CRIPTOGRAFIA

.

Introdução

" *As bases materiais históricas dessa mistificação (* ***o discurso único do mundo*** *) estão na realidade da técnica atual. A técnica apresenta-se ao homem comum como um mistério e uma banalidade. De fato, a técnica é mais aceita do que compreendida. Como tudo parece dela depender, ela se apresenta como uma necessidade universal, uma presença indiscutível, dotada de uma força quase divina à qual os homens acabam se rendendo sem buscar entendê-la. É um fato comum no cotidiano de todos, por conseguinte, uma banalidade, mas seus fundamentos e seu alcance escapam à percepção imediata, daí seu mistério. Tais características alimentam seu imaginário, alicerçado nas suas relações com a ciência, na sua exigência de racionalidade, no absolutismo com que, ao serviço do mercado, conforma os comportamentos; tudo isso fazendo crer na sua inevitabilidade.*

Quando o sistema político formado pelos governos e pelas empresas utiliza os sistemas técnicos contemporâneos e seu imaginário para produzir a atual globalização, aponta-nos para formas de relações econômicas implacáveis, que não aceitam discussão e exigem obediência imediata, sem a qual os atores são expulsos da cena ou permanecem escravos de uma lógica indispensável ao funcionamento do sistema como um todo. ***"***

SANTOS, Milton. POR UMA OUTRA GLOBALIZAÇÃO. 9ª ed. Rio de Janeiro: Record, 2002.

A criptografia tem sido, por centenas – talvez milhares – de anos, vista como assunto de interesse exclusivo daqueles que exercem o poder, em especial o poder militar. Por isso mesmo, manteve-se limitada aos militares, enquanto aplicação, ou aos centros acadêmicos, enquanto conhecimento. Para os demais, manteve um pitoresco mistério, realimentado freqüentemente pelas estórias que nos são trazidas pela literatura ou pelo cinema e que, ainda hoje, prestam-se para nutrir e preservar àquela curta percepção.

Com o grande avanço tecnológico trazido pela criação do microchip, e a rápida evolução dos meios técnicos, as formas pelas quais as sociedades operam vem sofrendo profunda transformação. Entramos na " Era da Informação ", o que significa dizer, em última instância, que a informação representa papel chave no exercício do poder.

Novas formas de transmissão de informações surgiram, eventualmente tornando as anteriores obsoletas, mas freqüentemente integrando-se às formas preexistentes, adicionando potencialidades, dinamizando-as. Essa tecnologia, intrusora por natureza, termina por contribuir na modificação das próprias relações sociais. A noção de tempo, a percepção do espaço, são algumas das "vítimas ".

Toda transformação, entretanto, sofre resistência. É uma característica do ser humano rejeitar a mudança. E é possível constatar com facilidade que as nações mais desenvolvidas são, via de regra, aquelas que mais rapidamente adaptam-se a existência das novas tecnologias, criando os padrões pelos quais a técnica funcionará, as normas que regerão a sociedade no seu uso.

Para que uma sociedade possa diminuir a resistência natural a um determinado fator de mudança e tenha condições de debater se essa mudança é ou não desejável, e sob que condições deve ser implementada, é necessário que exista compreensão da sua existência, dos seus princípios, do seu alcance.

A criptografia deixou de ser aplicação exclusivamente militar e passou a fazer parte fundamental de toda uma gama de aplicações que são comuns ao cidadão das sociedades modernas, aplicações essas centrais à própria forma como essas sociedades operam. Operações bancárias e comércio eletrônico são exemplos típicos. Na era da informação, a tecnologia também se presta para a vigilância global de milhões de indivíduos por parte de governos. A criptografia vem a ser uma das principais ferramentas para a garantia da privacidade.

Faz-se necessário compreendê-la e, então, fazer uso das vantagens que ela tem a oferecer para a estruturação de uma sociedade mais moderna.

É no desejo de ampliar a capacidade de debate nas diversas questões onde a criptografia tem peso que a ESGE traz esta exposição, ao longo da qual procuraremos identificar algumas das variadas áreas onde encontra aplicação corrente, e demonstrar tendências futuras que dependem do seu conhecimento.

Para que alcancemos este objetivo, porém, será necessário dar aos participantes conhecimento teórico sobre seus princípios de funcionamento.

FUNDAMENTOS

Para estabelecer uma comunicação entre duas entidades quaisquer, são necessários três componentes básicos: um emissor, um receptor e o meio físico por onde os dados irão trafegar.

Suponhamos que alguém deseje enviar uma mensagem; suponhamos ainda que esse alguém não queira que qualquer um, capaz de interceptar a mensagem, tenha condições de lê-la. Entretanto, é preciso garantir que o destinatário da mensagem tenha acesso às informações ali contidas.

