FIAP ON

BIOHACKING, DEEP WEB
E CRIPTOGRAFIA

Criptografia E VPNS

VINICIUS VIEIRA

5

LISTA DE FIGURAS

SUMÁRIO

5 CRIPTOGRAFIA E VPNS

5.1 Introdução

A Rede Mundial de Computadores geralmente não oferece segurança intrínseca, fim a fim, para seus usuários. Não existe, por exemplo, sigilo intrínseco para a informação que viaja de um ponto a outro na grande rede. A criptografia é a única tecnologia capaz de garantir o sigilo e a autenticidade da informação em trânsito pelos meios eletrônicos. A criptografia pode ser usada de muitas maneiras, sendo, muitas vezes, a principal linha de defesa contra bisbilhotagem (snooping) e falsificação (spoofing) (BRAGA; DAHAB, 2015).

A Criptografia (do grego kryptos, significando oculto) é a ciência que se dedica ao estudo e ao desenvolvimento das técnicas (matemáticas) utilizadas para tornar uma mensagem secreta. Historicamente, o verbo criptografar tem sido usado apenas nesse sentido. Entretanto, a criptografia moderna possui funções, como assinaturas digitais, resumo (hash) criptográfico e outras, que não se limitam a prover sigilo da informação (BRAGA; DAHAB, 2015).

De fato, a palavra Criptografia denota hoje um conjunto de técnicas matemáticas, das quais uma grande parte dos requisitos, mecanismos e serviços de segurança da informação não pode prescindir (BRAGA; DAHAB, 2015).

5.2 Objetivos e funções da criptografia

Conforme BRAGA e DAHAB (2015), historicamente associada ao sigilo, a criptografia moderna também oferece serviços para autenticação, integridade e irrefutabilidade. Os quatro serviços são os seguintes:

- **Confidencialidade (ou sigilo):** obtida com o uso da criptografia para manter a informação secreta, confidencial. Enviar e-mails encriptados e manter arquivos encriptados em cartões de memória são exemplos de confidencialidade.
- **Autenticação:** obtida com o uso da criptografia para validar a identidade de uma entidade. Um exemplo de autenticação é o uso de assinaturas

digitais para verificar a autoria de uma mensagem de texto ou de um documento eletrônico.

- **Integridade:** obtida com o uso da criptografia para garantir que uma porção de dados não foi modificada desde a sua criação. Códigos de detecção de erros são exemplos de mecanismos para a verificação de integridade de dados.
- **Irrefutabilidade:** obtida pelo uso da criptografia como meio de garantir que o autor de uma mensagem autêntica não possa negar para um terceiro a sua autoria.

Na prática, estes serviços são usados juntos. Por exemplo, uma mensagem de correio eletrônico pode ser encriptada e assinada digitalmente. Deste modo, tanto a confidencialidade quanto a autenticação estarão garantidas. Visto que a assinatura digital é única para a mensagem, a integridade também é preservada.

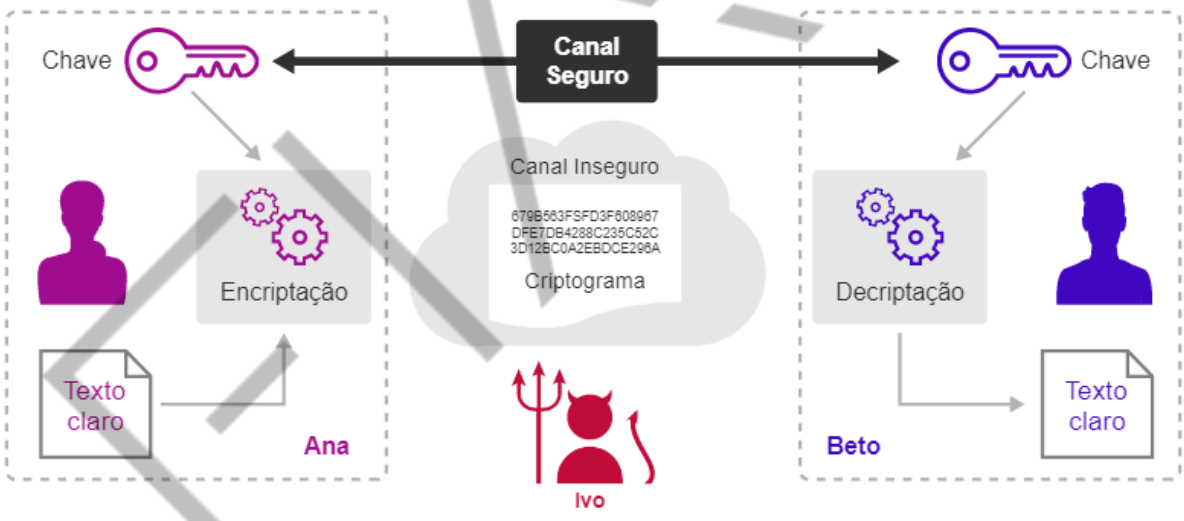

Figura 5.1 – Sistemas criptográficos
Fonte: Braga; Dahab (2015)

5.3 Sistemas criptográficos

De acordo com Braga e Dahab (2015), a Figura “Sistemas criptográficos” mostra um sistema criptográfico e seus elementos fundamentais. Três personagens ilustram a figura: Ana, a remetente das mensagens; Beto, o destinatário das mensagens; e Ivo, o adversário com desejo de conhecer os segredos de Ana e Beto. As mensagens passam por um canal de comunicação inseguro e controlado por Ivo. O algoritmo criptográfico é usado para transformar o texto em claro (legível por

qualquer um) em texto encriptado (o criptograma legível apenas por Ana e Beto) e vice-versa.

A chave criptográfica é o parâmetro de configuração do algoritmo que viabiliza a recuperação de um texto claro a partir do texto encriptado. Ana e Beto usam uma chave criptográfica conhecida apenas por eles e compartilhada (ou combinada) por um canal seguro diferenciado. Teoricamente, diz-se que a segurança do sistema criptográfico reside no segredo da chave e não no segredo do algoritmo criptográfico. Grosso modo, em sendo usado um algoritmo de boa reputação, a qualidade da implementação deste algoritmo e o tamanho da chave determinam a dificuldade em quebrar a encriptação da mensagem.

A figura acima tem os seguintes passos:

- Ana configura o algoritmo de encriptação com a chave compartilhada com Beto.
- Ana passa o texto claro para o algoritmo e obtém o criptograma.
- O criptograma é transmitido pelo canal inseguro e recebido por Beto.
- Beto configura o algoritmo de decriptação com a chave compartilhada com Ana.
- Beto decripta o criptograma recebido e obtém o texto claro original.

