Criptografia

1. Introdução

O envio e o recebimento de informações são uma necessidade antiga, proveniente de centenas de anos. Nos últimos tempos, o surgimento da Internet e de tantas outras tecnologias trouxe muitas facilidades para a transmissão de informações.

Junto a esse quadro, o conceito de **criptografia** se tornou cada vez mais necessário, tornando-se uma ferramenta fundamental para permitir que apenas emissor e receptor tenham acesso à informação trabalhada.

2. Conceitos e Terminologias

2.1. Criptografia

Criptografia (do grego *kryptós*, "escondido", e gráphein, "escrita") conjunto de conceitos e técnicas que visa codificar uma informação de forma que somente o emissor e o receptor possam acessá-la, evitando assim que um intruso consiga interpretá-la. É o ato de transformar alguma informação legível em ilegível para pessoas não autorizadas.

2.2. Criptoanálise e Criptologia

Criptoanálise é a análise das diversas técnicas de encriptação e decriptação, ou seja, estudo das melhores maneiras de esconder os dados e como consegui lê-los quando criptografados.

A fusão da criptografia com a criptoanálise forma a **criptologia**. Algumas pessoas consideram criptografia e criptologia palavras sinônimas, e outras preferem diferenciá-las, usando criptologia para se referir à ciência e criptografia para se referir à prática da escrita secreta.

2.3. Cifragem, Decifragem e Algoritmo

Cifragem é o processo de conversão de um texto claro para um código cifrado; **decifragem** é o processo de recuperação do texto original a partir de um texto cifrado.

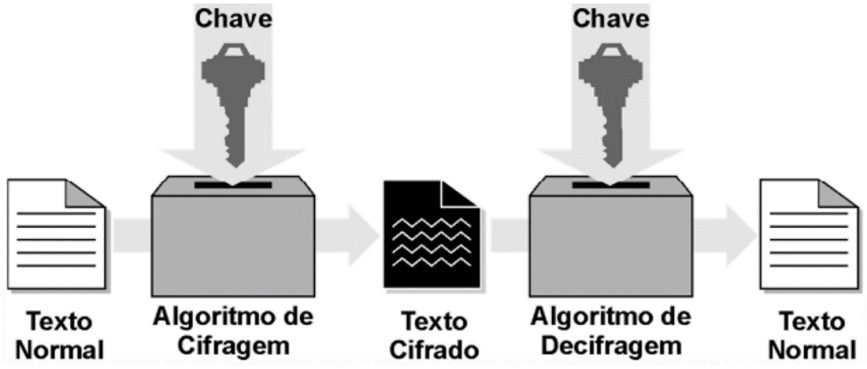

Figura 1: Cifragem e decifragem.

Algoritmo é a especificação da sequência ordenada de passos que deve ser seguida para a solução de um problema ou para a realização de uma tarefa.

A criptografia moderna é formada basicamente pelo estudo dos algoritmos criptográficos que podem ser implementados em computadores.

Termo	Significado
Texto claro	Informação legível (original) que será codificada.
Texto codificado	Texto ilegível gerado pela codificação de um texto claro.
Codificar (cifrar)	Ato de transformar um texto claro em um texto codificado.
Decodificar (decifrar)	Ato de transformar um texto codificado em um texto claro.
Método criptográfico	Conjunto de programas responsável por codificar e decodificar informações.
Chave	Similar a uma senha, é utilizada como elemento secreto pelos métodos criptográficos.
Canal de comunicação	Meio utilizado para a troca de informações.
Remetente	Pessoa ou serviço que envia a informação.
Destinatário	Pessoa ou serviço que recebe a informação.

Tabela 1: Termos empregados em criptografia e comunicações via Internet.

3. Objetivos

Os objetivos da criptografia são os seguintes:

- **Confidencialidade**: apenas o destinatário deve ter acesso aos dados da mensagem.
- **Integridade**: o destinatário deve saber se a mensagem foi alterada na transmissão.
- **Autenticidade**: o destinatário deve ter a certeza de quem realmente enviou a mensagem.
- **Não-repúdio**: o remetente não pode negar o envio da mensagem.

