

Matemática Computacional

Prof. MSc. Luis Gonzaga de Paulo

Criptografia

- Criptografia
- Cifra e Código
- Algoritmos e sistemas criptográficos:
 - Criptografia simétrica
 - Criptografia assimétrica
 - Hash
 - Assinatura Digital
 - Certificados Digitais

Para pensar...

- Como garantir a confidencialidade, a integridade e a disponibilidade das informações digitais?
- Como assegurar-se de estar comunicando com o interlocutor correto?
- É possível evitar golpes e fraudes no mundo digital?
- Quem pode garantir que a comunicação é segura?

CRIPTOGRAFIA

Origem do termo no Grego:

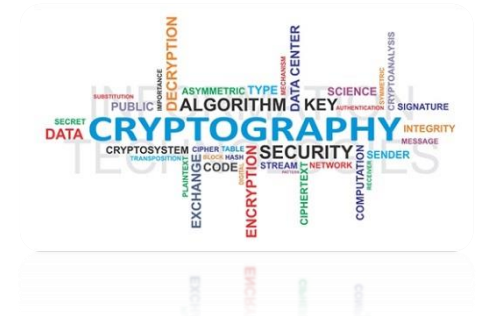
- Kryptós = Escondido;
- Gráphein = Escrita;
- Criptografia = Escrita escondida.



CRIPTOGRAFIA

Área da Matemática destinada ao estudo de técnicas e princípios de transformação da informação de sua forma original para outra, ininteligível, de forma que possa ser utilizada apenas quando autorizado.

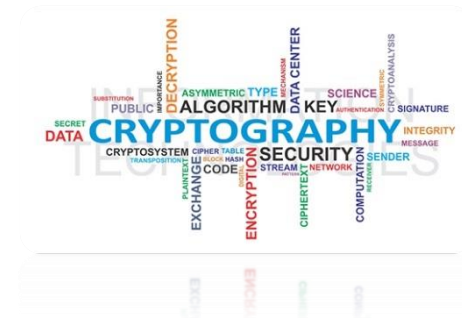
- Transformação de texto plano (*plain text*) em texto cifrado (cifragem) ou o contrário (decifragem);
- Uso de algoritmos criptográficos em programas de computador;
- Criptoanálise, Esteganografia, Esteganalise, Código, Critpologia.



CRIPTOGRAFIA

A criptografia contribui para a solução dos problemas de:

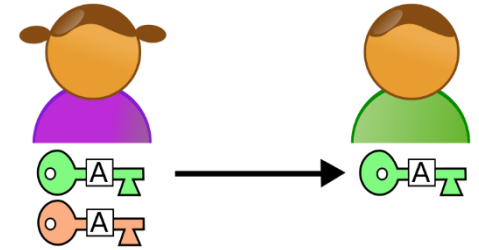
- Confidencialidade;
- Integridade;
- Disponibilidade;
- Privacidade;
- Autenticação;
- Irretratabilidade ou não-repúdio;



CRIPTOGRAFIA

Técnicas e métodos:

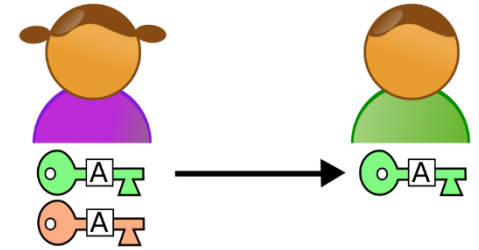
- Criptografia assimétrica (Chave Pública);
- Criptografia simétrica (Chave única);
- Resumo criptográfico (*Hash*);
- Assinatura digital;
- Certificação digital;



CIFRA E CÓDIGO

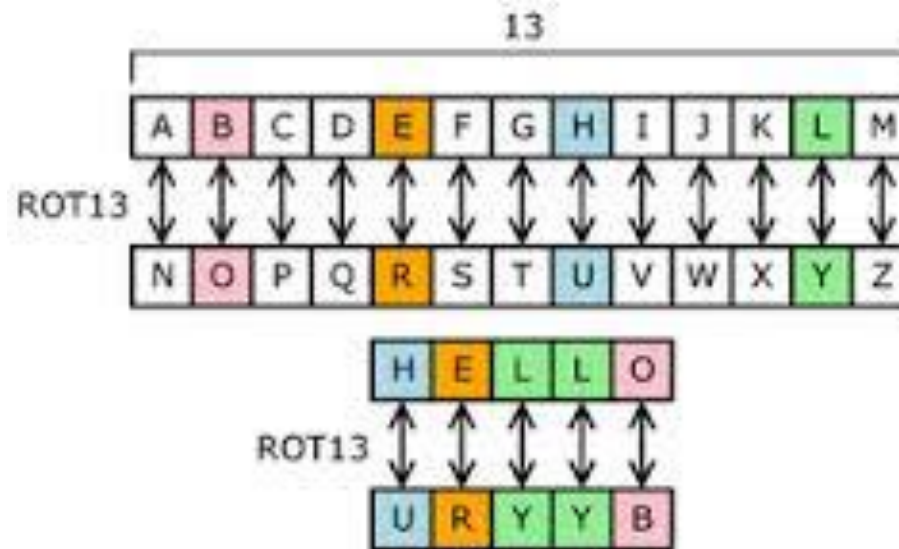
Cifra x Código:

- **Cifragem** é o tratamento de elementos mínimos da informação (nos computadores, o Bit) para dificultar a compreensão;
- **Codificação** é a substituição de palavras ou elementos da comunicação com o propósito de dificultar a compreensão;



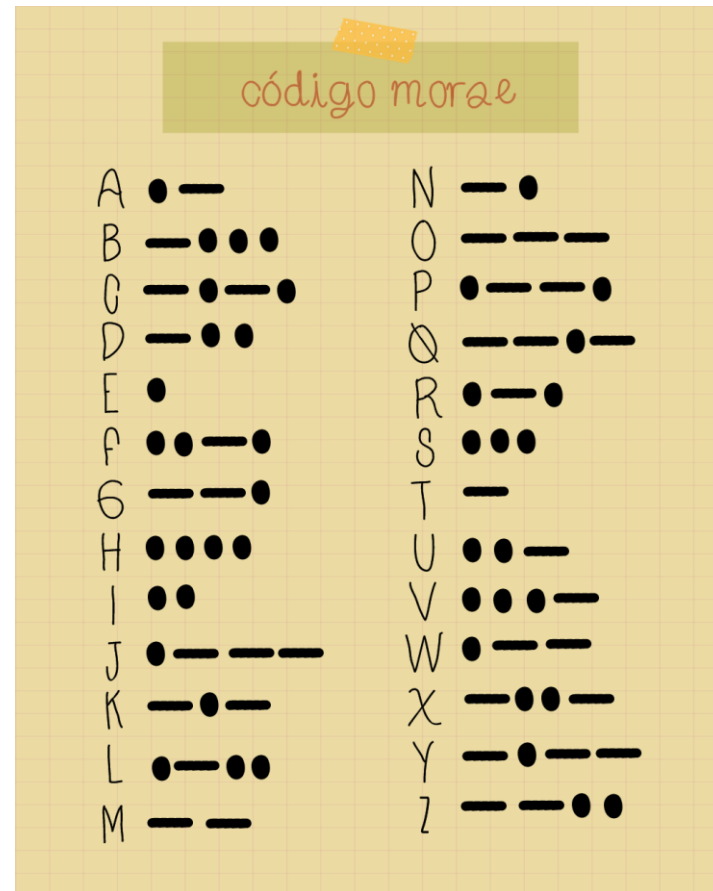
CIFRA E CÓDIGO

Cifra x Código:



CIFRA E CÓDIGO

Cifra x Código:



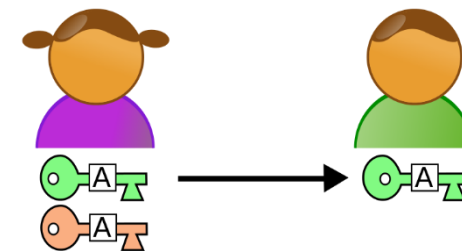
A hand-drawn code chart on a grid background. At the top center, there is a yellow sticky note with the text "código morse" written in red cursive. Below the sticky note, the chart lists the Morse code for letters A through Z, arranged in two columns. Each letter is followed by its corresponding sequence of dots (•) and dashes (—).

código morse	
A • —	N — •
B — • • •	O — — —
C — • — •	P • — — •
D — • •	Q — — • —
E •	R • — •
F • • — •	S • • •
G — — •	T —
H • • • •	U • • —
I • •	V • • • —
J • — — —	W • — —
K — • —	X — • • —
L • — • •	Y — • — —
M — —	Z — — • •

ALGORITMOS E SISTEMAS CRIPTOGRÁFICOS

Existem inúmeros modelos e técnicas de criptografia, entre os quais:

- **Hash:** MD5, SHA-1, RIPEMD-160, Tiger;
- **Free/Open Source:** PGP, GPG, SSL, IPSec, Free S/WAN;
- **Chave Pública (Assimétrica):** Diffie-Hellman, DSA, RSA;
- **Chave Única (Simétrica):** Enigma, DES/3-DES, RC4, RC5, Blowfish, IDEA, AES, RC6;



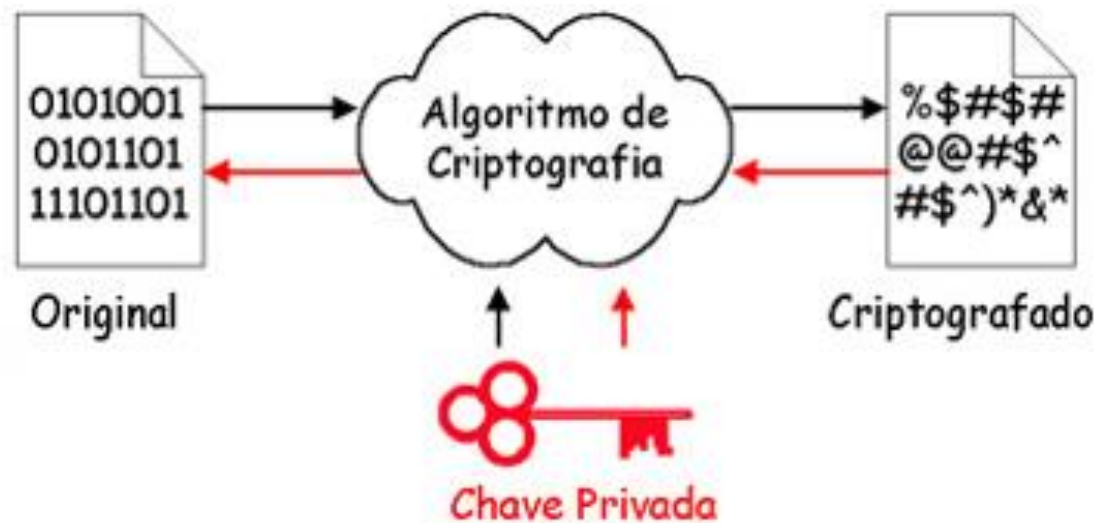
ALGORITMOS E SISTEMAS CRIPTOGRÁFICOS

- Os processos de **cifragem** e **decifragem** são obtidos por meio de um ou mais algoritmo.
- Os algoritmos utilizam funções matemáticas muito elaboradas e a fatoração de números primos para a geração da chave criptográfica.



ALGORITMOS E SISTEMAS CRIPTOGRÁFICOS

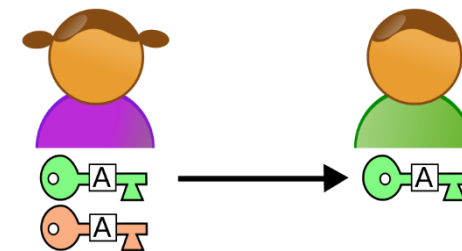
Na criptografia simétrica uma única chave – privada – é compartilhada e usada para cifrar e decifrar.



ALGORITMOS E SISTEMAS CRIPTOGRÁFICOS

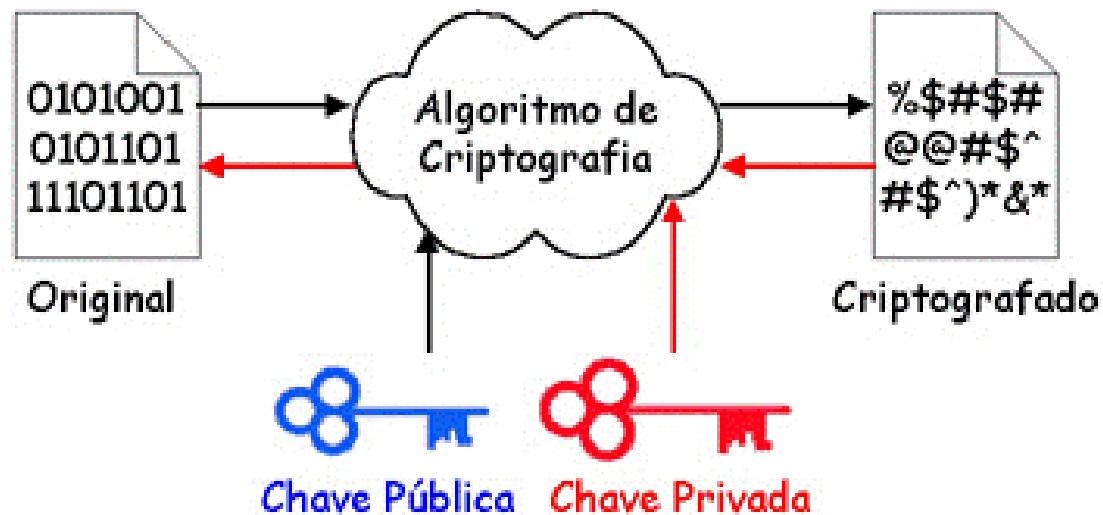
Na criptografia simétrica, se Bob quer compartilhar informações com Alice:

- 1) Bob gera uma chave criptográfica e encaminha para Alice;
- 2) Bob cifra a mensagem com a chave gerada e envia para Alice;
- 3) Alice decifra a mensagem com a chave recebida;
- 4) Se Alice quiser responder a Bob, usa a mesma chave para cifrar a resposta e enviar para Bob.



ALGORITMOS E SISTEMAS CRIPTOGRÁFICOS

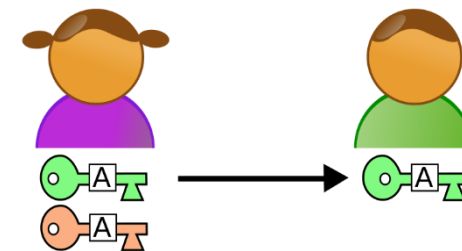
Na criptografia assimétrica um par de chaves – pública/privada – é compartilhado e usado para cifrar e decifrar.



ALGORITMOS E SISTEMAS CRIPTOGRÁFICOS

Na criptografia assimétrica, se Bob quer compartilhar informações com Alice:

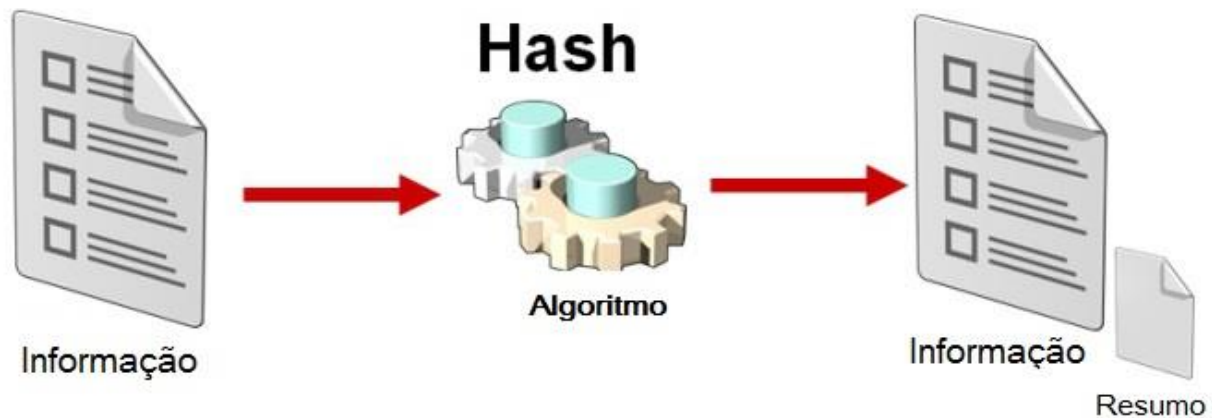
- 1) Alice compartilha sua chave pública com Bob;
- 2) Bob cifra a mensagem com a chave pública e envia para Alice;
- 3) Alice decifra a mensagem com a sua chave privada;
- 4) Se Alice quiser responder a Bob, usa sua privada para cifrar a resposta e enviar para Bob;
- 5) Bob usa a chave pública de Alice para decifrar a resposta;