5.4 Ameaças comuns aos sistemas criptográficos

Conforme Braga e Dahab (2015), encontrar vulnerabilidades em sistemas criptográficos, em vez de nas implementações destes sistemas, é uma tarefa complexa, pois, normalmente, os algoritmos criptográficos modernos são bem projetados, com segurança demonstrável, e submetidos ao escrutínio de pesquisadores por um bom período de tempo. Geralmente, o “teste do tempo” pode ser interpretado como evidência de robustez do algoritmo.

Em termos práticos, algoritmos criptográficos passam a ter valor a partir do momento em que são implementados, seja em software ou em hardware, para prover confidencialidade, integridade, autenticidade e irrefutabilidade. Tradicionalmente, maior atenção tem sido dada à implementação confiável dos

algoritmos criptográficos, visto que estas implementações podem expor problemas relacionados com o algoritmo subjacente ou elas mesmas, introduzir vulnerabilidades.

Ainda conforme Braga e Dahab (2015), recentemente tem crescido o interesse no uso correto dos algoritmos e suas implementações. Uma implementação robusta de um sistema criptográfico é difícil de ser obtida, pois exige do desenvolvedor uma grande variedade de conhecimentos teóricos e práticos sobre criptografia, desenvolvimento de software seguro, arquitetura de computadores, compiladores, linguagens de programação, entre outras áreas da Ciência da Computação. Mesmo que o desenvolvedor possua esse tipo de conhecimento amplo e, ao mesmo tempo, profundo, defeitos de implementação ainda podem ocorrer.

Por causa destas dificuldades, em vez de tentar encontrar falhas nos algoritmos criptográficos, é mais fácil e prático para um adversário (Ivo) procurar por falhas não apenas nas implementações criptográficas, mas também, e às vezes principalmente, nos outros componentes dos sistemas criptográficos, por exemplo, as camadas de software que encapsulam ou utilizam as implementações criptográficas.

Conforme Braga e Dahab (2015), um ataque simples (porém, quase sempre impraticável) realizado por Ivo contra sistemas criptográficos é aquele conhecido como ataque de força bruta, no qual todas as possibilidades de chaves criptográficas são testadas na tentativa de decriptar corretamente o criptograma. Em geral, chaves longas são mais seguras, pois possuem um número maior de possibilidades.

Vale observar que todos os outros ataques listados a seguir são facilitados se o primeiro ataque for bem-sucedido e a chave secreta ou privada for comprometida (descoberta, adivinhada ou deduzida). Ivo pode atacar um sistema criptográfico (por exemplo, um canal de comunicação protegido com criptografia) das seguintes maneiras:

- Realizando um ataque de força bruta contra as chaves. Neste ataque, todas as chaves válidas possíveis são testadas na decriptação de um criptograma, para uma mensagem conhecida, até que a chave correta seja encontrada.

- “Grampeando” o canal. Grampear um canal aberto é relativamente simples, pois basta ler a informação em trânsito. Para grampear um canal seguro, é preciso não somente ler o criptograma em trânsito, mas também decriptá-lo. Para tal, seria necessário conhecer a chave de decriptação.
- Reenviando mensagens antigas. Este ataque é possível se as mensagens não são unicamente identificadas (por exemplo, com carimbos temporais – timestamps) ou não possuem códigos de autenticação, ou ainda se as chaves não são trocadas periodicamente e com frequência adequada.
- Personificando uma das partes comunicantes (Ana ou Beto). Ivo pode se fazer passar por Ana ou Beto pela substituição da chave de Ana/Beto pela sua própria, sem o conhecimento de Ana/Beto.
- Assumindo o papel do intermediário (Man-in-the-Middle). Para este ataque, Ivo obtém as chaves de Ana e de Beto; personifica tanto Ana quanto Beto; intercepta os criptogramas de Ana/Beto para Beto/Ana; decripta estes criptogramas e os encripta novamente com sua própria chave de encriptação, antes de reenviá-los.

5.5 Tipos de sistemas criptográficos

Como explicam Braga e Dahab (2015), existem dois tipos de sistemas criptográficos, comumente conhecidos como criptografia de chave secreta (ou simétrica) e criptografia de chave pública (ou assimétrica). Na criptografia de chave secreta, uma única chave é usada para encriptar e decriptar a informação. Na criptografia de chave pública, duas chaves são necessárias.

Uma chave é usada para encriptar; a outra chave, diferente, é usada para decriptar a informação. Estas duas chaves são matematicamente relacionadas e trabalham aos pares, de modo que o criptograma gerado com uma chave deve ser decriptado pela outra chave do par. Cada chave inverte o trabalho da outra e nenhuma pode ser usada sozinha em um sistema criptográfico. Nos sistemas de chave pública, uma das chaves do par é dita privada (a de decriptação), a outra é feita pública (a de encriptação).

5.5.1 Criptografia de chave secreta

De acordo com Braga e Dahab (2015), os sistemas criptográficos de chave secreta modernos possuem geralmente bom desempenho, mesmo em computadores considerados lentos. Com esta tecnologia, apenas uma chave é usada para encriptar e decriptar a informação.

A Figura “Sistema criptográfico simétrico” ilustra os passos da encriptação com algoritmos simétricos de chave secreta:

- Ana configura o algoritmo para o modo de encriptação com a chave secreta.
- Ana alimenta o algoritmo com a mensagem original, o texto claro.
- Ana encripta a mensagem e obtém o criptograma (mensagem encriptada).

Apenas a chave usada na encriptação pode decriptar corretamente a informação. Por isso, esta chave deve ser protegida e guardada em segredo; daí o nome de chave secreta. A Figura “Sistema criptográfico simétrico” também ilustra os passos da decriptação com chave secreta:

- Beto configura o algoritmo para o modo de decriptação com a chave secreta.
- Beto alimenta o algoritmo com a mensagem encriptada (criptograma).
- Beto decripta a mensagem encriptada e obtém o texto claro original.

Teoricamente, este sistema criptográfico pode ser diretamente utilizado para encriptação bidirecional com a mesma chave. Porém, conforme tratado adiante neste texto, na prática, diversos detalhes de implementação dificultam a utilização segura da mesma chave para a encriptação nas duas direções do canal de comunicação.

De acordo com Braga e Dahab (2015), na criptografia simétrica, a chave secreta deve ser conhecida por todos aqueles que precisam decriptar a informação encriptada com ela. Mas como compartilhar a chave secreta sem que ela seja descoberta pelos adversários? Uma solução seria marcar um encontro secreto com todos que devem conhecer a chave. Porém, na Internet, isto não é fácil, afinal, usa-se a Internet quando encontros presenciais são difíceis. Sabe-se que a Internet é

insegura por natureza (por isso, usar a criptografia), então, não se pode simplesmente distribuir a chave secreta por e-mail ou mensagem de texto. A distribuição de chaves é um aspecto importante da criptografia de chave secreta.