4. Cifra de César

A **Cifra de César** (Código de César ou Cifra de Troca) é uma das mais simples e conhecidas técnicas de criptografia. Essa técnica foi criada pelo imperador romano Júlio César, em 50 a.C.

Segundo Suetónio (escritor latino de *A Vida de Júlio César*), se ele tinha qualquer coisa confidencial a dizer, ele escrevia cifrado, isto é, mudando a ordem das letras do alfabeto, para que nenhuma palavra pudesse ser compreendida. Se alguém deseja decifrar a mensagem e entender seu significado, deve substituir a quarta letra do alfabeto, a saber 'D', por 'A', e assim por diante com as outras.

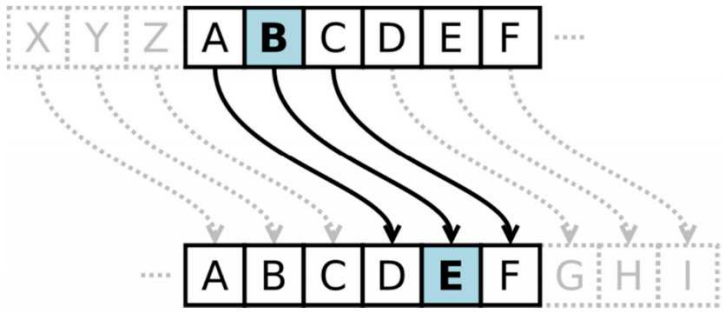

Figura 2: Cifra de César.

O código de César faz parte da classe criptográfica de substituição simples do tipo monoalfabética (usa apenas um alfabeto cifrante) monogrâmica (trata cada um dos caracteres individualmente), e consequentemente possui um nível de segurança baixíssimo. O trabalho de criptoanálise para decifrar o texto cifrado pela cifra de César é bastante simples.

Essa técnica também foi utilizada por oficiais sulistas na Guerra de Secessão americana e pelo exército russo em 1915. Nesse caso foi implementada a cifra ROT13, que se baseia na substituição de cada letra do alfabeto pela letra que está 13 posições após essa letra (A por N, B por O, etc.).

Exemplos:

- **Deslocamento 3**: CIFRA DE CESAR → FLIUD GH FHVDU.
- **Deslocamento 13**: GUERRA DE SECESSAO → THREEN QR FRPRFFNB.

5. Chaves

Em relação ao tipo de chave utilizada, os métodos criptográficos são classificados em duas categorias: **criptografia de chave simétrica** e **criptografia de chaves assimétricas**.

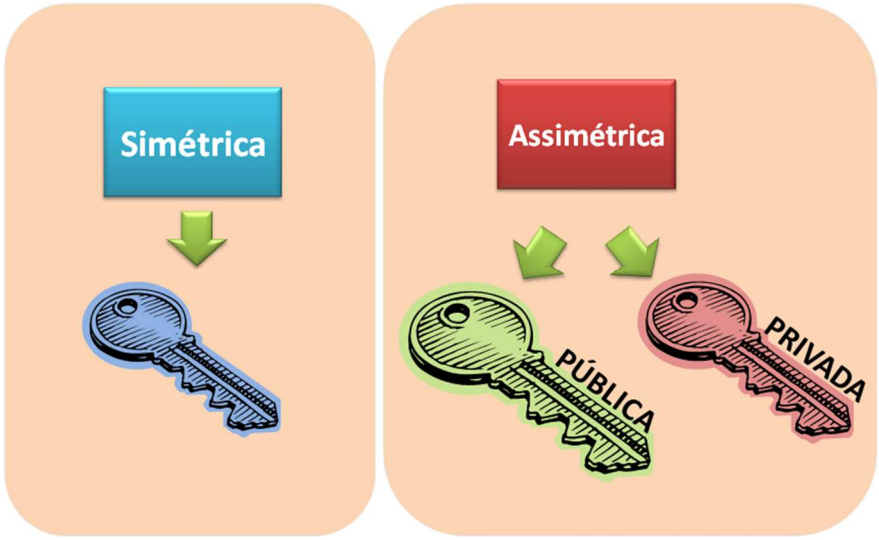

Figura 3: Chave simétrica e chaves assimétricas.

