

Engenharia de Controle e Automação – 9º Período
Disciplina: Aspectos de Segurança em Automação
Professor: José Maurício S. Pinheiro

AULA 5: Criptografia e Certificação Digital

1. Criptografia

A forma mais utilizada para prover a segurança em pontos vulneráveis de uma rede de computadores é a utilização da criptografia. A criptografia é utilizada para barrar as ameaças e os ataques. A palavra tem origem grega (kriptos = escondido, oculto e grifo = grafia) e define a arte ou ciência de escrever em cifras ou em códigos (Figura 1), utilizando um conjunto de técnicas que torna a mensagem incompreensível e chamada comumente de “texto cifrado”, através de um processo chamado cifragem, permitindo que apenas o destinatário desejado consiga decodificar e ler a mensagem com clareza. As mensagens legíveis são chamadas de texto plano ou texto limpo e as ilegíveis, são chamadas de texto cifrado.

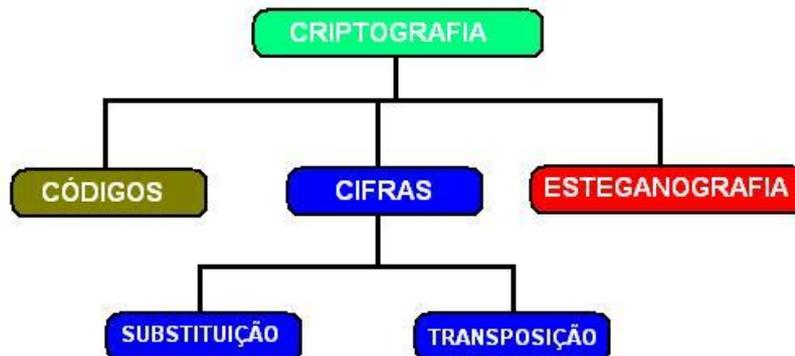


Figura 1 - Criptografia

A RFC 2828 (*Request for Comments* nº 2828) define criptografia como a ciência matemática que lida com a transformação de dados para mudar seu significado em algo ininteligível para o inimigo, isto é, esconder seu conteúdo semântico prevenindo sua alteração ou o seu uso sem autorização.

A criptografia é o meio primário para oferecer confidencialidade às informações transmitidas entre as redes locais de computadores ou através da Internet. Pode ser usada para qualquer tipo de dado transmitido, desde um e-mail até um arquivo com dados confidenciais. Também pode ser usada para proteger dados armazenados onde a segurança física é de difícil implementação ou impossível. Pode-se citar o exemplo dos laptops, que, ao serem deixados em um quarto de hotel, poderiam ter as tuas informações lidas por pessoas não autorizadas.

O processo criptográfico consiste em transformar um texto simples, através de uma função parametrizada por uma chave (senha), em um texto inteligível. A saída desse processo de criptografia é chamada texto cifrado ou criptograma. Após o processo de criptografia, o texto é então transmitido ao destinatário. Este conhece o método utilizado para a criptografia e também conhece a

chave, possibilitando a transformação do texto criptografado em texto simples novamente. Se a mensagem for interceptada por alguém, será necessário descobrir a chave de criptografia bem como o seu método, para que se possa utilizar a mensagem capturada.

1.1. Métodos criptográficos

Os métodos de criptografia podem ser divididos em duas categorias:

- **Cifra de substituição** - cada letra ou grupo de letras é substituído por outra letra ou grupo de letras, a fim de ocultá-la. Por exemplo, pode-se definir que para um texto ser cifrado, as letras de cada palavra do texto devem ser deslocadas em k letras. Nesse caso, k torna-se uma chave para o método de criptografia.
- **Cifra de transposição** - as letras são reordenadas, mas não ocultadas. A cifra é chaveada por uma palavra ou frase que não contém quaisquer letras repetidas.

Deve-se observar que número de bits que compõe uma chave criptográfica é uma variável fundamental no sistema de segurança. Seu tamanho indica o nível de esforço necessário para que um atacante consiga determinar a chave e conseqüentemente ter acesso aos dados protegidos. Uma encriptação é dita computacionalmente segura se atende estes dois critérios:

- O custo para quebrar o cifrador excede ao valor da informação encriptada;
- O tempo requerido para quebrar o cifrador excede o tempo de vida útil da informação.

Na Tabela 1 está um resumo do tempo médio de busca de acordo com o tamanho da chave de criptografia. Na primeira coluna temos o tamanho das chaves, na segunda coluna o número possível de combinações. Na terceira coluna está o tempo estimado para descriptografia da chave considerando-se o tempo base de $1\mu s$. Na quarta e última coluna, é mostrado o tempo necessário para que um sistema que fosse capaz de processar 1 milhão de chaves por microssegundo pudesse quebrar o cifrador.

