Criptografia

O que é Criptografia:

Criptografia é um mecanismo de segurança e privacidade que torna determinada comunicação (textos, imagens, vídeos e etc) ininteligível para quem não tem acesso aos códigos de "tradução" da mensagem.

Nas comunicações digitais, a criptografia auxilia na proteção de todos os conteúdos transmitidos entre duas ou mais fontes, evitando a intercepção por parte de cibercriminosos, hackers e espiões, por exemplo.

Atualmente, a maioria dos sites na internet utilizam comunicações criptografadas, principalmente em locais onde dados bancários, passwords e arquivos pessoais estejam armazenados.

Além de prevenir que pessoas não-autorizadas tenham acesso aos dados e informações trocadas na rede online, a criptografia também impede que backups sejam acessados por usuários indevidos.

Etimologicamente, o termo "criptografia" se originou a partir do grego, formado pela união dos elementos kruptós, que significa "secreto" ou "oculto", e graphía, que quer dizer "escrita". Assim, o significa literal de criptografia é "escrita secreta".

No cotidiano, sistemas de criptografia são utilizadas pelos usuários de aplicativos e softwares de troca de mensagens instantâneas, como o Whatsapp, por exemplo.

Tipos de Criptografia

Nas comunicações feitas através de dispositivos eletrônicos, o método mais utilizado de criptografia são as chamadas "chaves critptográficas".

As chaves criptográficas consistem em conjuntos de algoritmos que codificam uma mensagem publicamente legível em um texto cifrado, ou seja, composto por valores secretos que só podem ser decifrados com o código de acesso correto.

Existem dois principais tipos de chaves criptográficas, estudadas através do ramo da Matemática conhecido por Criptologia: as simétricas e as assimétricas.

Simétrica

Também conhecida por "criptografia de chave única" ou "criptografia de chave privada", este modelo utiliza apenas um conjunto de algoritmos responsáveis tanto pela cifragem de determinada operação, assim como a sua decifragem.

Neste caso, o pressuposto da confiabilidade entre os interlocutores deve ser total, visto que ambos partilham de uma única chave de criptografia, tanto para codificar como para descodificar uma mensagem, por exemplo.

Assimétrica

Também conhecido como "criptografia de chave pública", este é um sistema de protocolos criptográficos que requer a formação de duas chaves, sendo uma privada (usada para descodificar) e a outra pública (utilizada para codificar e autenticar assinaturas digitais, por exemplo).

Com a criptografia assimétrica, qualquer pessoa pode enviar uma mensagem criptografada usando a chave pública, mas apenas os receptores com a chave privada conseguem descodifica-la. O segredo da informação consiste em manter em sigilo o código da chave privada, por exemplo.

Em linhas gerais, criptografia é o nome que se dá a técnicas que transformam informação inteligível em algo que um agente externo seja incapaz de compreender. De forma mais simples, a criptografia funciona como códigos: sem ela, um criminoso poderia interceptar a sua senha de e-mail durante o login.

Com a criptografia, caso ele intercepte seu acesso, mas não tenha a chave correta, verá apenas uma lista desordenada e aparentemente confusa de caracteres, que não leva a lugar nenhum.

A criptografia é um método de proteção e privacidade de dados muito importante e cada vez mais presente. Do ponto de vista prático para quem usa Internet e dispositivos que oferecem proteção criptográfica, há tipos ou termos, que é preciso conhecer: criptografia simétrica e assimétrica (ou de ponta a ponta).

Criptografia Simétrica

O tipo de criptografia simétrica é o mais comum e pressupõe que uma mesma chave usada para ocultar informação precisa ser aplicada para revela-la na outra ponta. É o tipo de criptografia usada na época da Segunda Guerra Mundial, por exemplo, e protagonista da história da invenção do computador, como conhecemos hoje.

Criptografia Assimétrica ou de Ponta-a-Ponta

Atualmente, os dois protocolos mais usados para proteção de dados na Internet, o SSL (Secure Sockets Layer) e o TLS (Transport Layer Security) utilizam a criptografia simétrica para proteger os dados transmitidos e armazenados.

No entanto, a criptografia simétrica possui um desafio conceitual importante e impossível de ser resolvido. Como combinar uma chave secreta entre duas pessoas que querem se comunicar através da Internet de forma que ela não possa ser obtida por um invasor? Essa pergunta não teve solução até a década de 1970.