Apesar das dificuldades de distribuição de chaves, a criptografia de chave secreta é muito usada. Suas dificuldades aparentes podem ser contornadas pela combinação desta tecnologia com a criptografia de chave pública, originando sistemas criptográficos híbridos.

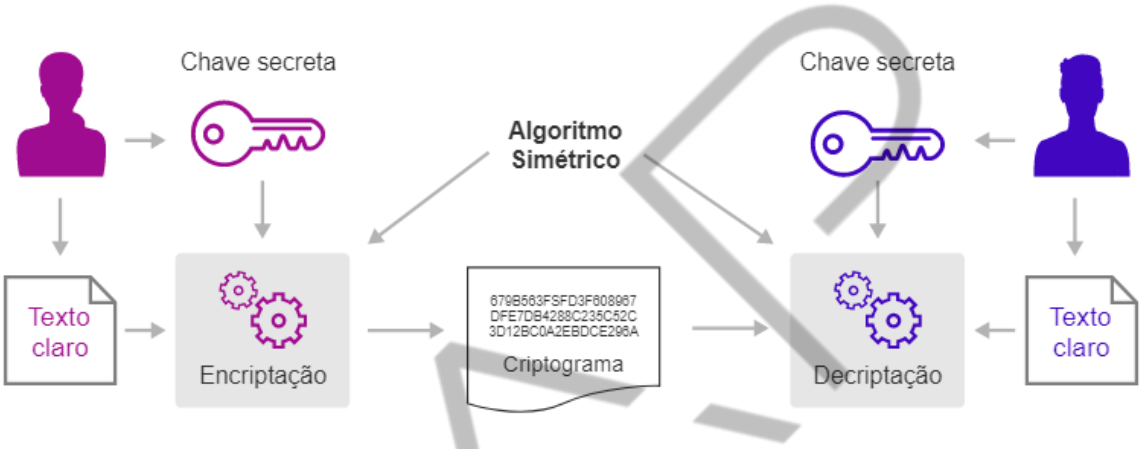

Figura 5.2 – Sistema criptográfico simétrico
Fonte: Braga e Dahab (2015)

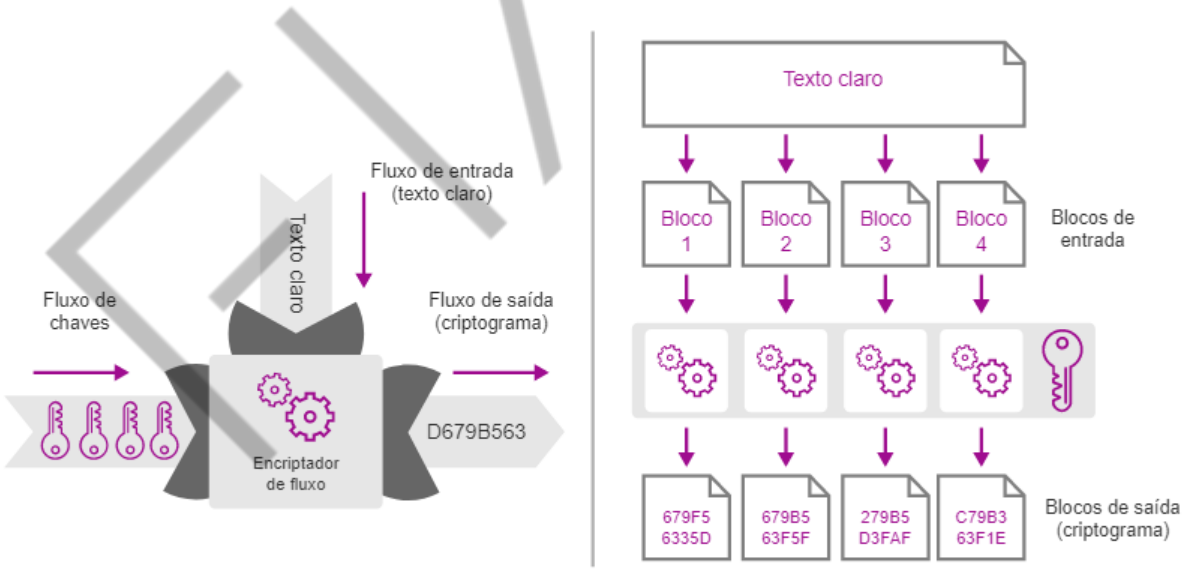

Figura 5.3 – Encriptadores de fluxo (à esquerda) e de bloco (à direita)
Fonte: Braga e Dahab (2015)

5.5.2 Encriptadores de fluxo e de bloco

Segundo Braga e Dahab (2015), existem duas categorias de algoritmos simétricos, como mostra a Figura Encriptadores de fluxo (à esquerda) e de bloco (à

direita), ou seja, os encriptadores de fluxo e de bloco. Nos encriptadores de bloco, o texto claro é quebrado em blocos de bits de tamanho fixo. O encriptador trabalha sobre blocos e produz saídas em blocos também. O tamanho da chave criptográfica é geralmente um múltiplo do tamanho do bloco.

Os encriptadores de fluxo atuam sobre sequências (de bits). A sequência ou fluxo de entrada é transformado continuamente na sequência ou fluxo de saída, bit a bit. É importante que a chave criptográfica seja uma sequência de bits pelo menos do mesmo tamanho do fluxo de entrada. Na prática, os bits da chave podem ser produzidos por um gerador de sequências de bits pseudoaleatórias, a partir de uma chave mestra de tamanho fixo.

5.5.3 Criptografia de chave pública

De acordo com Braga e Dahab (2015), devido à complexidade das operações matemáticas envolvidas, a criptografia de chave pública tradicional possui, em geral, um desempenho pior se comparada à criptografia de chave secreta, no mesmo hardware. A criptografia de chave pública utiliza duas chaves, que são relacionadas matematicamente e construídas para trabalharem juntas.

Uma das chaves do par é dita a chave privada (pessoal) e é mantida em segredo, sendo conhecida apenas pelo dono do par de chaves. A outra chave do par é dita a chave pública por poder ser conhecida publicamente. A criptografia de chave pública pode ser usada para obter sigilo. Neste caso, a encriptação com a chave pública torna possível que qualquer um envie criptogramas para o dono da chave privada.

