

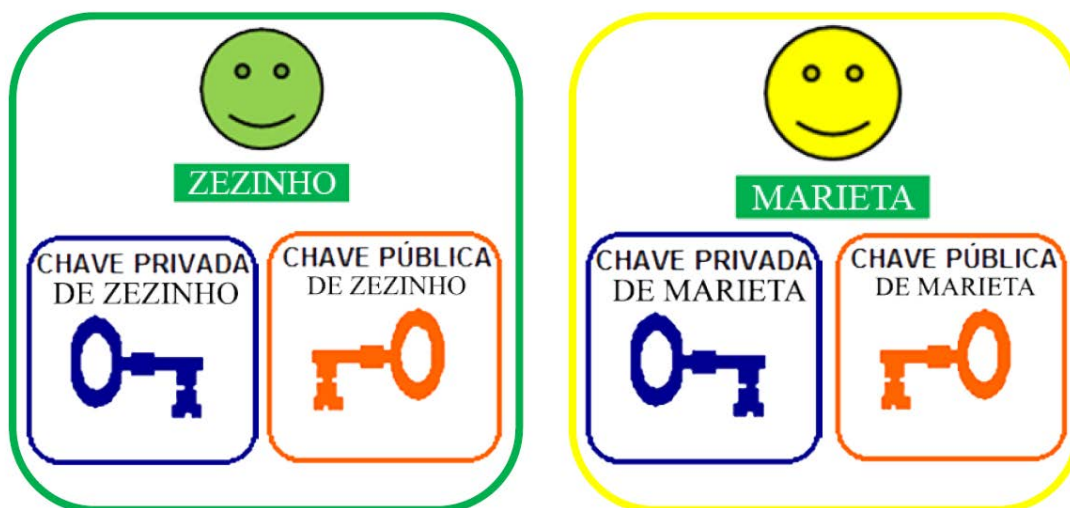
SEGURANÇA DA INFORMAÇÃO IV

CRIPTOGRAFIA ASSIMÉTRICA

No pix, há duas chaves: a chave pública e a analogia com a conta bancária. Numa transação bancária, deve ser fornecida a chave pública, que, de um modo geral, pode comprometer a segurança se for o CPF.

A chave privada é única e intransferível.

Para cada pessoa, há duas chaves: os dados públicos, que são os dados da conta; e os dados privados, que são as senhas.



As chaves das pessoas não se misturam.

CHAVES DE UMA MESMA PESSOA



Obs.: | não há como usar a chave pública de uma pessoa com a chave privada de outra pessoa.



CRIPTOGRAFIA ASSIMÉTRICA

PODE SER UTILIZADA PARA GARANTIR:

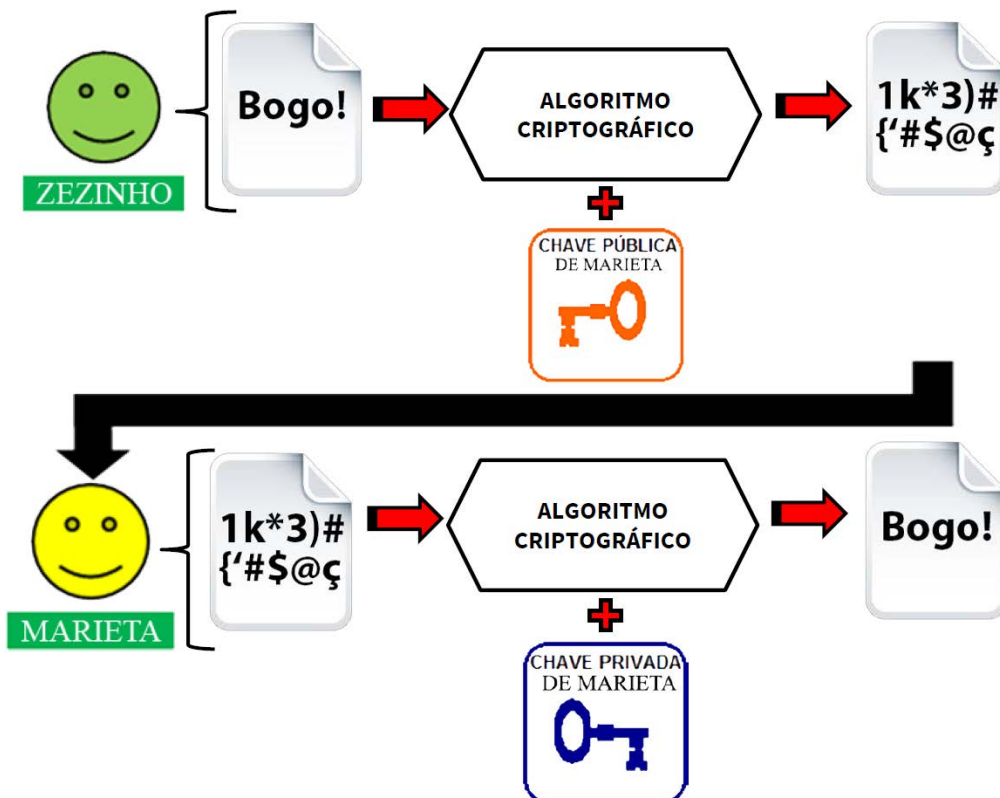
I – SIGILO.