Será necessário, então, que remetente e destinatário tenham acertado entre si um modo exclusivo de acesso aos dados contidos na mensagem. Em outras palavras, é preciso que exista um conjunto de regras que, seguidas à risca, tornarão a mensagem disponível ao seu manipulador, e esse conjunto de regras precisa ser conhecido por ambas as partes.

Consideremos as seguintes possibilidades:

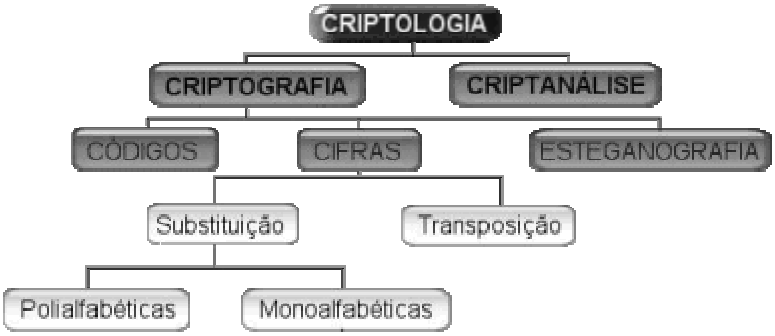
1- A mensagem pode ser enviada em claro, ou seja, contendo os dados na forma como foi redigida pelo emissor; a proteção ao seu conteúdo é definida pela forma como trafega no meio. Por exemplo: uma carta em um envelope pardo, levada por um mensageiro.
2- Pode-se usar da segurança pela obscuridade: a mensagem pode trafegar em claro, em um meio cujo volume de tráfego seja tão grande que dificulte a percepção de que a mensagem foi enviada. Por exemplo: um cartão postal simples, pelo correio.
3- O conteúdo da mensagem será "embaralhado", de forma que não possa ser interpretado corretamente sem que se tenha conhecimento de todos os processos e valores usados para faze-lo.

Podemos entender a Criptografia como o estudo das técnicas que visam transformar uma mensagem inteligível – denominada " texto em claro " – em uma que não poderá ser compreendida – o " criptograma " ou " texto cifrado " – senão pelo destinatário. Trata-se de um ramo dos estudos de linguagem, sendo considerada um ramo da Matemática.

Ao conjunto de regras a que nos referimos acima, chamaremos "algoritmo de encriptação ". Algoritmo, aliás, é um termo matemático entendido como um sistema particular de disposição que se dá a uma sucessão de cálculos numéricos.

Encriptação é o ato de converter o texto em claro em texto cifrado. Decriptação, o processo de recuperação do texto em claro à partir do texto cifrado.

Na matemática, a Criptografia completa-se com a Criptoanálise, que é o estudo das formas de recuperação do texto cifrado (decifração ou decriptação) sem que se tenha acesso aos processos e/ou valores normalmente necessários para faze-lo. A Criptologia é o ramo das linguagens que estuda os métodos – especialmente os matemáticos – de cifragem, do qual a Criptografia e a Criptoanálise são ramificações.



.

PROCESSOS HISTÓRICOS

São considerados processos históricos, os processos em que a segurança da mensagem baseia-se no segredo dos algoritmos. Embora obsoletos, sua compreensão é fundamental.

Sabe-se que Júlio César valeu-se de um sistema simples para enviar mensagens a seus oficiais. Naquele sistema, cada letra do alfabeto utilizado teria correspondência com o caractere que se localizava 3 posições a frente:

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

Chamamos este processo de substituição monoalfabética, porque para cada letra do alfabeto original, corresponde uma letra do alfabeto cifrado. Abaixo, vemos uma mensagem em texto claro, e após a sua cifragem:

I	s	t	o		é		u	m	a		m	e	n	s	a	g	e	m
M	V	X	R	C	H	C	Z	P	D	C	P	H	Q	V	D	J	H	P

Métodos de transposição: Consistem em trocar a posição dos caracteres da mensagem original de acordo com uma ordem pré-estabelecida. Por exemplo, podemos definir a seguinte tabela de transposição:

1	2	3	4	5	6	7	8
2	7	4	5	6	3	8	1

E teríamos então:

ISTOÉUMA MENSAGEM

AIUTOESM MMGNSAEE

Outras variantes do método de transposição:

1 – Escrever a mensagem de trás para a frente, reagrupando as letras:

MEGA SNEM AMU E OTSI

MEGA SNEM AMU EO TSI

2 – Separar a mensagem em pares de letras, escrevendo cada par de trás para frente, reagrupando em seguida:

IS TO EU MA ME NS AG EM

SI OT UE AM EM SN GA ME

SIOT UE AM EMSN GAME

3 – Escrever a primeira metade da mensagem com espaço entre as letras, e inserir a Segunda metade nos espaços. Após, reagrupar as letras.