Tabela 1- Tempo médio de busca de acordo com o número de bits da chave

Tamanho da Chave	Número de Chaves	Tempo requerido (1 cripto/ μs)	Tempo requerido (10^6 cripto/ μs)
32	$2^{32} = 4,3 \times 10^9$	35,8 minutos	2,15 ms
56	$2^{56} = 7,2 \times 10^{16}$	1.142 anos	10,01 horas
128	$2^{128} = 3,4 \times 10^{38}$	$5,4 \times 10^{24}$ anos	$5,4 \times 10^{18}$ anos
26 caracteres (permutação)	$26! = 4 \times 10^{26}$	$6,4 \times 10^{12}$ anos	$6,4 \times 10^6$ anos

1.2. Técnicas Básicas de Criptografia

Existem várias técnicas disponíveis para o uso da criptografia. Os dois modelos clássicos são a transposição e substituição.

A substituição pode ser monoalfabética ou polialfabética:

- **Substituição simples ou monoalfabética** - técnica mais básica, onde a chave se constitui de um alfabeto permutado, por exemplo, DEFGHIJKLMNOPQRSTUVWXYZABC. Usando-se esse alfabeto chave, o A é substituído por D, o B por E, o C por F, e assim por diante;
- **Substituição polialfabética** - diversos, e não somente um alfabeto-chave, são empregados, periodicamente, para decifrar mensagens.

Por exemplo, a palavra RAINHA ficaria criptografada como UDLQKD. Esse exemplo, onde cada letra da mensagem é substituída por outra letra defasada de três posições no alfabeto, configura a “Cifra de Cezar”, empregada por Júlio Cezar, na campanha da Gália em 55 a.C. Considerando o alfabeto com 26 letras, temos chaves possíveis da ordem de 25! (fatorial de 25), isto é, aproximadamente, 1.5×10^{25} situações possíveis.

A transposição pode ser simples ou dupla:

- **Transposição simples** - a mensagem é escrita sob uma palavra-chave e o criptograma é obtido retirando-se as letras, coluna por coluna, na sequência numérica das letras da palavra-chave, em grupos de cinco;
- **Transposição dupla** - consiste em aplicar, ao criptograma da transposição simples, uma segunda transposição, porém, com uma chave diferente.

Por exemplo, a palavra MICROPROCESSOR, pode ser criptografada como MCORCSOIRPOESR utilizando-se a transposição simples.

1.3. Tipos de Criptografia

A criptografia é um mecanismo de segurança que permite a implementação de diversos serviços (autenticação, não-repúdio, integridade, confidencialidade) e utiliza conceitos matemáticos para a construção de seus algoritmos. Para tanto existem dois tipos básicos de criptografia: simétrica e assimétrica.

Na criptografia simétrica os usuários envolvidos devem ter prévio conhecimento da chave (senha). Isto a torna muito vulnerável a falhas de segurança. Na criptografia assimétrica existem duas chaves relacionadas entre si. Qualquer texto encriptado com uma delas somente poderá ser decifrado com a outra.

1.3.1. Sistema de chave simétrica

A criptografia por chave simétrica (ou chave privada) é utilizada para prover a segurança das informações (Figura 2). Nesta técnica uma mesma chave

(senha) é utilizada para criptografar e decriptografar uma mensagem que, portanto, deve ser de conhecimento tanto do emissor como do receptor da mensagem. Em cifradores simétricos, o algoritmo de criptografia e descryptografia são os mesmos, mudando apenas a forma como são utilizadas as chaves. Um exemplo de algoritmo simétrico é o DES (Data Encryption Standard), cuja chave possui tamanho de 56 bits. Entretanto algoritmos com chaves maiores estão disponíveis resultando em maior segurança.

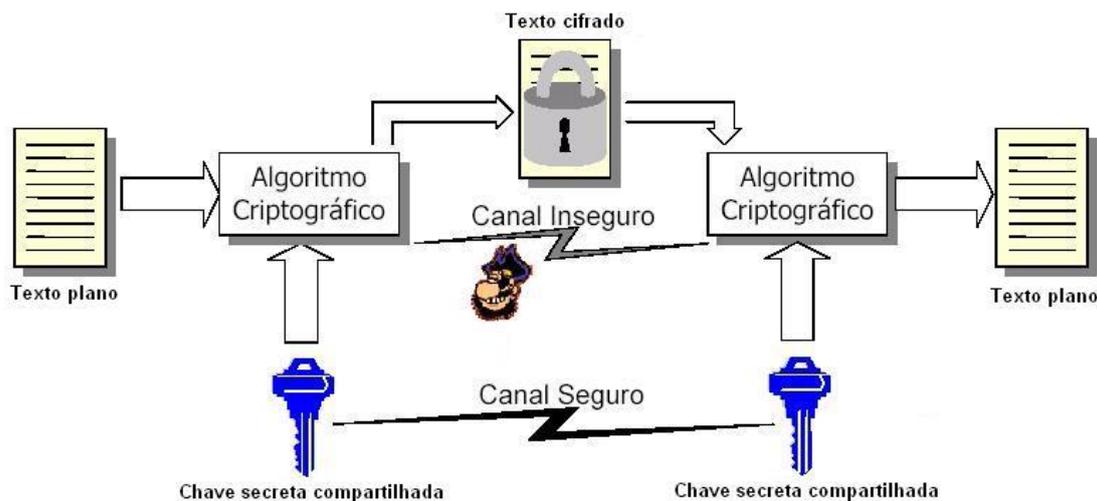


Figura 2 - Exemplo de chave simétrica

Uma mensagem para ser enviada é encriptada pelo emissor, com uma chave secreta compartilhada que é de seu conhecimento. Para o receptor decifrar a mensagem, deve ter a mesma chave secreta utilizada pelo transmissor. A chave secreta compartilhada é enviada por um canal seguro para o receptor. Com este modelo pode-se garantir a confidencialidade da mensagem, porque somente o transmissor e o receptor têm conhecimento da chave secreta. O texto cifrado não sofre alteração quanto ao seu tamanho. É importante salientar também que o texto cifrado não contém qualquer parte da chave.