5.1. Criptografia de Chave Simétrica

A **criptografia de chave simétrica** (criptografia de chave secreta ou única) utiliza uma só chave tanto para encriptar (cifrar) como para decriptar (decifrar) informações.

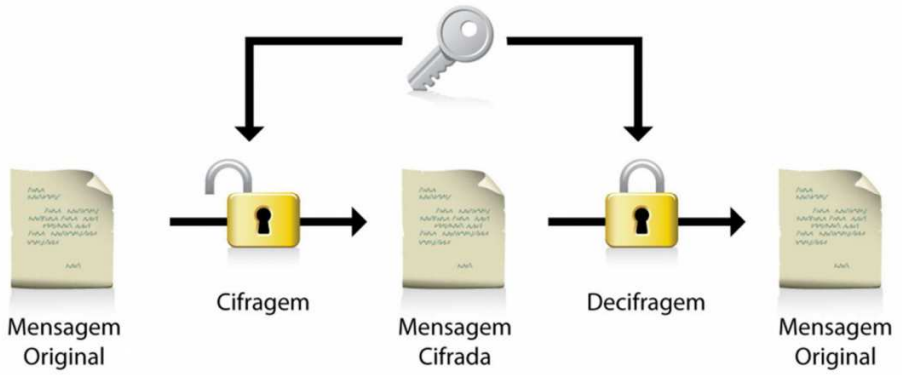

Figura 4: Criptografia de chave simétrica.

A principal utilização dessa técnica se dá quando a informação é criptografada e decriptografada pela mesma pessoa, pois não há necessidade do compartilhamento da chave.

A desvantagem da chave simétrica é quando pessoas ou equipamentos diferentes participam da operação de codificação/decodificação, já que se deve compartilhar a chave entre os participantes. Essa operação deve ser feita por meio de um canal de comunicação seguro (garantindo a confidencialidade), pois se alguém não autorizado interceptar a comunicação e tomar posse da chave poderá ler toda e qualquer informação manipulada pela chave.

Uma boa vantagem do uso de chave simétrica é que seu processamento é rápido (se comparada ao uso de chaves assimétricas) e mais indicado para garantir a confidencialidade de grandes volumes de dados.

Alguns métodos criptográficos que fazem uso de chave simétrica são:

- **DES** – *Data Encryption Standard*;
- **3DES** – Variação do DES;
- **IDEA** – *International Data Encryption Algorithm*;
- **RC** – *Ron's Code / Rivest Cipher*;
- **AES** – *Advanced Encryption Standard*.

5.2. Criptografia de Chaves Assimétricas

A **criptografia de chaves assimétricas** (criptografia de chave pública) utiliza duas chaves distintas: uma pública, que pode ser divulgada livremente, e uma privada, que deve ser mantida em sigilo.

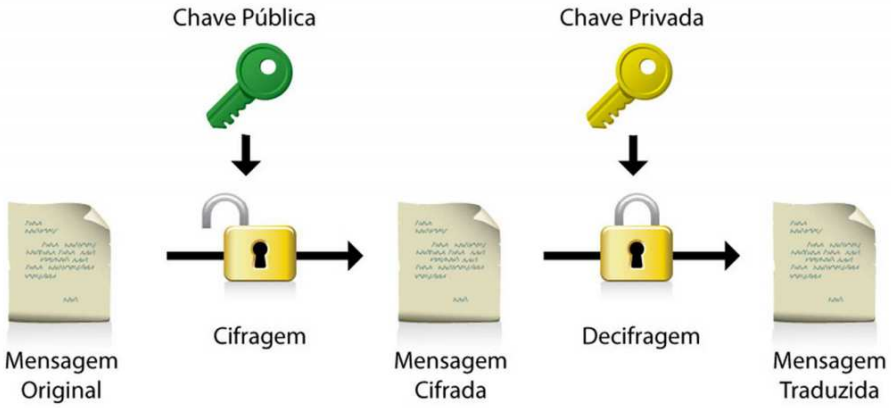

Figura 5: Criptografia de chaves assimétricas.