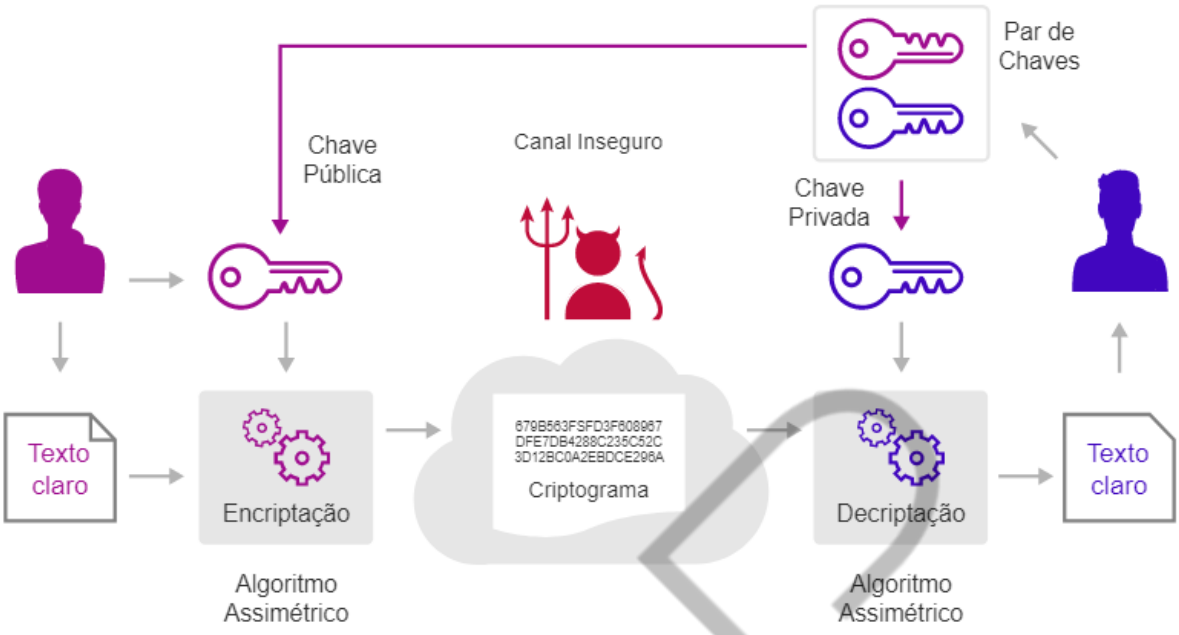

Figura 5.4 – Sistema criptográfico assimétrico para sigilo
Fonte: Braga e Dahab (2015)

5.5.4 Encriptação para sigilo e privacidade

Conforme Braga e Dahab (2015), a Figura: Sistema criptográfico assimétrico para sigilo ilustra um sistema criptográfico assimétrico para sigilo e seus elementos básicos. Mais uma vez, Ana, Beto e Ivo são os personagens. As mensagens de Ana para Beto são transmitidas por um canal inseguro, controlado por Ivo. Beto possui um par de chaves, uma chave pública e outra privada. Ana conhece a chave pública de Beto, mas somente o dono do par de chaves (Beto) conhece a chave privada (não há segredo compartilhado).

A Figura Sistema criptográfico assimétrico para sigilo contém os passos a seguir:

- Ana configura o algoritmo de encriptação com a chave pública de Beto.
- Ana alimenta o algoritmo com a mensagem original (o texto claro).
- O texto claro é encriptado e transmitido pelo canal inseguro para Beto.
- Beto configura o algoritmo de decriptação com a sua própria chave privada.
- 5. O criptograma é decriptado e o texto claro original é obtido por Beto.

Analisando a figura anterior, como propõe Braga e Dahab (2015), observa-se que Ana envia uma mensagem privada para Beto. Para fazer isso, Ana encripta a mensagem usando a chave pública de Beto. Ana conhece a chave pública de Beto por que ela foi divulgada por Beto. Porém, o criptograma só pode ser decriptado pela chave privada de Beto; nem Ana pode fazê-lo.

Para obter comunicação segura bidirecional, basta acrescentar ao sistema criptográfico o mesmo processo no sentido oposto (de Beto para Ana), com outro par de chaves. Isto é, Beto usa a chave pública de Ana para enviar mensagens encriptadas para ela. Ana, ao receber a mensagem, usa sua própria chave privada pessoal para decriptar a mensagem enviada por Beto. A criptografia de chave pública é indispensável para a segurança da Internet, pois torna possível a comunicação privada em uma rede pública.

A criptografia de chave pública é a base para outros dois serviços: a autenticação das partes e a verificação de integridade das mensagens.

5.5.5 Autenticação e Irrefutabilidade

Conforme abordado por Braga e Dahab (2015), o uso da criptografia de chave pública para a autenticação de mensagens é quase o oposto do uso para sigilo. A criptografia de chave pública para assinatura digital é usada para obter integridade, autenticidade e irrefutabilidade. Chama-se assinatura digital ao resultado de uma certa operação criptográfica com a chave privada sobre o texto claro.

Neste caso, o dono da chave privada pode gerar mensagens assinadas, que podem ser verificadas por qualquer um que conheça a chave pública correspondente, portanto, sendo capaz de verificar a autenticidade da assinatura digital. Nem sempre a operação de assinatura é uma encriptação e a sua verificação é uma decriptação. Visto que qualquer um de posse da chave pública pode “decriptar” a assinatura digital, ela não é mais secreta, mas possui outra propriedade: a irrefutabilidade. Isto é, quem quer que verifique a assinatura com a chave pública, sabe que ela foi produzida por uma chave privada exclusiva; logo, a mensagem não pode ter sido gerada por mais ninguém além do proprietário da chave privada.

Na Figura Sistema criptográfico assimétrico para sigilo, Ana usa sua chave privada para assinar digitalmente uma mensagem para Beto. O texto claro e a assinatura digital são enviados por um canal inseguro e podem ser lidos por todos, por isso, a mensagem não é secreta. Qualquer um que conheça a chave pública de Ana (todo mundo, inclusive Beto) pode verificar a assinatura digital. Ivo pode ler a mensagem, mas não pode falsificá-la, pois não conhece a chave privada de Ana.

Segundo Braga e Dahab (2015), o principal problema administrativo deste modelo de autenticação é justamente a confiança depositada na chave pública. Se a chave pública de alguém pode ser encontrada em qualquer lugar, então, fica difícil saber se esta chave não foi corrompida ou substituída. O problema de garantir a autenticidade da chave pública é muito importante e, se não for solucionado satisfatoriamente, pode comprometer a confiança no sistema criptográfico. Uma maneira de validar chaves públicas é fazer com que elas sejam emitidas por Autoridades Certificadoras (AC) de uma Infraestrutura de Chaves Públicas (ICP), que torne possível a verificação da autenticidade de tais chaves.

