

CRIPTOGRAFIA





Criptografia é um sistema de algoritmos matemáticos que codificam dados do usuário para que só o destinatário possa ler. Por mais simples que possa parecer, a matemática e os passos adicionais podem se tornar difíceis para os principiantes. Mas, antes que você decida adiar isso em troca de outras maneiras para proteger suas comunicações online, alguns exemplos podem convencê-lo de que a criptografia é um dos melhores métodos para proteger sua privacidade, mesmo em momentos em que você acha que ela não conta.

Telefonemas, e-mails, compras online, mídia social e navegação em geral são atividades online que não podemos dispensar em nossas vidas. Enquanto estamos constantemente procurando ou compartilhando informações online, nossos dados estão essencialmente armazenados em algum lugar. A maioria das pessoas não tem certeza onde é esse “algum lugar”, mas esses dados deveriam estar disponíveis só para o provedor de serviço de intermediação de sua conversa. Porém, ela pode estar visível para as empresas de telecomunicação transportando seus pacotes de Internet e, assim, suas comunicações supostamente privadas e seguras podem ser interceptadas.

Como muitos casos provaram, dados de usuários e empresas estão cada vez mais sendo alvos de hackers e cibercriminosos, resultando em violações de dados e ataques direcionados. Só essa razão deveria servir como um alerta para os que não pensaram em proteger suas comunicações por meio de criptografia.

A criptografia reforça a segurança de uma mensagem ou arquivo embaralhando o conteúdo. Para criptografar uma mensagem, você também precisa da chave certa para decodificá-la. É o modo mais eficaz para ocultar comunicações através de informações em código, onde o remetente e o destinatário têm a chave para decifrar os dados. O conceito não é diferente de crianças que inventam palavras de código secreto e outras maneiras discretas para se comunicar, pelas quais só elas são capazes de entender a mensagem. Criptografia é como enviar de mensagens secretas entre grupos – se alguém tenta bisbilhotar sem as chaves certas, não conseguirá entender a mensagem.

Existem dois métodos de criptografia: criptografia simétrica e assimétrica. Criptografia simétrica, também conhecida como criptografia de chave secreta, diz respeito ao remetente e o destinatário, sendo que a mesma chave é usada para criptografar e decodificar uma mensagem. A criptografia assimétrica, ou criptografia de chave pública usa o que é chamado de um ‘par de chaves’ – uma chave pública para criptografar a mensagem e uma chave privada para decodificá-la.

Papel da criptografia simétrica na segurança da comunicação

Contra esses adversários, podemos utilizar a criptografia. Se voltarmos às perguntas no início do texto, veremos como a encriptação de dados é importante, pois garante o sigilo das mensagens. Essa técnica, no padrão de segurança TLS, utiliza cifras simétricas como AES, Salsa20, dentre outras. Tais cifras são designadas “simétricas” porque ambos lados da comunicação devem utilizar uma mesma chave para encriptar e decriptar as mensagens. A outra alternativa seriam os algoritmos de encriptação ditos assimétricos, que utilizam chaves diferentes para encriptar e decriptar as mensagens, no entanto, por questão de eficiência o padrão é utilizar algoritmos simétricos na comunicação entre os computadores e servidores.

O uso da criptografia assimétrica

Para estabelecer uma chave simétrica que permita encriptar as mensagens, bem como verificar sua integridade, é necessário fazer uso da criptografia assimétrica, ou também chamada de criptografia de chave pública.

Ela recebe esse nome pois baseia-se em pares de chaves, na qual uma é secreta e outra é pública. Dessa forma, um participante de uma comunicação conhece as chaves públicas dos outros participantes, enquanto sua chave secreta é conhecida e acessada apenas por ele.

Para elucidar como a criptografia assimétrica é utilizada, vamos recorrer aos personagens mais famosos da criptografia: Alice e Bob.

Digamos que Alice deseja estabelecer uma comunicação segura com Bob e, para isso, deve concordar com Bob em uma chave simétrica (conhecida apenas por ela e Bob) para utilizar os algoritmos simétricos que vão garantir confidencialidade e integridade da comunicação.

Para tanto, Alice pode utilizar diferentes estratégias para troca de chaves (i.e.: estabelecimento da chave simétrica). Uma maneira bastante simples é gerar uma chave (simétrica) aleatoriamente e utilizar a chave pública de Bob em um sistema de encriptação assimétrico para encriptar essa chave recém gerada.