Com o uso de chaves assimétricas, se uma informação é codificada com uma chave, ela só poderá ser decodificada pela outra chave. A cifragem da informação pode ser feita por qualquer uma das chaves dependendo da finalidade desejada (confidencialidade ou autenticação, integridade e não repúdio).

Se por um lado a criptografia chaves assimétricas cobre a desvantagem da criptografia de chave simétrica no que diz respeito ao risco no compartilhamento da chave (dispensa até mesmo o uso de um canal de comunicação seguro), por outro lado o seu processamento é mais lento quando é utilizada com grandes volumes de dados.

Alguns métodos criptográficos que fazem uso de chaves assimétricas são:

- **RSA** – *Rivest, Shamir and Adleman*;

- **ElGamal**;
- **DSA** – *Digital Signature Algorithm*.

6. Função Hash

Função Hash se trata de um método criptográfico que, quando aplicado sobre uma informação, independentemente do tamanho que ela tenha, gera um resultado único e de tamanho fixo, chamado hash.

A função hash é um algoritmo unidirecional, que impossibilita a descoberta do conteúdo original da informação a partir do hash (resultado). Qualquer modificação na informação original irá resultar em um hash diferente (é teoricamente possível que informações distintas gerem hashes iguais, mas a possibilidade disso acontecer é extremamente baixa).

O hash é, em geral, representado em base hexadecimal (0 a 9 e A a F).

Alguns exemplos de funções hash:

- **Whirlpool**;
- **MD5** - *Message-Digest Algorithm 5*;
- **SHA-1** - *Secure Hash Algorithm*;
- **SHA-256**;
- **SHA-512**.

6.1. MD5

O **MD5** é um algoritmo de hash de 128 bits (32 caracteres hexadecimais) unidirecional desenvolvido pela RSA Data Security, Inc., é muito utilizado por softwares com protocolo ponto-a-ponto (P2P) na verificação de integridade de arquivos e logins.

Exemplos:

- CRIPTOGRAFIA → 2437F60358006BEBE71B8367DFB77E1B;
- CRIPTOGRAFIa → D2751A930A2F8FBF4DF785AEE6CBE613.

6.2. SHA-1

SHA-1 é a função mais utilizada da família de SHA (*Secure Hash Algorithm*), possuindo saída de 160 bits (40 caracteres hexadecimais), foi considerada a sucessora da MD5. É usada em uma grande variedade de aplicações e protocolos de segurança, incluindo TLS, SSL, PGP, SSH, S/MIME e IPSec.

Exemplos:

- CRIPTOGRAFIA → 5158EF595F8FAC293DC3C8B770FA3B95FB625DFE;

- CRIPTOGRAFIa → E64913C94080FFCEAA193C0CE44028CD7080FFEA.

7. Assinatura Digital

A **assinatura digital** é um método criptográfico que, como o próprio nome já revela, tem uma ideia similar à assinatura típica de papel. Sua principal função é garantir a autenticidade, a integridade e o não repúdio.

Existem algumas formas de se trabalhar com assinatura digital, mas o mais comum é com a utilização de dois métodos criptográficos: função hash e criptografia de chaves assimétricas.

Primeiramente, a função hash é aplicada sobre a mensagem original, gerando o seu hash (resultado) correspondente. Logo depois, o autor da mensagem faz uso de sua chave privada para criptografar o hash que foi gerado anteriormente, armazenando o hash criptografado junto com a mensagem original.

Para verificar a validade da assinatura basta usar a chave pública para decodificar o hash codificado. Com o resultado da decriptografia, deve-se passar novamente a mensagem original pela mesma função hash, a fim de comparar se o novo resultado será igual ao hash decodificado. Se os hashes forem iguais, a mensagem está íntegra.