1.3.2. Sistema de chave assimétrica

A criptografia por chave assimétrica (ou chave pública) utiliza um par de chaves, sendo uma chave para cifrar a informação e uma outra chave diferente para decifrar a informação. O que for encriptado utilizando uma chave somente poderá ser visualizado com a outra. A chave pública, como o próprio nome diz, é de conhecimento público e é divulgada em diversas maneiras. Com a chave pública é possível prover os serviços de confidencialidade, autenticação e distribuição de chaves. A garantia da confidencialidade é que somente as pessoas ou organizações envolvidas na comunicação possam ler e utilizar as informações transmitidas de forma eletrônica pela rede. Já a autenticação é a garantia de identificação das pessoas ou organizações envolvidas na comunicação. Esse sistema tem como principal padrão o RSA (Ron Rivest, Adi Shamir e Leonard Adleman). As chaves são criadas através de operações matemáticas de tal forma que, apesar de serem relacionadas, é virtualmente impossível adivinhar a outra, tendo apenas uma delas.

Em um sistema de chave assimétrica (Figura 3) cada pessoa tem duas chaves: uma chave pública que pode ser divulgada e outra privada que deve ser mantida em segredo. Mensagens cifradas com a chave pública só podem ser decifradas com a chave secreta e vice-versa. Se duas pessoas quiserem se comunicar secretamente usando a criptografia com chave assimétrica, elas terão de fazer o seguinte:

- O emissor escreve uma mensagem e a criptografa utilizando a chave pública do receptor. Essa chave está disponível para qualquer pessoa;
- O emissor envia a mensagem através de um meio qualquer, por exemplo, a Internet, para o receptor;
- O receptor recebe a mensagem e a descriptografa utilizando a chave privada que só ele conhece;
- O receptor lê a mensagem e se quiser responder ao emissor deverá fazer o mesmo procedimento anterior com a diferença de que dessa vez a chave pública do emissor é que será utilizada.

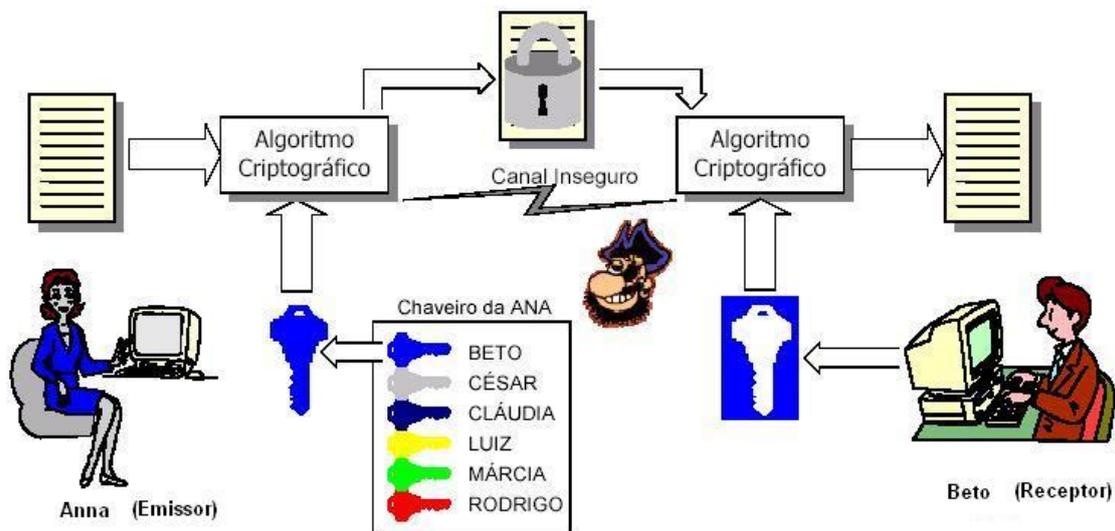


Figura 3 - Exemplo de chave assimétrica

Como apenas o receptor da mensagem tem acesso a sua chave privada, somente ele pode decifrar a mensagem. A grande vantagem é que não só o emissor pode enviar mensagens criptografadas para o receptor, mas qualquer pessoa, bastando conhecer a chave pública do receptor, além disso, emissor e receptor não precisam combinar chaves antecipadamente.

Pode-se também criar uma assinatura digital com chaves assimétricas. Para isso basta inverter o processo: o emissor criptografa a mensagem com sua própria chave privada e envia ao receptor. Para descriptografar deve-se usar a chave pública de emissor. Agora qualquer pessoa pode ler a mensagem, mas tem-se a certeza de foi o emissor que a enviou (acreditando-se que somente ele conhece sua chave privada).