ALGORITMOS E SISTEMAS CRIPTOGRÁFICOS

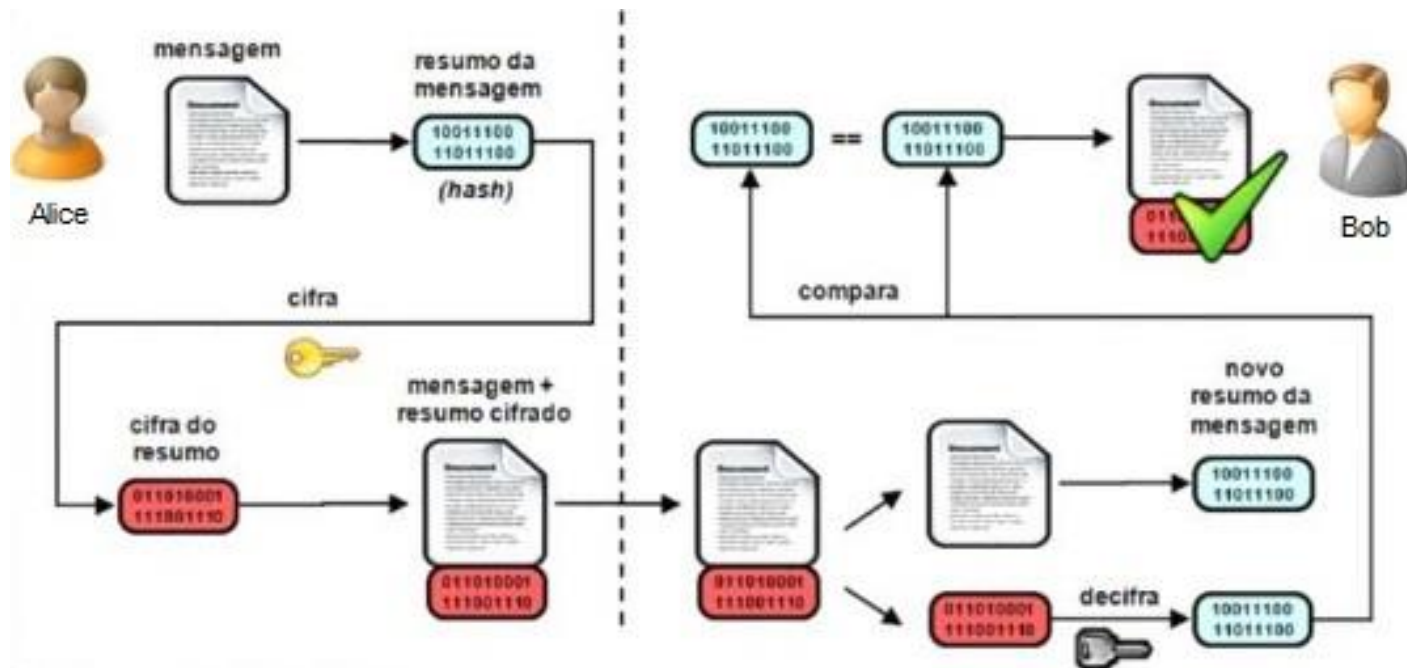
O **Hash** é um resumo criptográfico de comprimento padrão, gerado por funções matemáticas e tabelas de *hashing*;

Exemplos online: [MD5](#) [Diversos](#)



ALGORITMOS E SISTEMAS CRIPTOGRÁFICOS

A Assinatura Digital é um processo criptográfico para assegurar o não-repúdio da comunicação.



ALGORITMOS E SISTEMAS CRIPTOGRÁFICOS

A Assinatura Digital possibilita:

- Garantir que o emissor da comunicação seja conhecido do destinatário;
- Assegurar que o emissor da mensagem não possa repudiar uma mensagem que enviou;
- Assinar a mensagem com a chave privada do emissor;
- Acessar a mensagem com a chave pública do emissor;

ALGORITMOS E SISTEMAS CRIPTOGRÁFICOS

Um Certificado Digital é um arquivo de computador que contém:

- Um conjunto de informações referentes à entidade para a qual o certificado foi emitido (empresa, pessoa física ou computador)
- A chave pública referente à chave privada que se acredita estar de posse somente da entidade especificada no certificado.