A solução foi dada pela criptografia assimétrica, na qual utiliza-se duas chaves distintas, mas que se complementam. Por essa propriedade, dá-se o nome de par de chaves, que é composto pela chave pública e pela chave privada. A chave pública é liberada para todos que desejam se comunicar com o emissor da chave enquanto a chave privada fica em poder de quem a emitiu.

O algoritmo de criptografia mais usado atualmente é o RSA, denominado pelas iniciais dos seus criadores, Ronald Rivest, Adi Shamir e Leonard Adleman. Uma desvantagem dos algoritmos de criptografia assimétrica existentes é o seu desempenho, que são mais lentos que os métodos simétricos.

Sendo assim, na prática, a criptografia assimétrica é utilizada para definir uma chave de sessão, que será usada na criptografia simétrica durante a comunicação. Esse é o funcionamento dos protocolos SSL e TLS, usados largamente na Internet.

Na criptografia assimétrica, as chaves públicas podem ser forjadas, fazendo com que o emissor não obtenha a chave pública correta do destinatário. Para solucionar esse problema, os engenheiros da Internet criaram a figura da Autoridade Certificadora, que funciona como um cartório, autenticando as chaves públicas das pessoas.

É essa autenticação da chave pública do seu banco, por exemplo, que faz o seu navegador exibir o singelo cadeado de segurança, fazendo com que você saiba que o site é mesmo do banco e não de um criminoso.

Esses aplicativos de mensagens oferecem a criptografia de ponta-a-ponta, que pressupõe proteção de conteúdo das mensagens trocadas entre os usuários numa mecânica em que nem mesmo o próprio administrador dos aplicativos pode ler o conteúdo.

Ponta-a-ponta é um sinônimo para o tipo assimétrico, e no caso específico desses aplicativos, se refere ao fato de que cada usuário dentro dessas redes possui uma chave de criptografia específica que é combinada com a de seus contatos durante a troca de mensagens. Dessa forma, o conteúdo trocado entre duas pessoas pelos mensageiros só é visível por elas.

Criptografia no Computador e no Celular

Ainda é muito comum associar o uso da criptografia diretamente com a proteção de dados na Internet: com a técnica, é muito mais difícil o criminoso descobrir seu login e senha de qualquer site e seus dados bancários são protegidos a cada compra.

Mas a criptografia tem aplicações que vão além disso. No computador, caso você decida criptografar seus dados, o windows ou macOS aplicarão uma chave criptográfica que protegerá todo o conteúdo armazenado na máquina de forma que só se torne visível por quem possua a chave, no caso o seu PIN, senha de usuário na máquina, ou qualquer tipo de autenticação biométrica oferecida pelo Windows, por exemplo.

Para celulares android e iPhone (iOS) a mesma coisa é válida. Ao criptografar os dados no aparelho, você os torna essencialmente inacessíveis a um invasor.

Níveis de Segurança

A critpografia depende da aplicação e do nível de segurança exigido, mas em linhas gerais, uma critpografia de 128 bits é muito mais segura do que uma de 56 bits, por exemplo.

Uma chave de 56 bits oferece 72 quatrilhões de possibilidades de troca de caracteres para ocultar uma mensagem (parece absurdo, mas computadores já podem fazer bilhões de operações por segundo, então 56 bits pode não ser tão seguro assim se o hacker possuir um aplicativo que tenta milhões de alternativas para quebrar a critpografia a cada segundo).

Para comparar, uma chave de 128 bits tem 339,000,000,000,000,000,000,000,000,000,000,000 de possibilidades (arredondando, há uns trilhões a mais)

Criptografia

A criptografia é uma técnica utilizada há anos que com o passar do tempo evoluiu a ponto de oferecer soluções eficazes no que diz respeito à segurança da informação. Hoje, ela é uma ferramenta de segurança amplamente utilizada nos meios de comunicação e consiste basicamente na transformação de determinado dado ou informação a fim de ocultar seu real significado.

Este artigo apresenta os conceitos sobre criptografia, seus tipos, aplicabilidade e como ela é empregada no .NET por meio do namespace System.Security.Cryptography. Ao final do artigo será desenvolvida uma aplicação para criptografar dados usando um algoritmo simétrico. Além disso, iremos criar uma DLL contendo a classe de criptografia implementada, que poderá ser reutilizada em outros projetos.