I S T O E U M A
M E N S A G E M

IMSET NOSEA UGM EAM

Vários outros processos de "embaralhamento" alfabético foram desenvolvidos e empregados. Como se vê, trata-se de aplicar um conjunto de regras (protocolo) sobre a mensagem que se deseja enviar, para cifrar, e de aplicar o inverso do processo, para decifrar.

A inviolabilidade da mensagem depende, portanto, do segredo do processo utilizado. A descoberta do algoritmo implica na sua impossibilidade de uso. Para seu emprego, é necessário haver, inicialmente, contato direto entre as duas partes (emissor e receptor), ocasião em que será definido o processo a ser empregado.

Algumas questões devem ser observadas em relação ao uso: Deve-se, por exemplo, evitar o uso de sinais de pontuação, assim como diferenciar letras maiúsculas de minúsculas; a mensagem não deve ser "formatada" (por exemplo, uma carta costuma ter, no cabeçalho, o local de origem e a data em que foi escrita.).

Introduzindo as Chaves

Apesar de terem mantido bom grau de eficiência por longo período, os processos até aqui mencionados apresentavam alguns problemas que limitavam muito o seu emprego. O fato do sigilo encontrar-se no método escolhido tinha como conseqüência a impossibilidade de continuar usando aquele algoritmo, caso fosse descoberto. E o risco de que isso acontecesse levava à necessidade de se variar o processo de cifragem com freqüência. Por isso, era necessário manter um considerável número de variações possíveis nos processos. Além disso, a captura de um criptografista na linha de frente representava a provável descoberta, por parte do inimigo, dos processos em uso.

Além disso, somava-se outro inconveniente. Recuperar a mensagem original à partir do texto cifrado era um problema tão mais complexo quanto

mais elaborado fosse o algoritmo escolhido. Isso aumentava a possibilidade de incorreções, e aumentava o tempo da operação. Os criptografistas, não raro, procuravam valer-se de livretos com os alfabetos de origem, pranchetas com tabelas, cartões-código e outros " facilitadores ", o que diminuía o tempo de operação mas ampliava o risco de espionagem ou captura dos processos.

Chegou-se, então, à conclusão que a implementação da Criptografia deveria depender menos do segredo contido no algoritmo escolhido, e depender de um valor ou palavra secreta (a "chave"). Com isso, poder-se-ia adotar um ou dois algoritmos padrão, e mudar o "segredo" com freqüência satisfatória para diminuir os problemas anteriormente mencionados. Assim, ainda que o criptografista fosse capturado, ou seus meios auxiliares roubados ou copiados, a adoção de nova chave bastaria para manter a comunicação segura.

Vejamos, como exemplo, a adoção de um alfabeto à partir de uma chave simples. Consideremos, para o nosso alfabeto, a palavra " PERIGOSA ":

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

Também os métodos de transposição evoluíram à partir do uso das palavras-chave. Vejamos uma possibilidade simples de método de transposição:

Palavra-Chave: *BRASIL*

B	R	A	S	I	L
I	S	T	O	É	U
M	A	M	E	N	S
A	G	E	M		

As palavras foram escritas sem espaçamentos e de forma linear (normal) na tabela. Em seguida, o texto cifrado foi extraído obtendo-se palavras à partir das colunas, ordenadas de acordo com a ordem alfabética da palavra chave. Assim, a letra " A " em " BRASIL " corresponde a coluna "1", a letra " B " corresponde a coluna " 2 ", e assim sucessivamente.

Mensagem resultante: *TME IMA EN US SAG OEM*

Com o uso das chaves criou-se um número virtualmente ilimitado de possibilidades para um mesmo método de cifragem. Expirando o período de uso da chave, adotar-se-ia uma nova, modificando o alfabeto. O segredo deixou de residir exclusivamente no processo.

Apesar do avanço que o conceito das chaves representou, alguns problemas permaneciam como grandes limitadores do emprego da Criptografia

em larga escala. O problema maior era a persistente necessidade de haver contato prévio (por um canal seguro) entre o emissor e o receptor, já que ambos tinham de conhecer a chave utilizada no processo. A esse problema some-se outro: Como o emissor não desejasse que ninguém além de um receptor específico houvesse condições de ler a mensagem, era necessário, então, criar diferentes chaves para diferentes destinatários. Assim, o número de chaves necessário podia ser inconvenientemente grande para se lidar com segurança. Além disso, considerando a existência de um canal seguro, necessário para a troca das chaves, por que não usar esse mesmo canal para transmitir as mensagens em claro?

Também, como já vimos, era necessário levar-se em conta a relação *complexidade do algoritmo e tamanho da chave / tempo necessário para cifrar ou decifrar*.

Essas limitações contribuíram, durante muito tempo, para que a Criptografia não fosse aplicável senão em grupos muito específicos, como os militares. Era ainda necessário grande sigilo quanto a forma de proceder, canais seguros, planos de ação alternativos, etc.

