Tudo que você precisa saber sobre Criptografia

...e tinha medo de perguntar

Criptografia vem do grego e significa “escrita escondida”. Bem, ainda não temos a tecnologia dos filmes de fantasia onde um pergaminho aparentemente em branco revela um mapa do tesouro quando exposto ao luar, mas a criptografia simula isso transformando a informação em algo ilegível ou aparentemente sem valor. Muito fácil: se eu rabiscar bem um cheque de R$100.000,00 ele também perde seu valor por ficar ilegível.

O difícil é o inverso: tornar legível o ilegível, e é aí que está a magia da criptografia.

O primeiro lugar onde alguém antenado pensaria em usar criptografia é na guerra, para comunicar estratégia de movimentação a tropas distantes, espionagem, etc. Se o inimigo intercepta essa comunicação, principalmente sem o primeiro saber, ganha a guerra. Por isso quem primeiro estudou técnicas de criptografia foram os militares, governos e instituições de pesquisas secretas. Focavam em duas coisas: como criptografar melhor e como descriptografar as mensagens do inimigo (criptoanálise).

Na nossa Era da Informação e Internet, criptografia tem um papel central porque viabiliza comunicação segura. Mais até: não teríamos uma Era da Informação se criptografia não fosse de uso dominado por qualquer cidadão, simplesmente porque o mundo comercial não entraria nessa onda de trocar informação (e fazer negócios) por redes abertas se não houvesse um meio de garantir confidencialidade.

Trata-se de um tema muito vasto, fascinante, com muitos desdobramentos tecnológicos. Então vamos somente nos focar em entender aqui o vocabulário desse mundo.

Criptografia de Chave-Simétrica

Criptografia digital já era usada secretamente desde 1949 por militares e governos. Em meados da década de 1970 a IBM inventou o padrão **DES** (Data Encription Standard) de criptografia, que passou a ser largamente utilizado até os dias de hoje. A partir daí tudo mudou.

Como exemplo de seu funcionamento, se a Paula quer enviar uma mensagem secreta para Tatiana, ela deve fazer isso:

Mensagem + *ChaveSimétrica* = *MensagemCriptografada*

Então *MensagemCriptografada* é enviada para Tatiana por uma rede aberta, que para lê-la terá que fazer o seguinte:

MensagemCriptografada + *ChaveSimétrica* = *Mensagem*

Uma analogia a essas equações seria como se ambas trocassem caixas que abrem e fecham com uma chave (a chave simétrica), que contém cartas secretas. Para a Tatiana abrir a caixa da Paula, terá que usar uma cópia da chave que a última usou para fecha-la.

O que representamos pela soma (+) é na verdade o **algoritmo de cifragem** (ou o mecanismo da fechadura) que criptografa e descriptografa a mensagem. Hoje em dia, esses algoritmos tem geralmente seu código fonte aberto, e isso ajudou-os a se tornarem mais seguros ainda, pois foram limpos e revisados ao longo dos anos por muitas pessoas ao redor do mundo.

A **Chave Simétrica** é uma seqüencia de bits e é ela que define o nível de segurança da comunicação. Ela deve ser sempre secreta. Chama-se simétrica porque todos os interessados em se comunicar devem ter uma cópia da mesma chave.

O DES com chave de 56 bits pode ser quebrado (*MensagemCriptografada* pode ser lida sem se conhecer a chave), e outros **cifradores de chave simétrica** (symmetric-key, ou private-key) mais modernos surgiram, como **3DES**, **AES**, **IDEA**, etc.

O maior problema da criptografia de chave simétrica é como o remetente envia a chave secreta ao destinatário através de uma rede aberta (e teoricamente insegura). Se um intruso descobri-la, poderá ler todas as mensagens trocadas. Mais ainda, comprometerá a comunicação entre todo o conjunto de pessoas que confiavam nessa chave.

Criptografia de Chave Pública

Esses problemas foram eliminados em 1976 quando Whitfield Diffie e Martin Hellman trouxeram a tona os conceitos da **criptografia de chave pública** também conhecida por **criptografia por par de chaves** ou de **chave assimétrica**. Trata-se de uma revolução no campo das comunicações, tão radical quanto é o motor a combustão para o campo de transportes. Eles descobriram fórmulas matemáticas que permitem que cada usuário tenha um **par de chaves de criptografia** matematicamente relacionadas, uma privada e outra pública, sendo a última, como o próprio nome diz, publicamente disponível para qualquer pessoa. Essas fórmulas tem a impressionante característica de o que for criptografado com uma chave, só pode ser descriptografado com seu par. Então, no nosso exemplo, Paula agora enviaria uma mensagem para Tatiana da seguinte maneira:

Mensagem + ChavePública(Tatiana) = MensagemCriptografada

E Tatiana leria a mensagem assim:

MensagemCriptografada + ChavePrivada(Tatiana) = Mensagem

E Tatiana responderia para Paula da mesma forma:

Resposta + ChavePública(Paula) = RespostaCriptografada

Ou seja, uma mensagem criptografada com a chave pública de uma, só pode ser descriptografada com a chave privada da mesma, então a primeira pode ser livremente disponibilizada na Internet. E se a chave privada da Paula for roubada, somente as mensagens para a Paula estariam comprometidas.

O cifrador de chave pública tido como mais confiável é o **RSA** (iniciais de Rivest, Shamir e Adleman, seus criadores).