5.6 Virtual Private Network (VPN)

De acordo com Chin (1998), a ideia de utilizar uma rede pública como a Internet em vez de linhas privativas para implementar redes corporativas é denominada de Virtual Private Network (VPN) ou Rede Privada Virtual. As VPNs são túneis de criptografia entre pontos autorizados, criados através da Internet ou outras redes públicas e/ou privadas para a transferência de informações, de modo seguro, entre redes corporativas ou usuários remotos.

A segurança é a primeira e mais importante função da VPN. Uma vez que dados privados serão transmitidos pela Internet, que é um meio de transmissão inseguro, eles devem ser protegidos para não permitir que sejam modificados ou interceptados.

Outro serviço oferecido pelas VPNs é a conexão entre corporações (Extranets) pela Internet. Além de possibilitar conexões dial-up criptografadas que podem ser muito úteis para usuários móveis ou remotos e filiais distantes de uma empresa.

Ainda conforme Chin (1998), uma das grandes vantagens decorrentes do uso das VPNs é a redução de custos com comunicações corporativas, pois eliminam a necessidade de links dedicados de longa distância que podem ser substituídos pela Internet. As LANs podem, por meio de links dedicados ou discados, conectar-se a algum provedor de acesso local e interligar-se a outras LANs, possibilitando o fluxo de dados através da Internet.

Esta solução pode ser bem interessante sob o ponto de vista econômico, sobretudo nos casos em que enlaces internacionais ou nacionais de longa distância estão envolvidos. Outro fator que simplifica a operacionalização da WAN é que a conexão LAN-Internet-LAN fica parcialmente a cargo dos provedores de acesso.

5.6.1 Aplicações para VPN

Abaixo, são apresentadas as três aplicações ditas mais importantes para as VPNs, conforme Chin (1998).

- **Acesso remoto via Internet:**

O acesso remoto a redes corporativas pela Internet pode ser viabilizado com a VPN por ligação local a algum provedor de acesso (Internet Service Provider – ISP). A estação remota disca para o provedor de acesso, conectando-se à Internet, e o software de VPN cria uma rede virtual privada entre o usuário remoto e o servidor de VPN corporativo pela Internet.

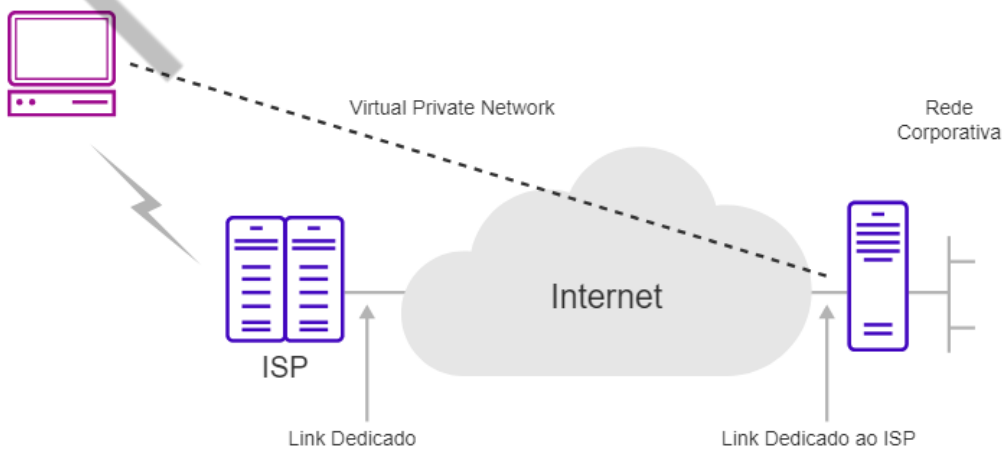

Figura 5.5 – Acesso Remoto via Internet
Fonte: Chin (1998)

- **Conexão de Lans Via Internet**

Uma solução que substitui as conexões entre LANs através de circuitos dedicados de longa distância é a utilização de circuitos dedicados locais, interligando-as à Internet. O software de VPN assegura esta interconexão, formando a WAN corporativa.

Dependendo das aplicações também, pode-se optar pela utilização de circuitos discados em uma das pontas, devendo a LAN corporativa estar, preferencialmente, conectada à Internet via circuito dedicado local, ficando disponível 24 horas por dia para eventuais tráfegos provenientes da VPN.

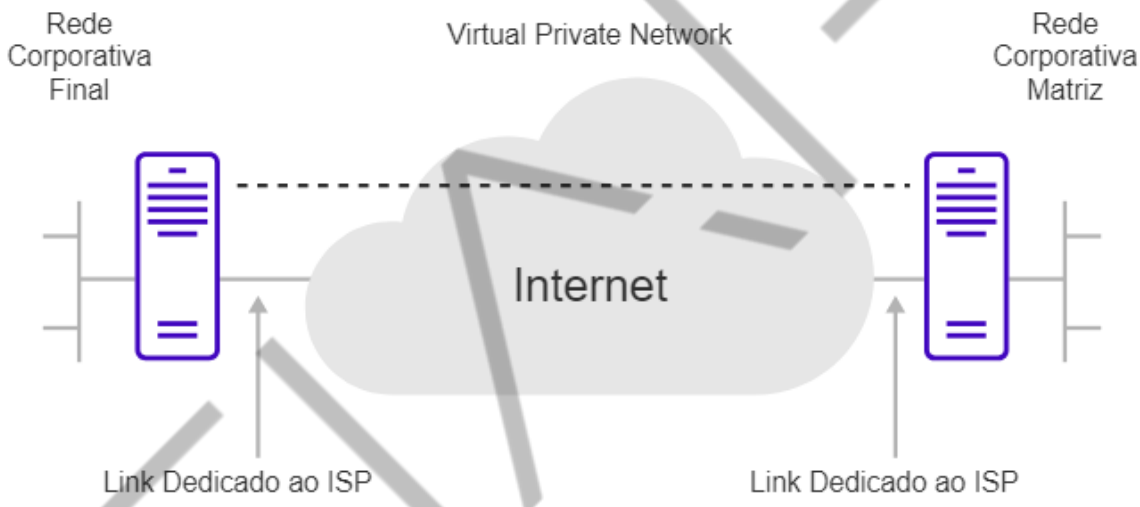

Figura 5.6 – Conexão de LANs via Internet
Fonte: Chin (1998)

- **Conexão de computadores numa Intranet**

Em algumas organizações, existem dados confidenciais cujo acesso é restrito a um pequeno grupo de usuários. Nestas situações, redes locais departamentais são implementadas fisicamente separadas da LAN corporativa. Esta solução, apesar de garantir a "confidencialidade" das informações, cria dificuldades de acesso a dados da rede corporativa por parte dos departamentos isolados.