Após a II Guerra Mundial, entretanto, alguns fatores possibilitaram (ou exigiram) o rompimento dessas limitações. Dentre esses fatores, podemos destacar:

1. O surgimento do microchip, com o conseqüente aumento na velocidade de cálculo em relação aos métodos anteriores;
2. O avanço do conhecimento matemático, que permitiu encontrar novas equações com maior grau de complexidade e segurança;
3. Necessidade de segurança, em função do avanço nas sociedades democráticas, da guerra-fria, etc.

Novos sistemas criptográficos foram desenvolvidos. A complexidade (e conseqüente segurança) dos sistemas tradicionais aumentou muito, mesclando mecanismos de transposição e de permutação e envolvendo grandezas matemáticas até então impraticáveis. Aqueles sistemas passaram a ser conhecidos como *Sistemas de Criptografia Simétrica*, ou *Criptografia de Chave Simétrica*, porque a mesma chave é usada para cifrar e decifrar. E surgiram os *Sistemas de Criptografia Assimétrica*, ou *Criptografia de Chave Pública*, baseados em complexas operações matemáticas.

SISTEMAS DE CRIPTOGRAFIA ASSIMÉTRICA

Os sistemas de Criptografia Assimétrica vieram eliminar a necessidade de canais seguros para a transmissão de chaves. Nesses sistemas, são criadas duas chaves, uma das quais é dita " Pública "- o que quer dizer que pode (e deve) ser

distribuída sem restrições – e outra, " Privada " – deve ser mantida em segredo. Uma chave é usada para cifrar, e a outra, para decifrar.

Assim, a troca de chaves criptográficas passou a ser possível mesmo que por canais não seguros. A combinação das chaves do emissor e do receptor resulta em uma combinação única. O processo é sucintamente descrito a seguir:

1. O remetente, após redigir a mensagem, seleciona o destinatário desejado;
2. Usando sua chave Privada E a chave Pública do destinatário, a mensagem é cifrada;
3. A mensagem é enviada.
4. O destinatário, de posse da mensagem, usa a sua chave Privada e a chave Pública do Remetente para decifrar a mensagem.

Percebe-se, claramente, que o algoritmo não faz mais parte do segredo envolvido na cifragem. Na verdade, o que ocorreu foi exatamente o oposto. Enquanto nos sistemas tradicionais, o processo usado para cifrar era, tanto quanto possível, mantido com discrição, os processos assimétricos, ao possibilitarem o surgimento de uma variada gama de aplicações, estimulou também a divulgação do algoritmo, como forma de ampliar a confiança nessas novas aplicações, de forma a induzir à sua aceitação.

Também o problema da manutenção de um grande número de chaves foi resolvido. A mesma chave pública pode ser distribuída para todos os destinatários sem comprometer a segurança. Surgiram " Chaveiros Digitais ", locais na Internet usados como repositórios de chaves públicas, facilitando assim a sua distribuição.

Os dois principais algoritmos de Criptografia Assimétrica são o RSA (Rivest, Shamir and Adleman) e o Diffie-Hellman. O primeiro baseia-se na dificuldade de se encontrar os fatores primos de um grande número inteiro, e o segundo na dificuldade de se computar pequenos logaritmos à partir das possibilidades geradas por um grande número primo. Ambos são códigos conhecidos, estudados detalhadamente nos principais centros acadêmicos de tecnologia. Por isso mesmo, é reconhecida sua confiabilidade e segurança.

O processo matemático de geração de chaves é fácil de resolver em um sentido, mas virtualmente impossível, no sentido inverso. Ou seja, não é possível deduzir a chave Privada à partir da Pública. Da mesma forma, o sentido cifrar – decifrar é único. A mensagem cifrada com a chave privada do remetente e a pública do destinatário só pode ser decifrada com a chave pública do remetente e a privada do destinatário. Após cifrar a mensagem, o remetente estará impossibilitado de decifrá-la.

Uma desvantagem dos processos de Criptografia Assimétricos em relação aos Simétricos diz respeito à velocidade dos processos, muito mais lentos.

.

AUTENTICAÇÃO DE MENSAGENS

Outro uso possível e de extrema importância para os sistemas de Chave-Pública, é o de Autenticação de Mensagens. Trata-se de métodos pelos quais o destinatário, ao receber a mensagem, pode certificar-se de que a mesma foi, de fato, enviada pelo suposto remetente, e que seu conteúdo não foi adulterado entre a emissão e a recepção.