Em que Situação o Tema é Útil

A criptografia pode ser utilizada em aplicações e ambientes cuja segurança das informações é algo relevante para o projeto, principalmente em sistemas WEB, onde o dado trafega em um meio público correndo um risco maior de ser interceptado, fato este que pode gerar prejuízos enormes para uma organização. O domínio das técnicas de criptografia não é algo complexo quando estamos trabalhando com o paradigma orientado a objetos, sendo essencial para a criação de aplicações seguras.

Há pouco tempo, quando a tecnologia ainda não era muito presente em nosso cotidiano, as informações e grande parte dos processos organizacionais eram geridos basicamente no papel, sendo armazenados em armários ou cofres protegidos por cadeados ou senhas.

Atualmente este paradigma mudou, pelo menos para uma parcela significativa da sociedade. As informações são processadas e armazenadas em meios digitais, criando uma forte dependência entre os sistemas de informação e as organizações. Com o advento da internet, os dados trafegam em meios públicos, podendo ser interceptado por qualquer um que esteja mal intencionado. Neste cenário, uma falha na segurança destes conteúdos pode acarretar em enormes prejuízos para uma corporação.

Então, o que fazer para garantir tal segurança? Existem diversos meios de proteção e um deles é o uso da criptografia. Ela não vai impedir que uma determinada informação seja interceptada, mas tem o objetivo de dificultar a compreensão do dado capturado. Mas como isso é feito? Há vários algoritmos de criptografia que cumprem este papel, cada um com suas particularidades, porém a ideia central é a mesma: modificar a informação de forma que apenas o destinatário consiga compreender a que foi transmitido.

Vale ressaltar que a criptografia não é aplicada apenas quando um dado é enviado de um local a outro, ela é utilizada também em dispositivos de armazenamento de dados (ex: discos rígidos, pen drives,

storages), que são alvos de ataques e roubos. Ou seja, de uma forma geral, a criptografia vai garantir a confidencialidade da informação. Nos próximos tópicos, veremos alguns conceitos relacionados a esta técnica.

Criptografia Simétrica

A criptografia simétrica foi o primeiro tipo de criptografia criado. Os algoritmos que a utilizam têm como característica principal o uso de uma mesma chave criptográfica (Nota do DevMan 1) para criptografar ou descriptografar uma informação, por isso o adjetivo "simétrico" dá nome a esta técnica. Exemplificando um pouco este conceito, quando um emissor cifra uma mensagem com um algoritmo de criptografia simétrico, ele utiliza uma chave, que é representada por uma senha ou um conjunto de bits para codificar os dados. O receptor então faz uso do algoritmo para descriptografar a mensagem e aplica a mesma chave que foi utilizada pelo emissor para voltar à mensagem em sua forma original. Sem a mesma, não é possível decifrar a informação recebida.

Nota do DevMan 1

Chave criptográfica é um conjunto de caracteres formando uma sequência de bits que trabalhando em conjunto com um algoritmo de criptografia irão determinar o resultado final do processo de cifragem e decifragem da mensagem. O nível de segurança da codificação depende tanto do algoritmo quanto do tamanho da chave escolhida (total de bits que ela possui).

Uma forma muita utilizada por invasores para descobrir esta chave é utilizando a força bruta, onde são utilizadas inúmeras combinações de caracteres na tentativa de uma delas ser a chave do algoritmo. Veja na Figura 1 o processo de criptografia simétrica. Observe que a mesma chave é utilizada nos algoritmos para cifragem e decifragem do texto.

Figura 1. Processo de criptografia simétrica.

Como vantagens deste método podemos citar a simplicidade na sua implementação, uma vez que é utilizada uma única chave no processo de cifragem e decifragem do dado, além da velocidade deste processo em relação à criptografia assimétrica, que veremos nos próximos tópicos, possibilitando assim que uma grande quantidade de dados seja encriptada em pouco tempo.

Por outro lado este modelo de criptografia apresenta algumas falhas que estão relacionadas à geração e compartilhamento das chaves: no primeiro caso uma chave muito simples pode ser facilmente quebrada utilizando um algoritmo de força bruta. Já na segunda situação deve-se atentar para a forma como as chaves são compartilhadas entre os interessados na informação, a fim de evitar que a mesma seja obtida por um invasor.

Alguns algoritmos de criptografia simétrica bem conhecidos são: DES (Data Encryption Standart), Triple DES, AES (Advanced Encryption Standard), IDEA (International Data Encryption Algorithm), Blowfish, RC4.

