com a subárea da Ciência da Computação denominada Complexidade de Computação. Certamente, estamos testemunhando e contribuindo para o desenvolvimento acelerado de aplicações, tanto militares quanto civis e comerciais.

Routo Terada é Professor Livre-Docente do Instituto de Matemática e Estatística da Universidade de São Paulo. Formado em Engenharia Eletrônica pela Politécnica da USP, obteve o grau de Mestre em Matemática Aplicada pelo Instituto de Matemática e Estatística da USP e o grau de Ph. D. em Ciência da Computação pela Universidade de Wisconsin-Madison. Suas áreas de pesquisa incluem Teoria de Computação, Otimização Combinatorial, Criptografia e Compiladores.