Para tornar possível conferir a origem da mensagem, o emissor coloca na mesma uma *Assinatura Digital*. Essa assinatura é gerada submetendo-se o arquivo original a uma função matemática conhecida como *hash*, que gera um valor numérico de acordo com o conteúdo do arquivo. Não é possível realizar essa operação no sentido inverso (ou seja, deduzir o conteúdo do arquivo à partir desse número). Após criar o valor *hash*, o programa cifra esse valor usando a chave privada do emissor. Então, cria uma nova versão da mensagem original, que contém a mensagem em claro e o valor *hash* cifrado.

Quando o destinatário receber a mensagem, o software inicialmente usará a chave pública do remetente para decifrar o valor hash. Então, armazenará o valor, e submeterá o conteúdo da mensagem à mesma função hash. Finalmente, comparará o resultado obtido com o valor recebido na mensagem. A igualdade entre os dois valores atesta a origem e a integridade da mensagem.

A CRIPTOANÁLISE

Também é necessário que se tenha algum entendimento sobre a Criptoanálise, ou o estudo das técnicas de se reverter um texto cifrado em uma texto em claro de forma a violar a segurança das transmissões.

Existem variadas técnicas de ataque aos sistemas de criptografia. Sua seleção depende do quanto se conhece à respeito da mensagem que se deseja decifrar ou a chave que se deseja descobrir.

Consideremos, inicialmente, a situação em que o Criptoanalista nada possui senão o texto cifrado. O trabalho consistirá, portanto, em inferir dados à partir de possibilidades, testar cada possibilidade até chegar-se a algum resultado. Como exemplo, podemos considerar o método da transposição de alfabetos, mencionado no início desta explanação. O Criptoanalista, provavelmente, copiaria a mensagem deixando espaço sob cada linha de texto. Em seguida, procuraria descobrir as vogais – cada palavra tem pelo menos uma delas. Também procuraria palavras de uma, duas ou tres caracteres, consoantes dobradas e outros pares de letras mais comuns. A presença de sinais de pontuação na mensagem auxiliaria muito o decifrador. Evidentemente, esses processos não são aplicáveis aos sistemas modernos.

Outra possibilidade é aquela em que o atacante conhece parte do texto em claro, e possui a mensagem cifrada. A tarefa consiste, então, em descobrir o resto

do texto usando a informação que já se tem. Geralmente, tentar-se-ia chegar a chave usada para a cifragem, através do estudo dos padrões. Embora seja possível obter algum resultado neste caso, a dificuldade é muito grande, exigindo muito tempo e processamento.

Consideremos, ainda o caso em que, sem dispor da chave, o atacante consegue fornecer texto em claro para, depois obter o resultado cifrado. Busca-se, neste caso, obter a chave. Esta forma de ataque representa risco para alguns algoritmos modernos, como o RSA.

A chave para o sucesso do Criptoanalista encontra-se nas correlações conhecidas ou inferidas entre o texto cifrado e o texto em claro. Se as informações puderem ser coletadas junto ao sistema de cifragem, o trabalho será em muito facilitado.

Outra possibilidade de ataque aos sistemas modernos diz respeito a valores que se possa mensurar junto ao Hardware (equipamento) onde é executada a cifragem. Provou-se que, se for possível medir precisamente o tempo consumido na operação de cifragem, um atacante pode deduzir matematicamente o expoente usado pelo algoritmo Diffie-Hellman, ou o Fator das chaves RSA. Assim, é possível minimizar o tempo de procura pelas chaves corretas, através do chamado "*Ataque de Força-Bruta* ".

E o que vem a ser este "*Ataque de Força-Bruta* " ? Trata-se da forma de ataque mais elementar, e consiste em tentar todas as combinações (chaves) possíveis, até encontrar a chave correta. Pode-se dizer que esta forma de ataque é a única que poderia ser empregada contra qualquer Sistema Criptográfico. Mas, será praticável? Vejamos: Se considerarmos, novamente, o sistema de transposição monoalfabética apresentado no início deste estudo, e considerando um alfabeto de 27 caracteres, teremos 27 correspondências possíveis para cada caractere. Claramente, percebemos que o tempo gasto para testar todas as chaves é proporcional ao número de possibilidades que a chave oferece.

CONSIDERAÇÕES SOBRE A SEGURANÇA

É necessário, agora que já compreendemos um pouco mais sobre métodos criptográficos, tecer algumas considerações sobre a segurança da Criptografia.

Os sistemas modernos baseiam-se em operações matemáticas muito complexas, sendo que essas equações não possuem sigilo algum. São, muito pelo contrário, amplamente conhecidas e estudadas no meio acadêmico. Até onde a matemática atual conhece, tais equações são extremamente confiáveis.

O segredo encontra-se, portanto, na chave. Desta forma a confiabilidade da chave é que define quão segura uma transmissão pode ser.