Criptografia Assimétrica

A criptografia assimétrica, também denominada como criptografia de chave pública, possui como característica básica o uso de duas chaves ao invés de uma, sendo elas:

Chave pública: Chave que pode ser distribuída para outros usuários.

Chave privada. Chave que deve ser mantida em segredo.

A criptografia diz respeito a conceitos e técnicas usadas para codificar uma informação, de tal forma que somente seu real destinatário e o emissor da mensagem possam acessá-la, com o objetivo de evitar que terceiros interceptem e entendam a mensagem.

Atualmente, as técnicas de criptografia mais conhecidas envolvem o conceito das chaves criptográficas, que são um conjunto de bits, baseados em um algarismo capaz de interpretar a informação, ou seja, capaz de codificar e decodificar. Se a chave do receptor não for compatível com a do emissor, a informação então não será extraída.

O termo criptografia surgiu da fusão das palavras gregas "kryptós" e "gráphein", que significam "oculto" e "escrever", respectivamente. Trata-se de um conjunto de conceitos e técnicas que visa codificar uma informação de forma que somente o emissor e o receptor possam acessá-la, evitando que um intruso consiga interpretá-la. Para isso, uma série de técnicas são usadas e muitas outras surgem com o passar do tempo.

Na computação, as técnicas mais conhecidas envolvem o conceito de chaves, as chamadas chaves criptográficas. Trata-se de um conjunto de bits baseado em um determinado algoritmo capaz de codificar e de decodificar informações. Se o receptor da mensagem usar uma chave incompatível com a chave do emissor, não conseguirá extrair a informação.

Existem dois tipos de chave: a chave pública e a chave privada.

A chave pública é usada para codificar as informações, e a chave privada é usada para decodificar. Assim, na pública, todos têm acesso, mas para 'abrir' os dados da informação, que aparentemente são sem sentido, é preciso da chave privada, que só o emissor e receptor originais têm.

Atualmente, a criptografia pode ser considerada um método 100% seguro, ou seja, quem a utiliza para mandar e-mails e proteger seus arquivos, estará protegido contra fraudes e tentativas de invasão.

Os termos 'chave de 64 bits' e 'chave de 128 bits' são usados para expressar o tamanho da chave, assim, quanto mais bits forem utilizados, mais segura será essa criptografia. Um exemplo disso é se um algoritmo usa uma chave de 8 bits, por exemplo, apenas 256 chaves poderão ser utilizadas para decodificar essa informação, porque 2 elevado a 8 é igual a 256. Assim, um terceiro pode tentar gerar 256 tentativas de combinações e decodificar a mensagem, que mesmo sendo uma tarefa difícil, não é impossível. Por isso, quanto maior o número de bits, mais segura será a criptografia.

Existem dois tipos de chaves criptográficas, as chaves simétricas e as chaves assimétricas.

Chave Simétrica

É um tipo de chave simples, que é usada para a codificação e decodificação. Entre os algoritmos que usam essa chave, estão:

DES (Data Encryption Standard): Faz uso de chaves de 56 bits, que corresponde à aproximadamente 72 quatrilhões de combinações. Mesmo sendo um número absurdamente alto, em 1997, conseguiram quebrar esse algoritmo através do método de 'tentativa e erro', em um desafio na internet.

RC (Ron's Code ou Rivest Cipher): É um algoritmo muito utilizado em e-mails e usa chaves de 8 a 1024 bits, além de possuir várias versões que se diferem uma das outras pelo tamanho das chaves.

EAS (Advanced Encryption Standard): Hoje em dia é um dos melhores e mais populares algoritmo de criptografia existente. Voce pode definir o tamanho da chave como sendo de 128bits, 192bits ou 256bits.

IDEA (International Data Encryption Algorithm): É um algoritmo que usa chaves de 128 bits, parecido com o DES. Seu ponto forte é a fácil implementação de software.

As chaves simétricas não são totalmente seguras quando se trata de informações muito valiosas, principalmente pelo fato de que o emissor e o receptor têm que conhecer a mesma chave. Assim, a transmissão pode não ser segura e o conteúdo chegar a terceiros.

Chave Assimétrica

A chave assimétrica utiliza duas chaves: a privada e a pública. Elas se resumem da seguinte forma: a chave pública para codificar e a chave privada para decodificar, levando-se em consideração que a chave privada é secreta.