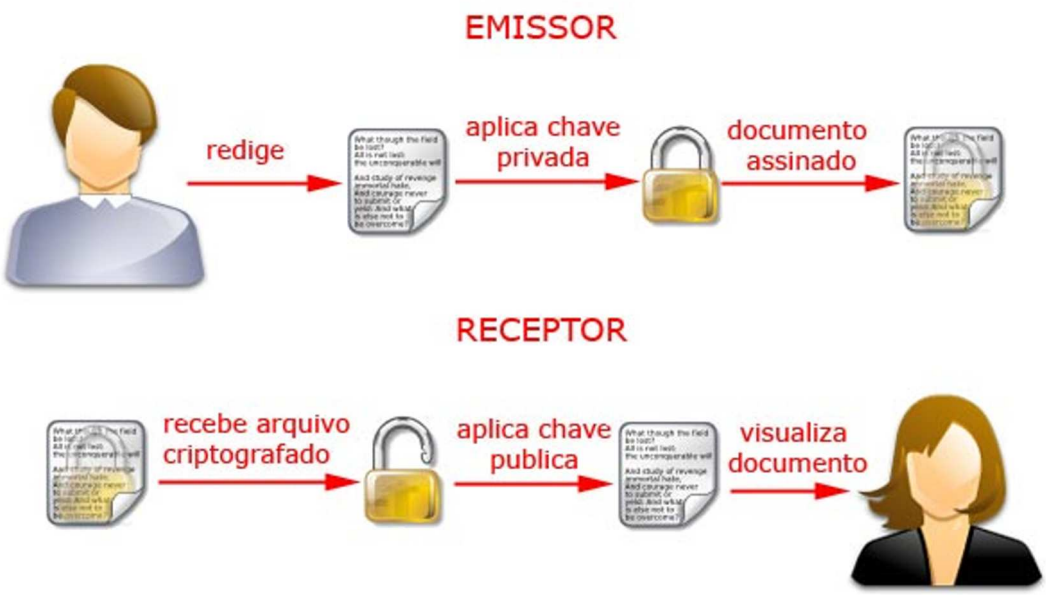

Figura 6: Processo de assinatura digital.

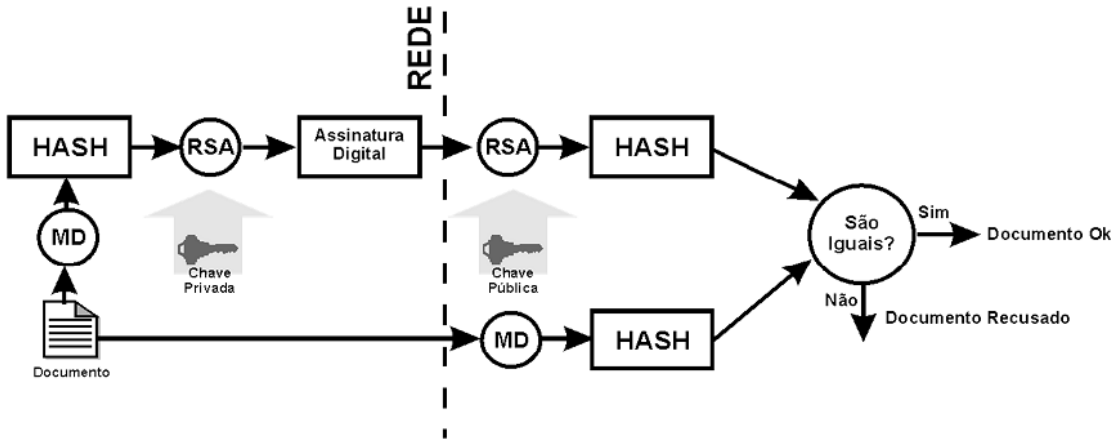

Figura 7: Geração e verificação da assinatura digital.

8. Certificado Digital

Fortemente relacionado ao conceito de assinatura digital, o **certificado digital** trata-se de um registro eletrônico composto por um conjunto de dados que distingue uma entidade (pessoa, serviço, etc.) e associa a ela uma chave pública. Em outras palavras, pode ser considerado como a certificação de uma assinatura digital.