Embora a criptografia simétrica seja menos segura, ela é mais rápida, sendo atualmente utilizada em conjunto com a criptografia assimétrica para aumentar a eficiência da troca de mensagens seguras. As chaves são criadas através de

operações matemáticas de tal forma que, apesar de serem relacionadas, é virtualmente impossível descobrir a outra, tendo apenas uma delas.

1.4. Objetivos da Criptografia

A criptografia computacional protege o sistema quanto à ameaça de perda de confiabilidade, integridade ou não repúdio, é utilizada para garantir:

- **Sigilo:** somente os usuários autorizados têm acesso à informação;
- **Integridade:** garantia oferecida ao usuário de que a informação correta, original, não foi alterada, nem intencionalmente, nem acidentalmente.
- **Autenticação do usuário:** é o processo que permite ao sistema verificar se a pessoa com quem se está comunicando é de fato a pessoa que alega ser.
- **Autenticação de remetente:** é o processo que permite a um usuário certificar-se que a mensagem recebida foi de fato enviada pelo remetente, podendo-se inclusive provar perante um juiz, que o remetente enviou aquela mensagem.
- **Autenticação do destinatário:** consiste em se ter uma prova de que a mensagem enviada foi como tal recebida pelo destinatário.
- **Autenticação de atualidade:** consiste em provar que a mensagem é atual, não se tratando de mensagens antigas reenviadas.

Entretanto, a criptografia não soluciona todos os problemas de segurança:

- A criptografia não impede um atacante de apagar todos os seus dados.
- Um atacante pode comprometer o programa de criptografia modificando o programa para usar uma chave diferente ou gravar as chaves em arquivo para análise posterior.
- Um atacante pode encontrar uma forma de decifrar a mensagem dependendo do algoritmo utilizado.
- Um atacante pode acessar os arquivos antes de serem criptografados ou após a decifração.

A criptografia deve ser parte da estratégia de segurança, mas não deve ser a substituta de outras técnicas de segurança. Na Tabela 2 são apresentadas as características principais entre chaves pública e privada.

Tabela 2 - Comparações entre chave privada e chave pública

CHAVE PRIVADA	CHAVE PÚBLICA
Um algoritmo e uma chave	Um algoritmo e duas chaves
Os usuários compartilham o algoritmo e a chave	Os usuários compartilham um par de chaves
Chave secreta	Apenas uma das chaves é secreta
Impossibilidade de decifrar a mensagem	Impossibilidade de decifrar a mensagem
O algoritmo e as amostras do texto cifrado não devem ser suficientes para determinar a chave	O algoritmo, as amostras do texto cifrado e uma das chaves não devem ser suficientes para determinar a outra chave.

2. Resumo Criptográfico (hash)

A tradução literal de hash é "picar, misturar, confundir". Funções criptográficas de resumo são usadas em vários contextos, por exemplo, para computar um resumo de mensagem ao criar uma assinatura digital. A Função Resumo (hash) é uma transformação matemática que faz o mapeamento de uma sequência de bits de tamanho arbitrário para uma sequência de bits de tamanho fixo menor – conhecido como resultado hash ou resumo criptográfico - de forma que seja muito difícil encontrar duas mensagens produzindo o mesmo resultado hash (resistência à colisão) e que o processo reverso também não seja realizável (dado um resultado hash, não é possível recuperar a mensagem que o gerou). Entre outras aplicações, as funções de resumo são usadas em criptografia para:

- Garantia de integridade dos dados.
- Garantia de origem de uma mensagem.
- Cálculo de respostas que são função de uma chave secreta e de uma mensagem de desafio (em protocolos de identificação através de desafio).
- Confirmação de chave.
- Confirmação de conhecimento (habilidade de comprovar conhecimento prévio de algo sem a necessidade de expor os dados previamente).
- Derivação de chave.
- Geração de números pseudoaleatórios.

Em um primeiro momento é gerado um resumo criptográfico da mensagem através de algoritmos complexos (MD5, SHA-1, SHA-256, por exemplo) que reduzem qualquer mensagem sempre a um resumo de mesmo tamanho. A este resumo criptográfico se dá o nome de hash. O resumo criptográfico, em conjunto com a criptografia assimétrica, é utilizado para garantir a integridade de um documento digital. Após gerar o hash, ele deve ser criptografado através de um sistema de chave pública, para garantir a autenticação e a irretratabilidade. O autor da mensagem deve usar sua chave privada para assinar a mensagem e armazenar o hash criptografado junto a mensagem original.

Para verificar a autenticidade do documento, deve ser gerado um novo resumo a partir da mensagem que está armazenada, e este novo resumo deve ser comparado com a assinatura digital. Para isso, é necessário descriptografar a assinatura obtendo o hash original. Se ele for igual ao hash recém gerado, a mensagem está íntegra. Além da assinatura existe o selo cronológico que atesta a referência de tempo à assinatura. A ideia básica desta função é que um valor resumo serve como uma imagem representativa compacta (às vezes chamada de impressão digital ou MD - *Message Digest*) da cadeia de bits da entrada, e pode ser usada como se fosse unicamente identificável com aquela entrada. As funções de resumo criptográfico funcionam semelhantes ao dígito verificador do CPF. Por exemplo, se um número qualquer do CPF for modificado, o dígito verificador também sofrerá alteração.