Entre os algoritmos utilizados, estão:

RSA (Rivest, Shamir and Adleman): É um dos algoritmos de chave assimétrica mais utilizados, em que dois números primos (aqueles que só podem ser divididos por 1 e por eles mesmos) são multiplicados para a obtenção de um terceiro valor. Para isso, é preciso fazer fatoração, que é descobrir os dois primeiros números a partir do terceiro, que é um cálculo trabalhoso. Assim, se números grandes forem utilizados, será praticamente impossível descobrir o código. A chave privada do RSA são os números que são multiplicados e a chave pública é o valor que será obtido.

O termo criptografia surgiu da fusão das palavras gregas "kryptós" e "gráphein", que significam "oculto" e "escrever", respectivamente. Trata-se de um conjunto de conceitos e técnicas que visa codificar uma informação de forma que somente o emissor e o receptor possam acessá-la, evitando que um intruso consiga interpretá-la.

Para isso, uma série de técnicas são usadas e muitas outras surgem com o passar do tempo.

Na computação, as técnicas mais conhecidas envolvem o conceito de chaves, as chamadas chaves criptográficas. Trata-se de um conjunto de bits baseado em um determinado algoritmo capaz de codificar e de decodificar informações. Se o receptor da mensagem usar uma chave incompatível com a chave do emissor, não conseguirá extrair a informação.

Os primeiros métodos criptográficos existentes usavam apenas um algoritmo de codificação. Assim, bastava que o receptor da informação conhecesse esse algoritmo para poder extraí-la. No entanto, se um intruso tivesse posse desse algoritmo, também poderia efetuar um processo de decifragem, caso capturasse os dados criptografados.

Há ainda outro problema: imagine que a pessoa A tivesse que enviar uma informação criptografada à pessoa B. Esta última teria que conhecer o algoritmo usado. Imagine agora que uma pessoa C também precisasse receber uma informação da pessoa A, porém a pessoa C não poderia descobrir qual é a informação a ser enviada à pessoa B. Se a pessoa C capturasse a informação enviada à pessoa B, também conseguiria decifrá-la, pois quando a pessoa A enviou sua informação, a pessoa C também teve que conhecer o algoritmo usado. Para a pessoa A evitar esse problema, a única solução seria utilizar um algoritmo diferente para cada receptor.

Com o uso de chaves, um emissor pode usar o mesmo algoritmo (o mesmo método) para vários receptores. Basta que cada um receba uma chave diferente. Além disso, caso um receptor perca ou exponha determinada chave, é possível trocá-la, mantendo-se o mesmo algoritmo.

Você já deve ter ouvido falar de chave de 64 bits, chave de 128 bits e assim por diante. Esses valores expressam o tamanho de uma determinada chave. Quanto mais bits forem utilizados, mais segura será a criptografia. Explica-se: caso um algoritmo use chaves de 8 bits, por exemplo, apenas 256 chaves poderão ser usadas na decodificação, pois 2 elevado a 8 é 256. Isso deixa claro que 8 bits é inseguro, pois até uma pessoa é capaz de gerar as 256 combinações (embora demore), imagine então um computador! Porém, se forem usados 128 ou mais bits para chaves (faça 2 elevado a 128 para ver o que acontece), teremos uma quantidade extremamente grande de combinações, deixando a informação criptografada bem mais segura.

Chaves Simétricas e Assimétricas

Há dois tipos de chaves criptográficas: chaves simétricas e chaves assimétricas. Ambas são abordadas a seguir:

Chave Simétrica

Esse é um tipo de chave mais simples, onde o emissor e o receptor fazem uso da mesma chave, isto é, uma única chave é usada na codificação e na decodificação da informação. Existem vários algoritmos que usam chaves simétricas, como o DES, o IDEA, e o RC:

- DES (Data Encryption Standard): criado pela IBM em 1977, faz uso de chaves de 56 bits. Isso corresponde a 72 quatrilhões de combinações. É um valor absurdamente alto, mas não para um computador potente. Em 1997, esse algoritmo foi quebrado por técnicas de "força bruta" (tentativa e erro) em um desafio promovido na internet;

- IDEA (International Data Encryption Algorithm): criado em 1991 por James Massey e Xuejia Lai, o IDEA é um algoritmo que faz uso de chaves de 128 bits e que tem uma estrutura semelhante ao DES. Sua implementação em software é mais fácil do que a implementação deste último;

- RC (Ron's Code ou Rivest Cipher): criado por Ron Rivest na empresa RSA Data Security, esse algoritmo é muito utilizado em e-mails e faz uso de chaves que vão de 8 a 1024 bits. Possui várias versões: RC2, RC4, RC5 e RC6. Essencialmente, cada versão difere da outra por trabalhar com chaves maiores.