O certificado digital pode ser comparado ao nosso CPF (Cadastro de Pessoa Física), pois é como um documento no qual consta a identificação de seu dono e de quem o emitiu. Em relação ao órgão emissor de certificados digitais, a entidade responsável pela emissão é chamada de Autoridade Certificadora (AC). Existem também as Autoridades de Registro (AR), que fazem apenas o registro do pedido do certificado.

A AC, além de ser responsável pela emissão de certificados, também é responsável por publicar informações sobre certificados que deixaram de ser confiáveis. A própria AC pode descobrir que um certificado não é mais confiável, como também pode ser informada disso, e então o inclui na chamada Lista de Certificados Revogados (LCR). A AC divulga essa lista periodicamente, constando informações como o número de série dos certificados e as respectivas datas de revogação.

As figuras a seguir ilustram como o Google Chrome apresenta informações de certificação digital (embora os campos apresentados sejam padronizados, a representação gráfica pode variar entre diferentes navegadores e sistemas operacionais).

Figura 8: Exemplo de certificado digital (layout do Google Chrome).

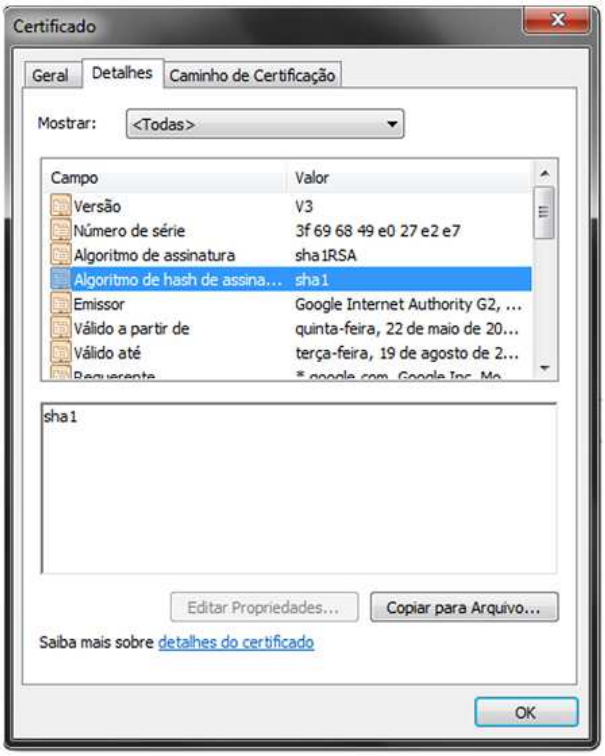

Figura 9: Exemplo de certificado digital (layout do Google Chrome).

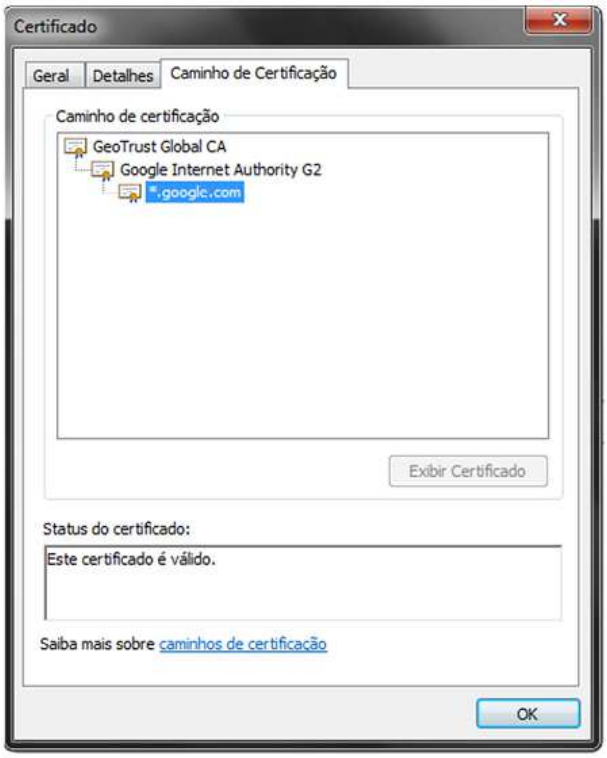

Figura 10: Exemplo de certificado digital (layout do Google Chrome).