As funções de resumo criptográfico são usadas para garantir a integridade de dados. Algumas das propriedades desta função são:

- Deve ser computacionalmente inviável fazer a operação inversa, ou seja, dado um resumo, deve ser inviável obter uma mensagem original;
- Duas mensagens semelhantes devem produzir um resumo completamente diferente;
- Deve ser fácil e rápido produzir o resumo.

Considerando que as mensagens possíveis são infinitas, mas o tamanho do hash é fixo, é impossível impedir que mensagens diferentes levem a um mesmo hash. Quando isto ocorre é dito que foi encontrada uma colisão de hashes e o algoritmo deve ser abandonado. As funções de hash estão em constante evolução para evitar que colisões ocorram.

A função resumo pode ser utilizada para garantir a integridade de uma mensagem. Isso pode ser feito enviando-se para Beto a mensagem e o resumo da mensagem cifrada com a chave privada de Alice. Beto decifra o resumo com a chave pública de Alice, calcula um novo resumo com base na mensagem recebida e compara os dois valores. Se forem iguais, a mensagem não foi alterada, garantindo-se dessa forma a sua integridade (Figura 4).

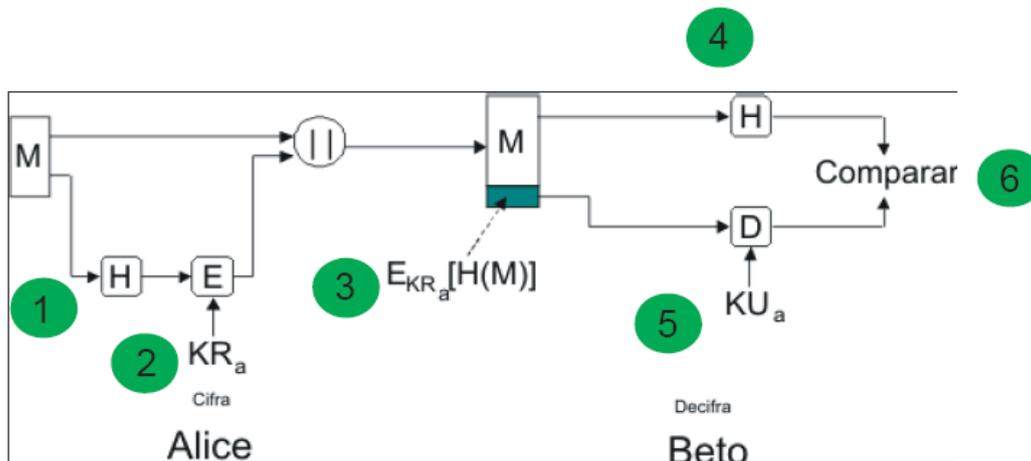


Figura 4 - Exemplo de utilização de função de resumo criptográfico

Na figura, “M” representa a mensagem. (1) obtém-se o resumo da mensagem M. (2) cifra o resumo com a chave privada (KR_a) de Alice. (3) Mensagem original + resumo cifrado. (4) Beto obtém o hash do documento. (5) Beto decifra o hash com a chave pública de Alice. (6) Beto compara os resultados obtidos no processo 4 e 5. Se forem iguais, a mensagem está correta.

2.1. O algoritmo Hash

O algoritmo hash é composto por fórmulas matemáticas complexas, para poder garantir a irreversibilidade e a unicidade do MD gerado - textos diferentes não produzem o mesmo MD. A alteração de um simples bit na mensagem gera um MD completamente diferente e o valor de conferência (*check-sum*) muda se um

único bit for alterado, acrescentado ou retirado da mensagem. O tamanho do MD depende do algoritmo escolhido (MD1, MD2, MD5 ou SHA1, por exemplo), que é medido em bits - por exemplo, o SHA1 é o mais recente dentre estes anteriores e gera um hash de 160 bits.

A capacidade de descobrir uma mensagem que dê um hash a um dado valor possibilita a um agressor substituir uma mensagem falsa por uma mensagem real que foi assinada. Permite ainda que alguém repudie uma mensagem, alegando que assinou uma mensagem diferente, dando um hash ao mesmo valor e violando assim a propriedade de não-repúdio das assinaturas digitais. Várias funções hash têm sido desenvolvidas com objetivo de melhorar a versão anterior a fim de obter maior segurança e evitar que os ataques sejam bem-sucedidos. As mais conhecidas são:

- **MD4** - Produz um valor hash de 128 bits. Efetua uma manipulação de bits para obter o valor do hash, de forma rápida. É um padrão da Internet (RFC-1320). Porém, vários ataques foram detectados, o que fez com que o algoritmo fosse considerado frágil.
- **MD5** - Extensão do MD4. Produz como saída um valor hash de tamanho de 128 bits. A obtenção do valor de hash é mais lenta, mas é mais segura. Está definido como um padrão da internet. (RFC-1321). É usado pelo PGP (Pretty Good Privacy).
- **SHA-1** (Secure Hash Algorithm) - Desenvolvido pelo NIST (National Institute of Standards and Technology), produz um valor hash de 160 bits. É considerado mais seguro que o MD4 e MD5 pelo seu tamanho.
- **RIPEMD-160**. É uma função hash criptográfica desenhada em um projeto chamado RIPE (Race Integrity Primitives Evaluation) e produz uma saída de 160 bits.