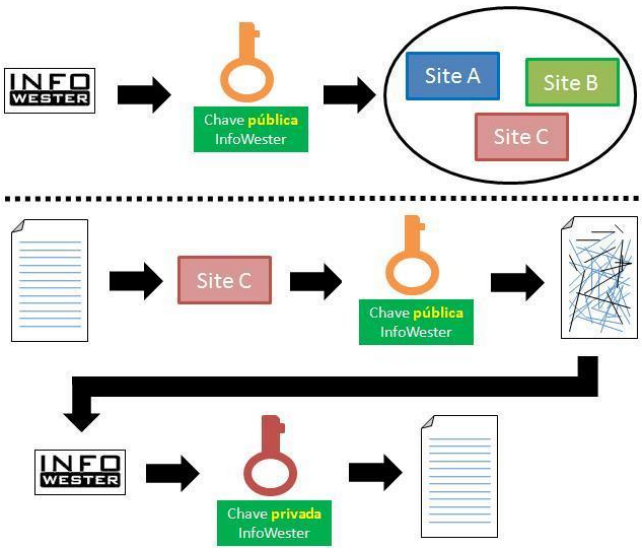
Há ainda outros algoritmos conhecidos, como o AES (Advanced Encryption Standard) - que é baseado no DES - , o 3DES, o Twofish e sua variante Blowfish, entre outros.

O uso de chaves simétricas tem algumas desvantagens, fazendo com que sua utilização não seja adequada em situações onde a informação é muito valiosa. Para começar, é necessário usar uma grande quantidade de chaves caso muitas pessoas ou entidades estejam envolvidas. Ainda, há o fato de que tanto o emissor quanto o receptor precisam conhecer a mesma chave. A transmissão dessa chave de um para o outro pode não ser tão segura e cair em "mãos erradas".

Chave Assimétrica

Também conhecida como "chave pública", a chave assimétrica trabalha com duas chaves: uma denominada privada e outra denominada pública. Neste método, um emissor deve criar uma chave de codificação e enviá-la ao receptor. Essa é a chave pública. Uma outra chave deve ser criada para a decodificação. Esta, a chave privada, é secreta.

Para melhor compreensão, imagine o seguinte: O InfoWester criou uma chave pública e a enviou a vários outros sites. Quando qualquer desses sites quiser enviar uma informação criptografada ao InfoWester deverá utilizar a chave pública deste. Quando o InfoWester receber essa informação, apenas será possível extraí-la com o uso da chave privada, que só o InfoWester tem. Caso o InfoWester queira enviar uma informação criptografada a outro site, deverá obter uma chave pública fornecida por este.



Entre os algoritmos que usam chaves assimétricas, têm-se o RSA (o mais conhecido) e o Diffie-Hellman:

RSA (Rivest, Shamir and Adleman): criado em 1977 por Ron Rivest, Adi Shamir e Len Adleman nos laboratórios do MIT (Massachusetts Institute of Technology), é um dos algoritmos de chave assimétrica mais usados. Nele, números primos (número primo é aquele que só pode ser dividido por 1 e por ele mesmo) são utilizados da seguinte forma: dois números primos são multiplicados para se obter um terceiro valor.

Porém, descobrir os dois primeiros números a partir do terceiro (ou seja, fazer uma fatoração) é muito trabalhoso. Se dois números primos grandes (realmente grandes) forem usados na multiplicação, será necessário usar muito processamento para descobrí-los, tornando essa tarefa praticamente inviável. Basicamente, a chave privada no RSA são os números multiplicados e a chave pública é o valor obtido;

ElGamal: criado por Taher ElGamal, esse algoritmo faz uso de um problema matemático conhecido por "logaritmo discreto" para se tornar seguro. Sua utilização é freqüente em

Existem ainda outros algoritmos, como o DSA (Digital Signature Algorithm), o Schnorr (praticamente usado apenas em assinaturas digitais) e Diffie-Hellman.