Os sistemas simétricos baseiam-se, como foi visto, em funções de permutação e transposição que, combinados, resultam em uma cifragem mais rápida e mais segura. Os mecanismos de chave pública, mais lentos, apresentam

menor dificuldade para serem decifrados. Mas, ambos os sistemas tem a sua segurança proporcional à chave empregada.

O estudo dos algoritmos mais comuns nos mostra, por exemplo, que um ataque de força-bruta é razoável quando consideramos valores de 10 ou 20 dígitos em tamanho. Mas os softwares modernos usam valores bem acima disso. Lembremo-nos da restrição que o governo dos EUA impunha à exportação de softwares daquele país em relação ao tamanho da chave: 40 *bits*. A cada *bit* o grau de segurança cresce exponencialmente. Até 1999, o governo americano sentia-se seguro para decifrar chaves até 44 *bits* em tempo "razoável". Até o presente, não se conseguiu decifrar chaves superiores a 512 *bits* por força-bruta. Em 1997, o padrão DES de cifragem foi quebrado, com uma chave de 56 bits, por uma rede de 14.000 computadores. Em 1999, pesquisadores do vale do silício conseguiram quebrar o mesmo código com chave de 56 bits em "apenas" 22 horas e 15 minutos. O software mais usado para Criptografia no mundo, o PGP, àquela época, já trabalhava com chaves de valores entre 512 e 2048 bits RSA...

É importante notarmos que, quando falamos anteriormente em criptoanálise, ou neste momento ao mencionarmos os valores dos ataques de força-bruta, estamos considerando o uso de hardware especial – os poderosos computadores disponíveis em algumas grandes universidades e centros de pesquisa – e pessoal especializado. Em um moderno microcomputador, o tempo necessário para violar um sistema cifrado com chave de 40 *bits* necessitaria de meses de processamento ininterrupto.

Assim, a questão da segurança dos dados pode ser claramente percebida em uma avaliação do tipo "custo-benefício". Quanto vale a informação que se deseja obter? Por quanto tempo ela é válida? Essas são as perguntas determinantes para quem terá de alocar grande poder computacional e mão de obra especializada por longo período de tempo.

A Criptografia nas Sociedades Modernas

As variadas implementações que o conhecimento da Criptografia de Chave Pública possibilitou estão presentes em vasta gama de aplicações que fazem parte da vida das pessoas. A maciça presença dos computadores nas diversas esferas sociais e a facilidade conferida, entre outros, pelo uso da Internet, trouxe grande aumento no número de documentos eletrônicos. A possibilidade de transferir de forma segura dados confidenciais e/ou verificar a procedência e integridade dos documentos representou grande avanço na prestação de serviços diversos.

Além dos aspectos acima mencionados, outro merece especial atenção: se uma determinada transação requer, para sua efetivação, o uso de sistemas de assinatura digital, elimina-se a possibilidade de que o remetente de um documento negue ser o seu autor. Esta consideração é de grande importância para o funcionamento do comércio eletrônico. Por meio dela, por exemplo, pode-se

confirmar que um pedido de compras feito pela internet foi feito pelo cliente e recebido pelo site de vendas.

Para que essa última consideração seja possível, é necessário um terceiro elemento participante dessa equação: um " cartório digital ". Os cartórios digitais atuam como os convencionais, e visam possibilitar a comprovação da origem e legitimidade dos documentos, que podem ser transmitidos por meios eletrônicos. Devem ser usados para validar comprar, autenticar documentos, realizar transações de fundos bancários, etc. Em alguns países, o cartório eletrônico já constitui, na maioria dos casos, prova inquestionável da autoria de um documento, como os cartórios tradicionais. O uso da assinatura digital passa a ter valor legal, assim como o uso de um cartão magnético para operações bancárias.

A extensão da funcionalidade dos cartórios eletrônicos para outras áreas que não exclusivamente o comércio eletrônico é, positivamente, uma tendência. Já se tem escrito sobre a eliminação de barreiras ainda existentes ao uso desta tecnologia. Podemos citar como exemplo o caso das eleições e o voto eletrônico. Cogita-se um futuro em que seja possível o eleitor efetuar o seu voto à partir de sua casa, de um hotel, ou, quem sabe, de outro país. Artigo publicado no Estadão em 02 de maio de 2001 já tratava da questão. É, sem dúvida, um assunto controverso. Mas, até algum tempo atrás, também o era a Declaração de Imposto de Renda pela Internet.

Podemos esperar, em um futuro talvez não muito distante, que os cartórios digitais incorporem – ou sejam incorporados – às funções de cartórios tradicionais. Veríamos mudanças na forma de proceder em relação a muitas questões, como o reconhecimento de firmas e o registro de procurações. Mas esse é o tipo de mudança que maior rejeição sofre na sociedade, seja pelos interesses de grupos em manter a estrutura tal como se encontra, seja pela incompreensão dos mecanismos que tornam possível. Exemplificando a questão: Em artigo de 02 de setembro deste ano no Jornal de Brasília, o professor de Criptografia e Segurança na Informática da UnB, Pedro Antônio Rezende, manifestou fazer sua Declaração de Imposto de Renda à mão, não porque o processo digital não seja seguro, mas porque " a declaração digital não autentica o declarante perante terceiros ". Nota-se, claramente, a referência ao fato da sociedade ainda não ter assimilado – ou aceitado – integralmente as mudanças.