As VPNs possibilitam a conexão física entre redes locais, restringindo acessos indesejados com a inserção de um servidor VPN entre elas. Observe que o servidor VPN não atuará como um roteador entre a rede departamental e o resto da

rede corporativa, visto que o roteador possibilitaria a conexão entre as duas redes, permitindo o acesso de qualquer usuário à rede departamental sensitiva.

Com o uso da VPN, o administrador da rede pode definir quais usuários estarão credenciados a atravessar o servidor VPN e acessar os recursos da rede departamental restrita. Adicionalmente, toda a comunicação ao longo da VPN pode ser criptografada, assegurando a "confidencialidade" das informações. Os demais usuários não credenciados nem sequer enxergam a rede departamental.

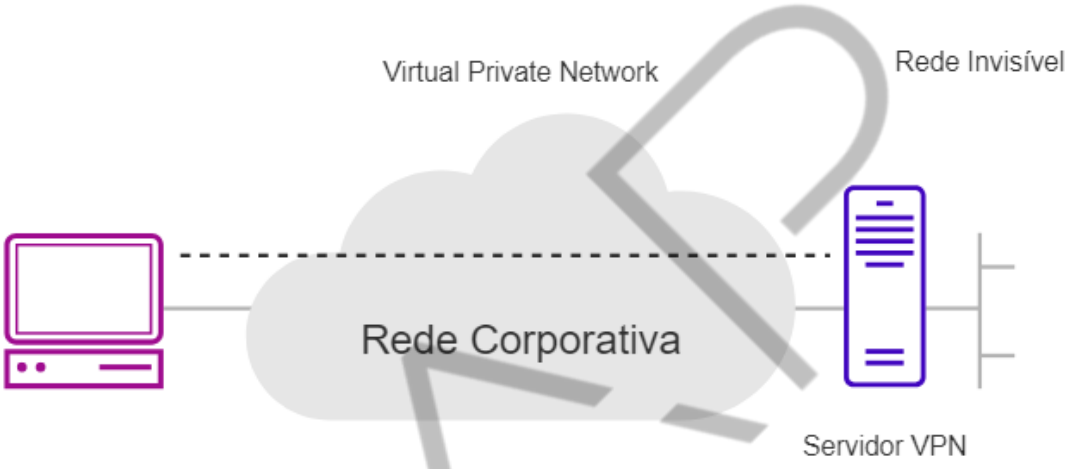

Figura 5.7 – Conexão de computadores numa Intranet
Fonte: Chin (1998)

5.6.2 Requisitos Básicos para uma VPN

Conforme Chin (1998), no desenvolvimento de soluções de rede, é muito desejável que sejam implementadas facilidades de controle de acesso a informações e a recursos corporativos. A VPN deve dispor de recursos para permitir o acesso de clientes remotos autorizados aos recursos da LAN corporativa, viabilizar a interconexão de LANs de forma que possibilite o acesso de filiais, compartilhando recursos e informações, e, finalmente, assegurar privacidade e integridade de dados ao atravessar a Internet e a própria rede corporativa.

A seguir, são enumeradas características mínimas desejáveis numa VPN:

- **Autenticação de usuários:**

Verificação da identidade do usuário, restringindo o acesso às pessoas autorizadas. Deve dispor de mecanismos de auditoria, provendo informações referentes aos acessos efetuados – quem acessou, o que e quando foi acessado.

- **Gerenciamento de endereço:**

O endereço do cliente na sua rede privada não deve ser divulgado, adotando-se endereços fictícios para o tráfego externo.

- **Criptografia de dados:**

Os dados devem trafegar na rede pública ou privada num formato cifrado e, caso sejam interceptados por usuários não autorizados, não deverão ser decodificados, garantindo a privacidade da informação. O reconhecimento do conteúdo das mensagens deve ser exclusivo dos usuários autorizados.

- **Gerenciamento de chaves:**

O uso de chaves que garantem a segurança das mensagens criptografadas deve funcionar como um segredo compartilhado exclusivamente entre as partes envolvidas. O gerenciamento de chaves deve garantir a troca periódica delas, visando manter a comunicação de forma segura.

- **Suporte a múltiplos protocolos:**

Com a diversidade de protocolos existentes, torna-se bem desejável que uma VPN suporte protocolos-padrão de fato usadas nas redes públicas.

5.6.3 Tunelamento

Como abordado por Chin (1998), as redes virtuais privadas baseiam-se na tecnologia de tunelamento cuja existência é anterior às VPNs. Ele pode ser definido como processo de encapsular um protocolo dentro de outro. O uso do tunelamento nas VPNs incorpora um novo componente a esta técnica: antes de encapsular o pacote que será transportado, este é criptografado para ficar ilegível caso seja interceptado durante o seu transporte. O pacote criptografado e encapsulado viaja através da Internet até alcançar seu destino, onde é desencapsulado e decriptografado, retornando ao seu formato original.

Uma característica importante é que pacotes de um determinado protocolo podem ser encapsulados em pacotes de protocolos diferentes. Por exemplo, pacotes de protocolo IPX podem ser encapsulados e transportados dentro de pacotes TCP/IP.

Chin (1998) explica que o protocolo de tunelamento encapsula o pacote com um cabeçalho adicional que contém informações de roteamento que permitem a travessia dos pacotes ao longo da rede intermediária. Os pacotes encapsulados são roteados entre as extremidades do túnel na rede intermediária. Túnel é a denominação do caminho lógico percorrido pelo pacote ao longo da rede intermediária. Após alcançar o seu destino na rede intermediária, o pacote é desencapsulado e encaminhado ao seu destino final. A rede intermediária por onde o pacote trafegará pode ser qualquer rede pública ou privada.

Note que o processo de tunelamento envolve encapsulamento, transmissão ao longo da rede intermediária e desencapsulamento do pacote.