Certificação Digital

Um recurso conhecido por certificação digital é muito utilizado com chaves públicas. Trata-se de um meio que permite, por exemplo, provar que um certo documento eletrônico foi mesmo emitido por uma determinada entidade ou pessoa. O receptor da informação usará a chave pública fornecida pelo emissor para se certificar da origem. Além disso, a chave fica integrada ao documento de forma que qualquer alteração por terceiros imediatamente a invalide.

Criptografia (do grego kryptos, oculto, e graphein, escrever) é o nome dado a um conjunto de regras que visa codificar a informação a de maneira que só o emissor e o receptor consiga decifrá-la.

A troca de informações sigilosas é uma prática antiga, existente há centenas de anos, e que até bem pouco tempo era predominante em meio aos livros e documentos. O surgimento da internet e a facilidade que esta proporciona de transmitir dados de maneira precisa e extremamente rápida fez de tal prática um recurso essencial para permitir que apenas emissor e receptor obtenham acesso livre à informação tratada.

A criptografia segue quatro princípios básicos: confidencialidade, autenticação, integridade da informação e não repudiabilidade (ou seja, o remetente não pode negar o envio da informação). Apesar de ser recurso importante na transmissão de informações pela internet, a criptografia não é capaz de garantir total segurança, pois sempre existe alguém que consegue desenvolver uma maneira de "quebrar" o código. Assim, as técnicas são constantemente aperfeiçoadas e tantas outras são criadas, como por exemplo a "criptografia quântica".

A primeira técnica utilizava apenas um algoritmo de decodificação. Assim, bastava o receptor do algoritmo para decifrá-la, mas caso um intruso conhecesse esse mesmo algoritmo, ele poderia decifrar a informações se interceptasse os dados criptografados. Hoje, entre as técnicas mais conhecidas há o conceito de chaves, ou então chaves criptográficas, no qual um conjunto de bits baseado em um determinado algoritmo é capaz de codificar e de decodificar informações.

Há dois tipos de chaves, a simétrica e a assimétrica, ou chave pública. Caso o receptor da mensagem resolva usar uma chave incompatível com a chave do emissor, a informação não será compartilhada. Há ainda outros conceitos envolvidos na área da criptografia, como a Função Hashing, usada em assinaturas digitais para garantir integridade, e as aplicações, como a certificação digital.

O avanço das técnicas de invasão e interceptação de dados forçou a consequente evolução da criptografia, que adotou codificações de 256, 512 e até 1024 bits. Isso significa que são geradas 21024combinações diferentes de chaves para cada mensagem enviada, sendo que apenas uma é correta, de conhecimento apenas do emissor e do receptor.

Com a intenção de ajudar na defesa da liberdade individual nos Estados Unidos e no mundo inteiro, Philip Zimmermman desenvolveu o PGP (Pretty Good Privacy) em 1991. Disponibilizado gratuitamente, o PGP se tornou um dos meios de criptografia mais conhecidos, principalmente na troca de e-mails, utilizando chaves assimétricas. O software pode realizar também um segundo tipo de criptografia através de uma "chave de sessão" método que representa um tipo de chave simétrica.

Consiste em cifrar um arquivo ou mensagem usando um conjunto de cálculos. O arquivo cifrado (ou encriptado) torna-se incompreensível até que seja desencriptado. Os cálculos usados para encriptar ou desencriptar o arquivo são chamados de chaves. Apenas alguém que tenha a chave poderá ler o arquivo criptografado.

Existem basicamente dois sistemas de uso de chaves. No primeiro são usadas chaves simétricas, onde as duas partes possuem a mesma chave, usada tanto para encriptar quanto para desencriptar os arquivos. No segundo sistema temos o uso de duas chaves diferentes, chamadas de chave pública e chave privada. A chave pública serve apenas para encriptar os dados e pode ser livremente distribuída, a chave privada por sua vez é a que permite desencriptar os dados.

Neste sistema o usuário A, interessado em enviar um arquivo para o usuário B encriptaria o arquivo utilizando a chave pública do usuário B, distribuída livremente, e ao receber o arquivo o usuário B utilizaria sua chave privada, que é secreta para desencriptar o arquivo e ter acesso a ele. Ninguém mais além do usuário B poderia ter acesso ao arquivo, nem mesmo o usuário A que o encriptou.

Existem vários níveis de criptografia e inclusive sistemas que utilizam vários níveis, encriptando várias vezes o mesmo arquivo utilizando chaves diferentes. Em geral, quanto mais complexo, for o sistema, mais seguro.