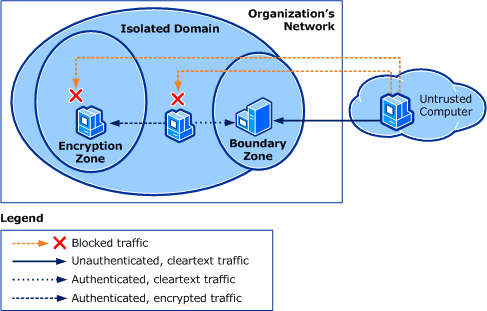
Dessa forma Alice pode enviar a mensagem encriptada a Bob e apenas ele será capaz de decriptar e recuperar a chave simétrica a ser utilizada doravante na comunicação – sem dar chances de que um adversário intercepte a comunicação e tenha acesso à chave simétrica ou ao conteúdo das demais mensagens encriptadas com essa chave.

Essa estratégia é chamada de envelopamento digital, em analogia ao conteúdo da mensagem (nesse caso, a chave simétrica) protegida por um “envelope digital”, que consiste na encriptação do conteúdo utilizando criptografia assimétrica.

Utilização de criptografia no Windows Server

Para os dispositivos que compartilham informações confidenciais na rede, o Windows Defender firewall com segurança avançada permite que você exija que todo o tráfego de rede seja criptografado. Usar a criptografia pode ajudá-lo a atender a requisitos regulatórios e legais, como aqueles encontrados na lei federal de gerenciamento de segurança das informações da 2002 (FISMA), a lei Sarbanes-Oxley do 2002, a lei de assistência médica e a lei de responsabilização da 1996 (HIPAA) e outras normas do governo e do setor. Ao criar regras de segurança de conexão que se aplicam a dispositivos que hospedam e trocam dados confidenciais, você pode ajudar a proteger a confidencialidade dos dados criptografando-os.

A ilustração a seguir mostra uma zona de criptografia em um domínio isolado. As regras que implementam o domínio isolado e as diferentes regiões são implantadas usando a política de grupo e o Active Directory.



Esse objetivo oferece os seguintes benefícios:

* Os dispositivos na zona de criptografia exigem autenticação para se comunicar com outros dispositivos. Isso não funciona de forma diferente da meta e do design de isolamento do domínio. Para obter mais informações, consulte [restringir o acesso a apenas dispositivos confiáveis](https://docs.microsoft.com/pt-br/windows/security/threat-protection/windows-firewall/restrict-access-to-only-trusted-devices).
* Os dispositivos na zona de criptografia exigem que todo o tráfego de rede de entrada e de saída seja criptografado.

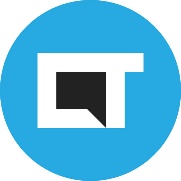
Por exemplo, o Woodgrove Bank processa dados confidenciais do cliente em um dispositivo que devem ser protegidos contra espionagem por dispositivos na rede. As regras de segurança de conexão especificam que todo o tráfego deve ser criptografado por um algoritmo de criptografia suficientemente complexo para ajudar a proteger os dados.

* Os dispositivos na zona de criptografia são geralmente bons candidatos para o isolamento do servidor, em que o acesso limita-se apenas a contas de computador e contas de usuário que são membros de um grupo de acesso autorizado. Em muitas organizações, a zona de criptografia e a zona de isolamento do servidor são uma e as mesmas. Para obter mais informações, consulte [restringir o acesso somente a usuários ou dispositivos especificados](https://docs.microsoft.com/pt-br/windows/security/threat-protection/windows-firewall/restrict-access-to-only-specified-users-or-devices).

Os seguintes componentes são necessários para esta distribuição:

* **Active Directory**: o Active Directory dá suporte ao gerenciamento centralizado de regras de segurança de conexão configurando as regras em um ou mais GPOs que podem ser automaticamente aplicadas a todos os dispositivos relevantes no domínio.

Fontes:



<https://canaltech.com.br/seguranca/criptografia-para-iniciantes-o-que-e-como-funciona-e-por-que-precisamos-dela-46753/>



<https://www.welivesecurity.com/br/2017/03/28/criptografia-simetrica-assimetrica/>



[https://docs.microsoft.com/pt-br/windows/security/threat- protection/windows-firewall/require-encryption-when-accessing-sensitive-network-resources](https://docs.microsoft.com/pt-br/windows/security/threat-%20%20%20protection/windows-firewall/require-encryption-when-accessing-sensitive-network-resources)