3. Assinatura Digital

A assinatura digital é a versão digital da assinatura de punho em documentos físicos. A assinatura digital apresenta um grau de segurança muito superior ao de uma assinatura de punho. O destinatário de uma mensagem assinada digitalmente pode verificar se a mensagem foi realmente emitida pela pessoa cuja assinatura nela consta, ou se a mensagem não foi em algum ponto adulterada intencional ou acidentalmente depois de assinada. Mais ainda, uma assinatura digital que tenha sido verificada não pode ser negada. Aquele que assinou digitalmente a mensagem não pode dizer mais tarde que sua assinatura digital foi falsificada. Em outras palavras, assinaturas digitais habilitam "autenticação" de documentos digitais, garantindo ao destinatário de uma mensagem digital tanto a identidade do remetente quanto a integridade da mensagem.

A assinatura digital é um conjunto de procedimentos matemáticos realizados com a utilização de técnicas de criptografia assimétrica que permite, de forma única e exclusiva, a comprovação da autoria de um determinado conjunto de dados. Por exemplo, para personalizar uma mensagem, um determinado usuário A codifica uma mensagem utilizando sua chave secreta e a envia para o destinatário B. Somente a chave pública de A permitirá a decodificação dessa mensagem. Portanto é a prova de que A enviou a mensagem para B. A

mensagem assim pode ser decodificada por qualquer um que tenha a chave pública de A. Uma assinatura é considerada autêntica quando um usuário usa a chave pública de A para decifrar uma mensagem. Nesse momento ele confirma que foi A e somente A quem enviou a mensagem. A assinatura não pode ser forjada porque somente A conhece sua chave secreta e um documento, uma vez assinado, não pode ser alterado. Se ocorrer qualquer alteração no texto criptografado, este não poderá ser restaurado com o uso da chave pública de A.

A assinatura digital não é reutilizável, ou seja, a assinatura é uma função do documento e não pode ser transferida para outro documento. Da mesma forma a assinatura não pode ser repudiada. O usuário B não precisa de nenhuma ajuda de A para reconhecer sua assinatura e A não pode negar ter assinado o documento. A assinatura digital pode ser implementada basicamente de três formas: função hash por meio dos padrões MD5 e SHA (Secure Hash Algorithm), DSS - Digital Signature Standard e utilizando o conceito de chaves públicas com o padrão RSA.

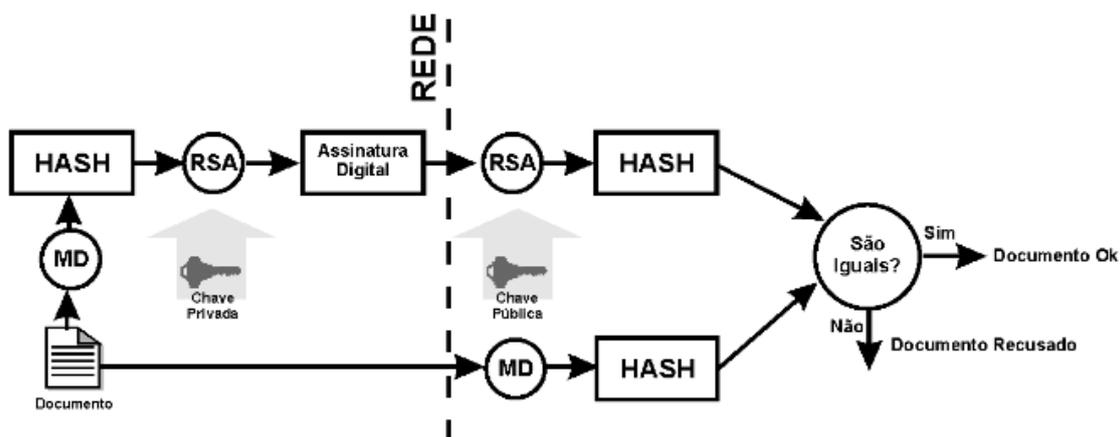


Figura 5 - Geração e verificação de assinatura digital

3.1.1. Propriedades da Assinatura Digital

A assinatura digital, analogamente à assinatura escrita, deve possuir as seguintes propriedades:

- Ser capaz de verificar o autor e a data/hora da assinatura;
- Autenticar o conteúdo original;
- A assinatura deve ser verificável por terceiros (resolver disputas).

Com base nas propriedades citadas, a assinatura digital deve satisfazer os seguintes requerimentos:

- Dependem do Conteúdo;
- Usar informação única do originador;
- Fácil de produzir;
- Fácil de reconhecer e verificar;

- Inviável de forjar;
- Prática para manter uma cópia da assinatura.