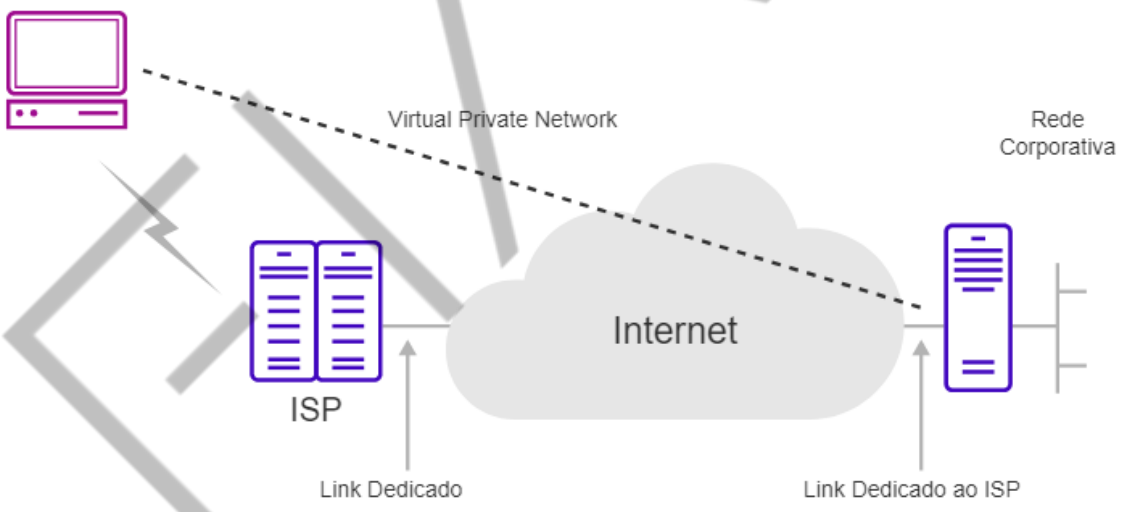

Figura 5.8 – Tunelamento
Fonte: Chin (1998)

Nas tecnologias orientadas à camada 2 (enlace), um túnel é similar a uma sessão em que as duas extremidades dele negociam a configuração dos parâmetros para o estabelecimento do túnel, tais como endereçamento, criptografia e parâmetros de compressão. Na maior parte das vezes, são utilizados protocolos que implementam o serviço de datagrama. A gerência do túnel é realizada por protocolos de manutenção. Nestes casos, é necessário que o túnel seja criado, mantido e encerrado. Nas tecnologias de camada 3, não existe a fase de manutenção do túnel.

Uma vez que o túnel é estabelecido, os dados podem ser enviados. O cliente ou servidor do túnel utiliza um protocolo de tunelamento de transferência de dados que acopla um cabeçalho, preparando o pacote para o transporte. Só, então, o cliente envia o pacote encapsulado na rede que o roteará até o servidor do túnel. Este recebe o pacote, desencapsula, removendo o cabeçalho adicional, e encaminha o pacote original à rede de destino. O funcionamento entre o servidor e o cliente do túnel é semelhante.

5.6.4 IPSEC

De acordo com Chin (1998), o IPSec é um protocolo-padrão de camada 3 projetado pelo IETF que oferece transferência segura de informações fim a fim através de rede IP pública ou privada. Essencialmente, ele pega pacotes IP privados, realiza funções de segurança de dados, como criptografia, autenticação e integridade, e, então, encapsula esses pacotes protegidos em outros pacotes IP para serem transmitidos. As funções de gerenciamento de chaves também fazem parte das funções do IPSec.

Tal como os protocolos de nível 2, o IPSec trabalha como uma solução para a interligação de redes e conexões via linha discada. Ele foi projetado para suportar múltiplos protocolos de criptografia, possibilitando que cada usuário escolha o nível de segurança desejado.

Segundo Chin (1998), os requisitos de segurança podem ser divididos em dois grupos, os quais são independentes entre si, sendo utilizados de forma conjunta ou separada, de acordo com a necessidade de cada usuário:

- Autenticação e Integridade.
- Confidencialidade.

Para implementar estas características, o IPSec é composto de três mecanismos adicionais, de acordo com Chin (1998):

- AH – Autentication Header.
- ESP – Encapsulation Security Payload.
- ISAKMP – Internet Security Association and Key Management Protocol.

Conforme Chin (1998), o ISAKMP combina conceitos de autenticação, gerenciamento de chaves e outros requisitos de segurança necessários às transações e comunicações governamentais, comerciais e privadas na Internet. Com o ISAKMP, as duas máquinas negociam os métodos de autenticação e segurança dos dados, executam a autenticação mútua e geram a chave para criptografar os dados.

Trata-se de um protocolo que rege a troca de chaves criptografadas utilizadas para decifrar os dados. Ele define procedimentos e formatos de pacotes para estabelecer, negociar, modificar e deletar as SAs (Security Associations).

As SAs contêm todas as informações necessárias para a execução de serviços variados de segurança na rede, tais como serviços da camada IP (autenticação de cabeçalho e encapsulamento), serviços das camadas de transporte e aplicação ou autoproteção durante a negociação do tráfego. Também define pacotes para geração de chaves e autenticação de dados. Esses formatos proveem consistência para a transferência de chaves e a autenticação de dados que independem da técnica usada na geração da chave, do algoritmo de criptografia e do mecanismo de autenticação.

Chin (1998) explica que o ISAKMP pretende dar suporte para protocolos de segurança em todas as camadas da pilha da rede. Com a centralização do gerenciamento dos SAs, o ISAKMP minimiza as redundâncias funcionais dentro de cada protocolo de segurança e também pode reduzir o tempo gasto durante as conexões através da negociação da pilha completa de serviços de uma só vez.

A autenticação garante que os dados recebidos correspondam àqueles originalmente enviados, assim como assegura a identidade do emissor. Integridade significa que os dados transmitidos chegam ao seu destino íntegros, eliminando a possibilidade de terem sido modificados no caminho sem que isso pudesse ser detectado.

Para Chin (1998), o AH é um mecanismo que provê integridade e autenticação dos datagramas IP. A segurança é garantida pela inclusão de informação para a autenticação no pacote, que é obtida através de algoritmo aplicado sobre o conteúdo dos campos do datagrama IP, excluindo-se aqueles que sofrem mudanças durante o transporte. Estes campos abrangem não só o

cabeçalho IP como todos os outros cabeçalhos e dados do usuário. No IPv6, o campo hop-count e o time-to-live (TTL) do IPv4 não são utilizados, pois são modificados ao longo da transferência.

Para alguns usuários, o uso da autenticação pode ser suficiente, não sendo necessária a "confidencialidade".

No IPV6, o AH, normalmente, é posicionado após os cabeçalhos de fragmentação e End-to-End, e antes do ESP e dos cabeçalhos da camada de transporte (TCP ou UDP, por exemplo).

De acordo com Chin (1998), a Confidencialidade é uma propriedade da comunicação que permite que apenas usuários autorizados entendam o conteúdo transportado. Desta forma, os usuários não autorizados, mesmo tendo capturado o pacote, não poderão ter acesso às informações nele contidas. O mecanismo mais usado para prover esta propriedade é chamado de criptografia.