Geralmente, os dados básicos que compõem um certificado digital são:

- Versão e número de série do certificado;
- Dados que identificam a AC que emitiu o certificado;
- Dados que identificam o dono do certificado;
- Chave pública do dono do certificado;
- Validade do certificado (quando foi emitido e até quando é válido);
- Assinatura digital da AC emissora e dados para verificação da assinatura.

9. Ataques

O sistema de criptografia usado atualmente é extremamente seguro. Especialistas estimam que para alguém quebrar uma criptografia usando chaves de 64 bits na base da tentativa-e-erro, levaria cerca de 100.000 anos usando um PC comum.

9.1. Força Bruta

Um **ataque de força bruta** é uma técnica utilizada para quebrar a cifragem de um dado. Utiliza um algoritmo de busca para percorrer uma lista de chaves possíveis até que a chave correta seja encontrada. Apesar do ataque de força bruta poder ser realizado manualmente, na grande maioria dos casos, ele é realizado com o uso de ferramentas automatizadas facilmente obtidas na Internet tornando o ataque bem mais efetivo.

Mesmo que o atacante não consiga descobrir a senha em questão, há a possibilidade de haver problemas, pois muitos sistemas bloqueiam contas quando várias tentativas de acesso sem sucesso são realizadas.

Dependendo de como é realizado, um ataque de força bruta pode resultar em um **ataque de negação de serviço** (**DoS** - *Denial of Service*), devido à sobrecarga produzida pela grande quantidade de tentativas realizadas em um pequeno período de tempo.

Curiosidade

Um site chamado Distributed.net (www.distributed.net) conseguiu vencer um concurso promovido pela RSA Security (www.rsasecurity.com), pagando US$ 10.000 para o primeiro que conseguisse quebrar sua criptografia de 64 bits.

Só um detalhe: o Distributed.net conseguiu quebrar essa senha porque ele pedia para as pessoas que rodassem em seu computador parte do processo de tentativa-e-erro, baixando um programa existente no site deles. No total foram 300.000 pessoas colaborando com esse projeto ao longo de 5 anos.

10. Exercícios de Fixação

1) Explique com suas palavras o conceito de criptografia.
2) Defina encriptação, decriptação e algoritmo.
3) Os objetivos da criptografia são: confidencialidade, integridade, autenticidade e não-repúdio. Explique cada um deles.
4) Cite características, vantagens e desvantagens da criptografia simétrica e da criptografia assimétrica.
5) O processo de uma função hash é unidirecional. O que isso quer dizer?
6) Explique como se dá o processo da assinatura digital e do certificado digital.
7) Suponha que Bob quer enviar uma mensagem secreta a Alice usando criptografia de chave pública. Neste caso, o que ele deve fazer?

11. Pesquisas

- MD4;
- SHA-256;
- SHA-512;
- WHIRLPOOL.

12. Referências

- Criptografia
  - http://www.infowester.com/criptografia.php
  - http://cartilha.cert.br/criptografia/
  - http://pt.wikipedia.org/wiki/Criptografia
- Criptoanálise
  - http://ciencia.hsw.uol.com.br/cracker.htm
  - http://pt.wikipedia.org/wiki/Criptoan%C3%A1lise
- Código de César
  - www.numaboa.com.br/criptografia/67-cripto-exercicios/166-Cesar
- Função Hash
  - http://www.gta.ufrj.br/grad/09_1/versao-final/assinatura/hash.htm
  - http://www.techtudo.com.br/artigos/noticia/2012/07/o-que-e-hash.html
  - http://pt.wikipedia.org/wiki/Fun%C3%A7%C3%A3o_hash
- Assinatura Digital
  - http://www.tecmundo.com.br/web/941-o-que-e-assinatura-digital-.htm
  - http://pt.wikipedia.org/wiki/Assinatura_digital
- Certificado Digital
  - https://www.oficioeletronico.com.br/Downloads/CartilhaCertificacaoDigital.pdf
  - http://www.infowester.com/assincertdigital.php
  - http://pt.wikipedia.org/wiki/Certificado_digital