Os sistemas bancários tem sido, no que tange a implementação de novas tecnologias (e conceitos), pioneiro. Enquanto o governo americano manteve a restrição para exportação de softwares criptográficos com chaves superiores a 40 bits, muitos bancos, buscando alcançar a segurança que garantiria a implementação de transações pela internet, adquiriram pacotes criptográficos de 128 bits e incorporaram ao seu sistema.

A limitação imposta pelo governo americano, por pressão de diversos setores e, principalmente, considerando o quanto o próprio governo americano tinha a perder criando óbices ao comércio eletrônico nas suas mais variadas vertentes, foi suspensa. Com isso, os browsers mais usados para navegação na Internet já vem preparados para trabalhar com chaves criptográficas seguras.

.

Quando um browser atual é instalado, ele, como parte do processo de instalação, gera as chaves pública e privada necessárias ao uso do protocolo SHTTP; As chaves ficam armazenadas para recuperação posterior. Quando uma conexão a um " site seguro " é iniciada, ocorre, inicialmente, a troca de chaves públicas pelo browser. Então, uma chave simétrica é gerada, e enviada através da Internet. Essa chave passa a ser usada para aquela transação, garantindo segurança ao longo da mesma.

"A DEFESA DA PRIVACIDADE E O INTERESSE DO ESTADO"

Esse foi o título de um artigo publicado no Estadão de 10 de dezembro de 2002, versando sobre " a tensão permanente entre os direitos do indivíduo e as pretensões do poder público " .

De fato, trata-se de assunto muito polêmico, cuja ampliação recente deveu-se às posturas adotadas pelo governo dos EUA após o episódio dos ataques de 11 de setembro. Mas o fato é que o governo daquele país sempre teve grande preocupação com a disseminação da tecnologia de segurança, suas maiores e mais recentes concessões sendo resultado da pressão em função da adoção do "livre-comércio", aliadas à constatação que as restrições legais à exportação de tecnologia mostraram-se ineficazes para a sua proliferação em outros países.

A questão, entretanto, permanece bem viva. Noticiou-se que o FBI estava trabalhando em uma maneira de espalhar (em forma de vírus de computador) um software que registra as senhas digitadas e as envia àquela instituição. Assim, resolver-se-ia parte do problema que representa a criptografia para os trabalhos investigativos. Verdadeira ou não, muita discussão foi gerada pela notícia.

A probabilidade que organizações criminosas ou terroristas estejam usando ferramentas criptográficas para enviar suas mensagens por e-mail tem levado alguns governos a investirem contra a liberdade de uso dessas ferramentas.

Destaca-se, nessa discussão, a questão da esteganografia.

A ESTEGANOGRAFIA

Ramo da Criptologia que consiste no estudo das formas de ocultação de uma mensagem. Ao invés de cifrá-la, o que se busca é tornar a sua presença imperceptível.

Muito antiga, a esteganografia também passou por grande crescimento com o avanço da computação pós-guerra. Hoje, mensagens podem ser camufladas em arquivos de áudio e vídeo, ou mesmo em fotografias digitais, e enviadas através da Internet. Seu funcionamento leva em consideração as

limitações dos sentidos humanos, escondendo a informação em posições, nos arquivos, em que o olho ou ouvido humano não possam perceber a modificação.

Isso tem preocupado muito os governos, devido ao volume de arquivos circulando na rede. O FBI, por exemplo, acredita que a organização de Bin Laden tenha usado a esteganografia para transmitir mensagens pela rede. Entretanto, após o 11 de setembro, foram localizadas centenas de mensagens de correio eletrônico associadas ao World Trade Center, escritas em inglês ou árabe e que foram transmitidas em claro.

A complexidade envolvida na discussão sobre a esteganografia é grande. O USA Today publicou, em junho de 2001, uma reportagem sensacionalista que dizia ser a esteganografia a ferramenta preferida de Bin Laden. Segundo o artigo, mensagens estariam sendo transmitidas ocultas em imagens colocadas nos sites eBay e Amazon. Um presquisador da Universidade de Michigan, então, trabalhou em dois milhões de imagens que circularam por aqueles sites. Inicialmente, efetuou extensas varreduras nas imagens, procurando identificar aquelas que poderiam conter alguma mensagem. Detectou " diversos milhares " de possibilidades, conforme informado no Wired News, em artigo datado de 08 Nov 2001. Então, buscou decifrar essas mensagens usando um dicionário de dados para um ataque de " força-bruta ". Não conseguiu identificar positivamente nenhuma ocorrência, durante os 6 meses em que conduziu a sua pesquisa.