3.1.2. Tipos de Assinatura Digital

A assinatura digital pode ser dividida em dois tipos básicos: direta e arbitrada. A assinatura digital direta envolve somente as partes comunicantes (origem “X” e destino “Y”). Assume-se que o destino conheça a chave pública da origem. A assinatura digital pode ser formada encriptando toda a mensagem com a chave privada de “X” ou encriptando apenas o código hash. Neste tipo de assinatura, “X” pode negar a assinatura em algum documento alegando que sua chave foi roubada. Para isto, existe também um selo de tempo que será anexada a mensagem com data e hora da assinatura. Os problemas associados com a assinatura digital direta podem ser resolvidos se usar um árbitro. A assinatura digital arbitrada prevê a presença de um arbitro “A”. A mensagem que será enviada de “X” para “Y” passa primeiramente por “A” para ser verificada e datada.

3.2. Certificado Digital

O Certificado Digital é um documento que contém dados de identificação da pessoa ou instituição que deseja comprovar, perante terceiros, a sua própria identidade. Serve, igualmente, para conferir a identidade de terceiros. Pode ser comparado como uma espécie de carteira de identidade eletrônica. Graças aos certificados digitais, uma transação eletrônica realizada via Internet torna-se perfeitamente segura, pois permite que as partes envolvidas apresentem cada uma, as suas credenciais para comprovar, à outra parte, a sua real identidade. Tecnicamente, os Certificados Digitais vinculam um par de chaves eletrônicas que pode ser usado para criptografar e assinar informações digitais. Possibilita verificar se um usuário tem, realmente, o direito de usar uma determinada chave, ajudando a impedir que as pessoas usem chaves falsificadas para personificar outros usuários. Usados em conjunto com a criptografia, os Certificados Digitais fornecem uma solução de segurança completa, assegurando a identidade de uma ou de todas as partes envolvidas em uma transação.

O Certificado Digital é emitido por uma terceira parte de confiança denominada Autoridade Certificadora (CA - *Certificate Authority*) e pode ser uma empresa, organização ou indivíduo, público ou privado, que atua como tabelião para verificar e autenticar a identidade de usuários de um sistema criptográfico de chave pública. As CA's devem tomar providências para estabelecer a identidade das pessoas ou organizações para as quais emitem Certificados Digitais. Depois de estabelecerem a identidade de uma organização, elas emitem um certificado que contém a chave pública da organização, e que é assinado com a chave privada da CA.

Os certificados digitais possuem uma forma de assinatura eletrônica de uma instituição reconhecida por todos como confiável, e que, graças à sua idoneidade, faz o papel de "Cartório Eletrônico". Os métodos criptográficos empregados impedem que a assinatura eletrônica seja falsificada, ou que os dados do documento sejam adulterados ou copiados, tornando-o

absolutamente inviolável. Garante-se, assim, por quem assina que os dados de identificação do certificado são verdadeiros. A Certificação Digital garante os três princípios básicos da comunicação segura em um ambiente em rede:

- Autenticidade;
- Privacidade;
- Inviolabilidade.

Assim, uma vez instalada no computador, a Certificação Digital o reconhecerá como habilitado. Da mesma forma, o equipamento estará apto a reconhecer um Site certificado como verdadeiro. Em outras palavras, o documento eletrônico gerado por quem possui um Certificado Digital não pode ser posteriormente refutado, sendo estabelecido um vínculo tão forte quanto o que é gerado por uma assinatura de punho em um documento em papel. O certificado digital é uma estrutura de dados, dentro da qual estão as seguintes informações:

- Chave pública e nome do usuário;
- Número de série do certificado;
- Nome da certificadora que o emitiu;
- Assinatura digital da CA, assinada com sua respectiva chave secreta.

4. Esteganografia

A palavra esteganografia vem do grego e significa "escrita coberta". Trata-se de um ramo particular da criptografia que consiste, não em fazer com que uma mensagem seja ininteligível, mas em camuflá-la, mascarando a sua presença (Figura 6). Por exemplo, uma sequência de letras de cada palavra pode formar a palavra de uma mensagem escondida. Algumas formas de esteganografia são:

- **Marcação de caracteres:** utilização de uma tinta com composto especial que, ao ser exposta à luz, faz com que os caracteres fiquem de forma diferente, compondo a mensagem secreta;
- **Tinta invisível:** pode-se utilizar uma tinta invisível para a escrita da mensagem em cima de outra pré-existente, aonde, somente com produtos químicos poderíamos obter o conteúdo;
- **Bits não significativos:** A moderna esteganografia utiliza o uso de bits não significativos que são concatenados a mensagem original e faz uso também de área não usada.



Figura 6 - Esteganografia por bits não significativos. Não há diferença visível nas figuras

Os dois métodos (criptografia e esteganografia) podem ser combinados para aumento da segurança. Por exemplo, pode-se criptografar uma mensagem e em seguida, utilizar a técnica de esteganografia, trocando-se os *bits* menos significativos de uma imagem digitalizada pelos *bits* da mensagem criptografada, e então transmitir a imagem. Se a imagem for interceptada, primeiro será necessário descobrir a mensagem oculta entre os *bits* da imagem, e, somente após isso, poderá ocorrer a tentativa de descryptografia.