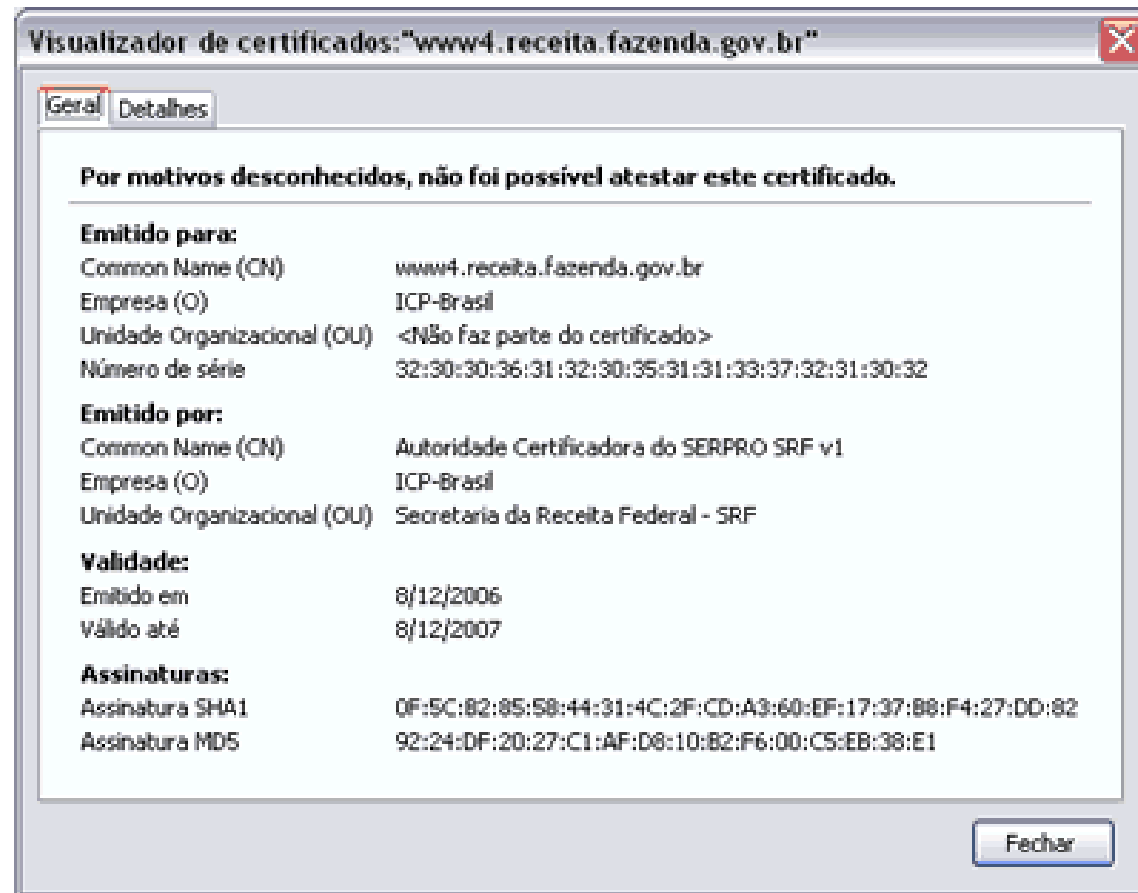
ALGORITMOS E SISTEMAS CRIPTOGRÁFICOS

Um Certificado Digital é usado para ligar uma entidade a uma chave pública.

- O certificado digital é assinado pela Autoridade Certificadora (AC) que o emitiu;
- A AC normalmente faz parte da ICP – Infraestrutura de Chaves Públicas;
- As assinaturas contidas em um certificado são atestados feitos por uma entidade que diz confiar nos dados contidos naquele certificado.

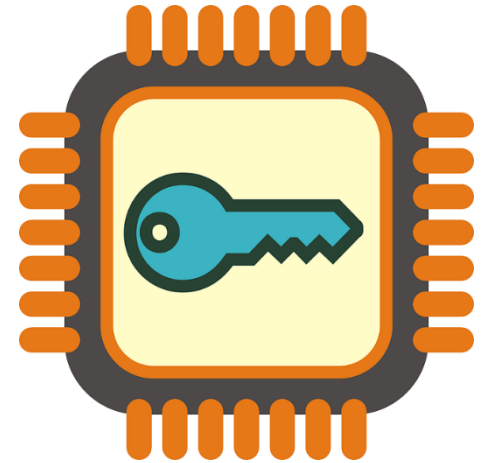
ALGORITMOS E SISTEMAS CRIPTOGRÁFICOS

Um exemplo de certificado digital:



Aplicação

- A criptografia tem um vasto uso na comunicação digital, e está presente em quase todas as trocas de informação feitas deste modo.
- A criptografia não é o único recurso – e tampouco o mais importante – para a garantia da segurança da informação, e requer profundo conhecimento da matemática computacional.
- A criptografia é uma das áreas da computação que mais tem exigido e recebido investimentos em termos de pesquisa e desenvolvimento.



Síntese

- Nesta aula foram abordados os conceitos e a aplicação da Criptografia nos sistemas computacionais e na comunicação digital;
- Foram apresentadas também as características da cifragem e da codificação;
- Alguns algoritmos e sistemas criptográficos, tais como os de criptografia simétrica, de criptografia assimétrica, de Hash, de Assinatura Digital e de certificados digitais foram abordados.