A questão mais controversa no uso da esteganografia é justamente o que trata da sua natureza. Os métodos de cifragem possibilitam a segurança das mensagens sem, conceitualmente, torná-las ilegítimas. O governo pode saber que estão circulando, ainda que não seja capaz de identificar o seu teor. Com a esteganografia, busca-se esconder a existência da mensagem, o que leva à teorizações sobre as intenções de quem estaria desejando passar despercebido.

.

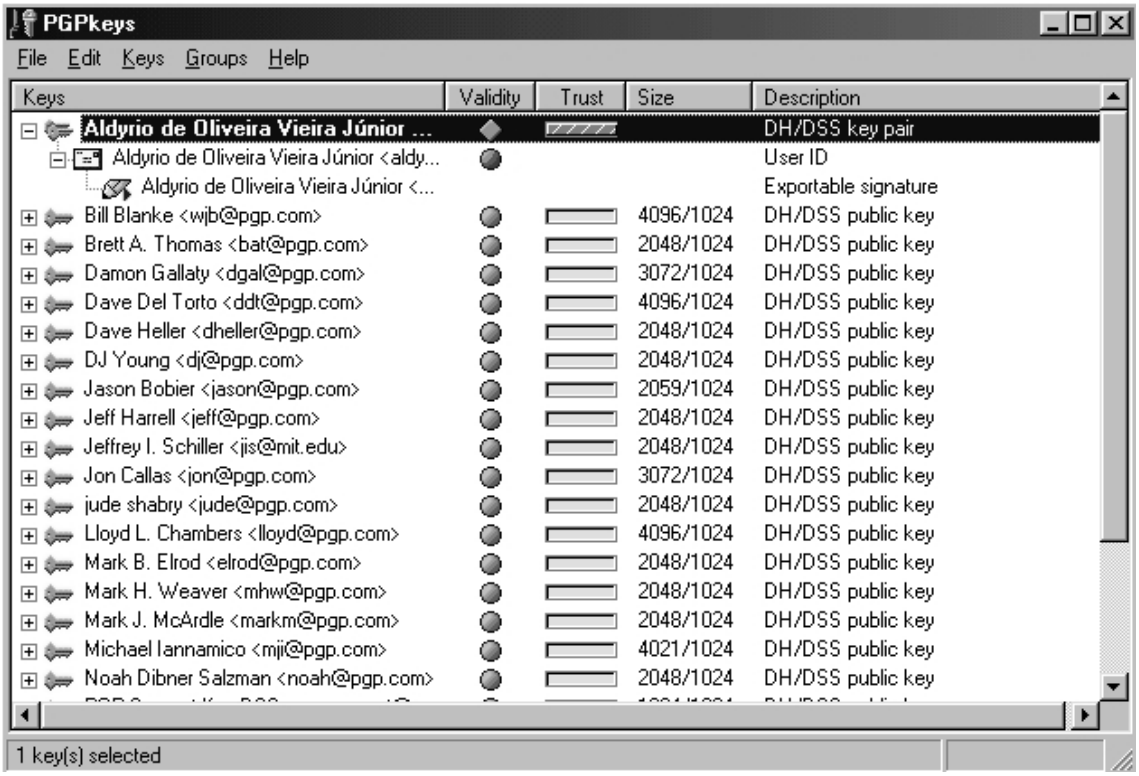
PGP

O Pretty Good Privacy (PGP) é o mais conhecido e usado sistema de criptografia no mundo. A revista Fortune, em 1997, divulgou que pelo menos a metade de sua " lista dos 100 " usavam PGP para transmitir informações seguras, incluindo IBM, American Express e Microsoft.

De operação bastante simples, possui versões freeware – que podem ser obtidas por download no site do MIT ou através do endereço http://www.pgp.com – e versão comercial.

O programa possui implementações tanto para cifragem de documentos quanto para autenticação, e permite ao usuário escolher entre os principais métodos de cifragem conhecidos, o tamanho das chaves, etc.

No momento da geração das chaves para criptografia assimétrica – que pode ocorrer durante o processo de instalação do software ou após – é também oferecida ao usuário a possibilidade de armazenar a sua chave pública em um "chaveiro digital " na Internet. A chave privada, após gerada, é cifrada através de um algoritmo simétrico, cuja chave tem de ser informada pelo usuário cada vez que houver necessidade de uso daquela.



Quando se deseja enviar uma correspondência cifrada, PGP usa um processo de cifragem simétrico (mais rápido e seguro), e usa o processo assimétrico para enviar a chave, gerada aleatoriamente.