Criptografia assimétrica permitiu ainda outras inovações revolucionárias: se Tatiana quer publicar um documento e garantir sua autenticidade, pode fazer:

Documento + ChavePrivada(Tatiana) = DocumentoCriptografado

Se um leitor conseguir descriptografar este documento com a **chave pública** da Tatiana significa que ele foi criptografado com a **chave privada** da Tatiana, que somente ela tem a posse, o que significa que somente a Tatiana poderia te-lo publicado. Nasce assim a **assinatura digital**.

Infraestrutura para Chaves Públicas

O **PGP** (Pretty Good Privacy) foi o primeiro sistema de segurança que ofereceu criptografia de chave pública e assinatura digital de qualidade para as massas. Ficou tão popular que virou o padrão OpenPGP e posteriormente recebeu várias implementações livres. É largamente usado até hoje, principalmente em troca de e-mails. Sua popularização exigiu que houvesse uma forma para as pessoas encontrarem as chaves públicas de outras pessoas, que muitas vezes nem eram conhecidas pelas primeiras. No começo dos tempos do PGP, haviam sites onde as pessoas publicavam suas chaves públicas para as outras encontrarem. Talvez esta foi a forma mais rudimentar de **PKI** ou **Public Key Infrastructure**. PKI é um conjunto de ferramentas que uma comunidade usa justamente para a classificação, busca e integridade de suas chaves públicas. É um conjunto de idéias e não um padrão nem um produto. Conceitos de PKI estão hoje totalmente integrados em produtos de colaboração como o Lotus Notes da IBM, e seu uso é transparente ao usuário.

Certificados Digitais

Como Tatiana pode ter certeza que a chave pública de Paula que ela tem em mãos, e que está prestes a usar para enviar uma mensagem segura, é realmente de Paula? Outra pessoa, agindo de má fé, pode ter criado uma chave aleatória e publicado-a como sendo da Paula. Podemos colocar isso de outra forma: como posso ter certeza que estou acessando realmente o site de meu banco e não um site impostor que quer roubar minha senha, e meu dinheiro? Não gostaria de confiar em meus olhos só porque o site realmente se parece com o de meu banco. Haveria alguma forma mais confiável para garantir isso ?

Em 1996, a Netscape, fabricante do famoso browser, atacou este problema juntando o que havia de melhor em criptografia de chave pública, PKI (através do padrão **X.509**), mais parcerias com entidades confiáveis, e inventou o protocolo **SSL** (Secure Socket Layer ou **TLS**, seu sucessor), e foi graças a este passo que a Internet tomou um rumo de

plataforma comercialmente viável para negócios, e mudou o mundo.

Para eu mandar minha senha com segurança ao site do banco, e poder movimentar minha conta, o site precisa primeiro me enviar sua chave pública, que vem assinada digitalmente por uma outra instituição de grande credibilidade. Em linhas gerais, os fabricantes de browsers (Mozilla, Microsoft, etc) instalam em seus produtos, na fábrica, os **certificados digitais** dessas entidades, que são usadas para verificar a autenticidade da chave pública e identidade do site do banco. Este, por sua vez, teve que passar por um processo burocrático junto a essa **entidade certificadora**, provando ser quem diz ser, para obter o certificado.

O SSL descomplicou essa malha de credibilidade, reduzindo o número de instituições em quem podemos confiar, distribuindo essa confiança por todos os sites que adquirirem um certificado SSL.

Na prática, funciona assim:

1. Acesso pela primeira vez o site de uma empresa que parece ser idônea.
2. Ele pede o número de meu cartão de crédito.
3. Se meu browser não reclamou da segurança desse site, posso confiar nele porque...
4. ...o site usa um certificado emitido por uma entidade que eu confio.

Pode-se verificar os certificados que o fabricante do browser instalou, acessando suas configurações de segurança. Você vai encontrar lá entidades como **VeriSign**, **Thawte**, **Equifax**, **GeoTrust**, **Visa**, entre outros.

Segurança Real da Criptografia

Quanto maior for a chave de criptografia (número de bits) mais difícil é atacar um sistema criptográfico. Outros fatores influenciam na segurança, como a cultura em torno de manter bem guardadas as chaves privadas, qualidade dos algoritmos do cifrador, etc. Este último aspecto é muito importante, e tem se estabilizado num bom nível alto, porque esses algoritmos tem sido produzidos num modelo de software livre, o que permite várias boas mentes audita-los e corrigir falhas ou métodos matemáticos ruins.

A segurança real de qualquer esquema de criptografia não foi comprovada. Significa que, teoricamente, qualquer um que tiver muito recurso computacional disponível pode usa-lo para quebrar uma mensagem criptografada. Teoricamente. Porque estaríamos falando de centenas de computadores interconectados trabalhando para esse fim. Na prática, hoje isso é intangível, e basta usar bons produtos de criptografia (de preferência os baseados em software livre), com boas práticas de administração, e teremos criptografia realmente segura a nossa disposição.

(1574 palavras)

Mini curriculum:

Avi Alkalay foi, por alguns anos, responsável pela segurança corporativa da IBM Brasil, e já trabalhou praticamente com todas as tecnologias da web. Hoje é arquiteto de soluções e consultor de Linux, Padrões Abertos e Software Livre na IBM.

outra opção, que prefiro mais:

Eu, Avi Alkalay, fui, por alguns anos, responsável pela segurança corporativa da IBM Brasil, e trabalhei praticamente com todas as tecnologias da web. Hoje sou arquiteto de soluções e consultor de Linux, Padrões Abertos e Software Livre na IBM; e adoro receber sugestões de temas para escrever artigos.