Segundo Chin (1998), o serviço que garante a "confidencialidade" no IPSec é o ESP – Encapsulating Security Payload. O ESP também provê a autenticação da origem dos dados, integridade da conexão e serviço anti-reply. A "confidencialidade" independe dos demais serviços e pode ser implementada de dois modos – transporte e túnel. No primeiro modo, o pacote da camada de transporte é encapsulado dentro do ESP, e, no túnel, o datagrama IP é encapsulado inteiro dentro do cabeçalho do ESP.

5.7 Lab

Neste Lab, utilizaremos os conhecimentos de Criptografia para, em um ambiente Linux, criarmos um par de chaves pública e privada para criptografar e descriptografar um arquivo.

- **Preparação do ambiente**

Para a realização deste Lab, utilizaremos uma máquina virtual do Kali Linux, que pode ser baixada neste link https://www.offensive-security.com/kali-linux-vm-vmware-virtualbox-image-download/.

Após o download, utilize o seu ambiente de virtualização preferido (VirtualBox, VMWare etc.) para importar a referida máquina.

Todos os passos abaixo devem ser feitos através do Shell (Terminal).

- **Instalação do PGP em ambiente Linux**

A instalação do PGP no Linux é bem simples e pode ser feita pelo comando abaixo: **apt-get install gnupg**.

Após instalar o gnupg, execute o comando **gpg** para criar o diretório **~/.gnupg** que armazenará as chaves pública e privada.

- **Criação de chaves pública e privada:**

Para gerar um par de chaves pessoais, use o comando **gpg --gen-key**. Ele executará os seguintes passos:

- **Chave criptográfica:** selecione *DSA e ELGamal* a não ser que tenha necessidades específicas.
- **Tamanho da chave:** 1024 bits trazem uma boa combinação de proteção/velocidade.
- **Validade da chave:** 0 = a chave não expira. Um número positivo tem o valor de dias, que pode ser seguido das letras w (semanas), m (meses) ou y (anos). Por exemplo, "7m", "2y", "60". Após a validade, a chave será considerada inválida.
- **Nome de usuário:** nome para identificar a chave.
- **E-mail:** do dono da chave.
- **Comentário:** uma descrição sobre a chave do usuário.
- **Confirmação:** tecle "O" para confirmar os dados ou uma das outras letras para modificar os dados de sua chave.
- **Digite a FraseSenha:** senha que o(a) identificará como proprietário(a) da chave privada. É chamada de FraseSenha, pois pode conter espaços e não há limite de caracteres. Para alterá-la posteriormente, siga as

instruções em [#s-d-cripto-gpg-chpasswd, mudando sua FraseSenha, Seção 20.5.11].

- Confirme e aguarde a geração da chave pública/privada.

- **Encriptando um arquivo:**

Use o comando **gpg -e** arquivo faz a encriptação de dados: gpg -e arquivo.txt

Será pedida a identificação de usuário, digite o nome que usou para criar a chave. O arquivo criado será encriptado usando a chave pública do usuário (**~/.gnupg/pubring.gpg**) e terá a extensão **.gpg** adicionada (**arquivo.txt.gpg**). Além de criptografado, este arquivo é compactado (recomendável para grande quantidade de textos). A opção ***-a*** é usada para criar um arquivo criptografado com saída ASCII 7 bits: gpg -e -a arquivo.txt

O arquivo gerado terá a extensão .asc acrescentada (**arquivo.txt.asc**) e não será compactado. A opção ***-a*** é muito usada para o envio de e-mails. Para criptografar o arquivo a ser enviado a outro usuário, você deverá ter a chave pública do usuário cadastrado no seu chaveiro e especificar a opção ***-r*** seguida do **nome/e-mail/ID** da chave pública: **gpg -r kov -e arquivo.txt**

O exemplo acima utiliza a chave pública de kov para encriptar o arquivo **arquivo.txt** (somente ele poderá decriptar a mensagem, usando sua chave privada).

É recomendável especificar o nome de arquivo sempre como último argumento.

- **Decriptando um arquivo**

Agora, vamos fazer a operação reversa da acima, a opção **-d** é usada para decriptar os dados, usando a chave privada:

```
gpg -d --decrypt arquivo.txt.asc > arquivo.txt

gpg -d --decrypt arquivo.txt.gpg > arquivo.txt
```

Decriptografa os arquivos arquivo.txt.asc e arquivo.txt.gpg recuperando seu conteúdo original. A sua "FraseSenha" será pedida para descriptografar os dados, usando a chave privada (**~/.gnupg/secring.gpg**).

- **Assinando arquivos**

Assinar um arquivo é garantir que você é a pessoa que realmente enviou aquele arquivo. Use a opção **-s** para assinar arquivos, usando sua chave privada: gpg -s arquivo.txt

A "FraseSenha" será pedida para assinar os dados, usando sua chave privada. Será gerado um arquivo arquivo.txt.gpg (assinado e compactado). Adicionalmente, a opção **--clearsign** poderá ser usada para fazer uma assinatura em um texto plano, este é um recurso muito utilizado por programas de e-mails com suporte ao gpg: gpg -s --clearsign arquivo.txt

Será criado um arquivo chamado arquivo.txt.asc, contendo o arquivo assinado e sem compactação.

- Checando assinaturas

A checagem de assinatura consiste em verificar que quem nos enviou o arquivo é realmente quem diz ser e se os dados foram, de alguma forma, alterados. Você deverá ter a chave pública do usuário no seu chaveiro para fazer esta checagem. Para verificar os dados assinados acima, usamos a opção **--verify**: gpg --verify arquivo.txt.asc

Se a saída for "Assinatura Correta", significa que a origem do arquivo é segura e que ele não foi, de qualquer forma, modificado. gpg --verify arquivo.txt.gpg

Se a saída for "Assinatura INCORRETA", significa que ou o usuário que enviou o arquivo não confere ou o arquivo enviado foi, de alguma forma, modificado.

REFERÊNCIAS

BRAGA, Alexandre; DAHAB, Ricardo. **Introdução à criptografia para programadores**: evitando maus usos da criptografia em sistemas de software. 2015. Disponível em: <https://siaiap34.univali.br/sbseg2015/anais/Minicursos/MC1.pdf>. Acesso em: 16 jun. 2020.

CHIN, Liou Kuo. **Rede Privada Virtual - VPN**. 1998. Disponível em: <http://memoria.rnp.br/newsgen/9811/vpn.html>. Acesso em: 16 jun. 2020.