5. Aplicação da Criptografia em Rede Privada Virtual

Uma Rede Privada Virtual (*Virtual Private Network - VPN*) é definida pela RFC 4949 como sendo uma conexão de computadores com uso restrito, que se estabelece sobre a estrutura física de uma rede pública, como a Internet. Utiliza-se de tecnologias como criptografia e tunelamento de links da rede virtual sob a rede real. Por exemplo, cita a ligação de várias LAN's de uma empresa através da Internet. Usando-se o firewall de cada LAN pode-se criar uma VPN entre as LAN's, usando túneis encriptados ligando um firewall a outro.

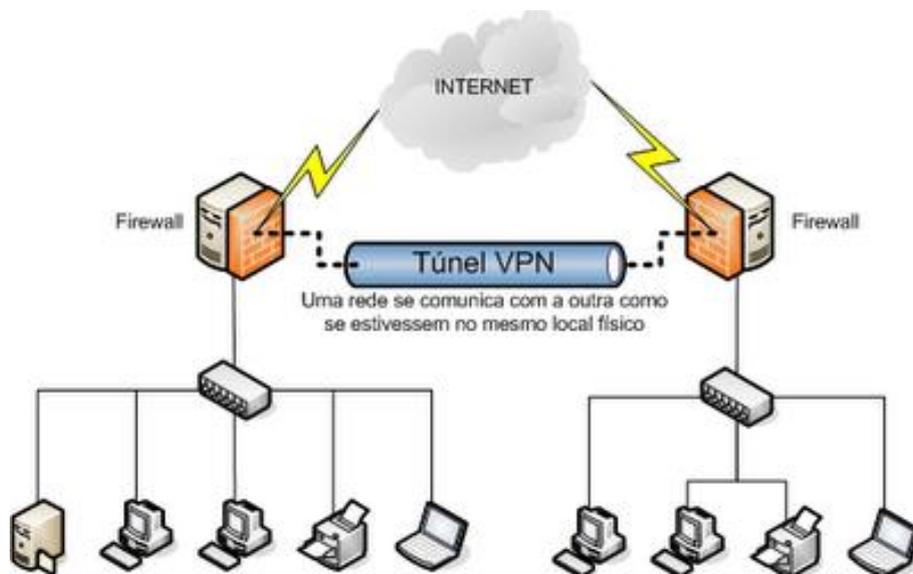


Figura 7 - Esquema de VPN

A VPN é uma solução para empresas que possuem funcionários em deslocamento e que precisam constantemente acessar os dados que estão na rede da empresa. O usuário simplesmente conecta-se a Internet pelo meio disponível e inicia a conexão através da VPN. Uma VPN possibilita uma conexão segura através de três serviços em conjunto (Figura 8):

- **Autenticação:** estabelece a identificação do remetente e do receptor da informação. É implementada através de senhas e identificação dos usuários;
- **Criptografia:** implementada através de algoritmo de criptografia aplicado sobre a mensagem ou texto. Quanto maior a chave de criptografia, maior será a dificuldade de quebrar essa chave;
- **Encapsulamento:** a VPN encapsula a mensagem criptografada em pacotes com o seu próprio endereço como origem, processo também conhecido como tunelamento. Existem dois tipos de tunelamento: tunelamento fim a fim (conexão de cliente ao servidor) e tunelamento nó a nó (conecta várias LAN's).

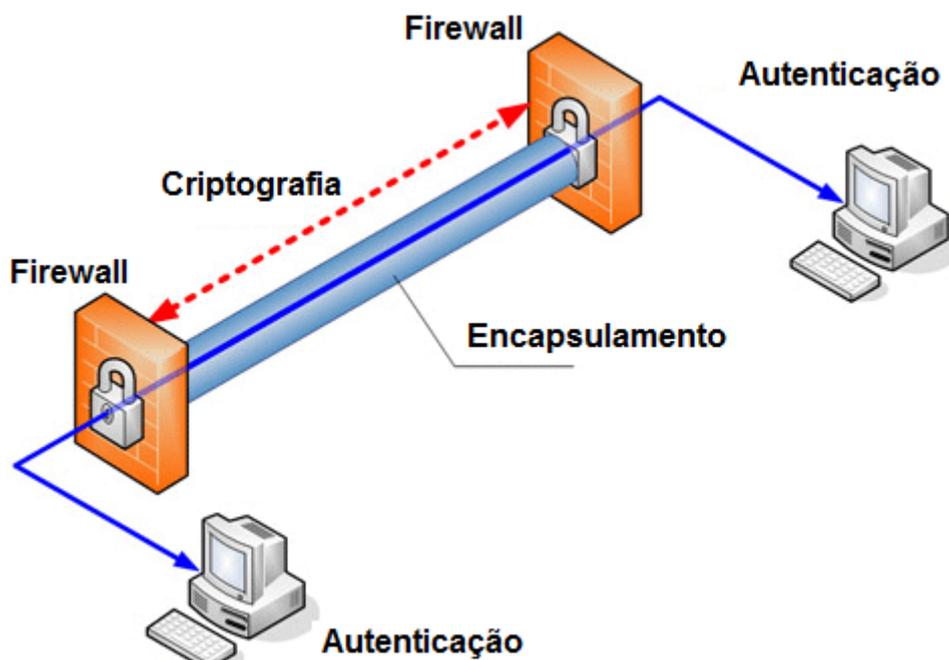


Figura 8 – Serviços na conexão com VPN