II – AUTENTICIDADE.



I – SIGILO

Entende-se que outras pessoas não podem ter acesso ou se tiverem acesso, não são capazes de compreender.



Zeinho quer passar a informação “Bogo” para Marieta. Passa pelo algoritmo criptográfico.

Se alguém pegar a informação, não vai entender.

Por exemplo, se uma pessoa quer transferir um dinheiro, terá que digitar corretamente os dados públicos de quem vai receber, ou seja, os dados da conta.

II – AUTENTICIDADE

COMO COMPROVAR VIRTUALMENTE A IDENTIDADE DE ALGUÉM?





15m

No “mundo real”, um documento comprova que a pessoa é aquela que alega.
Há como validar os documentos.

CERTIFICADO DIGITAL



Os certificados digitais emitidos por meio de uma boa infraestrutura têm amparo legal.

ASPECTO LEGAL NO BRASIL – MEDIDA PROVISÓRIA N. 2.200-2

Art. 1º Fica instituída a Infraestrutura de Chaves Públicas Brasileira – ICPBrasil, para garantir a autenticidade, a integridade e a validade jurídica de documentos em forma eletrônica, das aplicações de suporte e das aplicações habilitadas que utilizem certificados digitais, bem como a realização de transações eletrônicas seguras.

Fonte: http://www.planalto.gov.br/ccivil_03/MPV/Antigas_2001/2200-2.htm

INFRAESTRUTURA DE CHAVES PÚBLICAS DO BRASIL – ICP BRASIL

- Autoridade Certificadora Raiz (ITI) – Raiz única;
- Autoridades de Registro (AR);
- Autoridades Certificadoras (AC);
- Autoridade Certificadora do Tempo (ACT).



20m

AUTORIDADE CERTIFICADORA RAIZ (ITI)

- Emitir, expedir, distribuir, revogar e gerenciar os certificados das autoridades certificadoras;
- Emitir a Lista de Certificados Revogados – LCR;

Obs.: | por exemplo, alguém possui uma Carteira de Identidade emitida por órgão oficial, mas com dados falsos.

- Fiscalizar e auditar as Autoridades Certificadoras – ACs, Autoridades de Registro – ARs e demais prestadores de serviço habilitados na ICP-Brasil.

Obs.: | função de órgão regulamentador.

Fonte: <https://www.iti.gov.br/icp-brasil/entes-da-icp-brasil> Infraestrutura de Chaves Públicas do Brasil – ICP Brasil

AUTORIDADES CERTIFICADORAS (AC)

- Emitir, distribuir, renovar, revogar e gerenciar certificados digitais;
- Tem a responsabilidade de verificar se o titular do certificado possui a chave privada que corresponde à chave pública que faz parte do certificado;
- Cabe também à AC emitir Listas de Certificados Revogados – LCR.

Fonte: <https://www.iti.gov.br/icp-brasil/entes-da-icp-brasil>

AUTORIDADES DE REGISTRO (AR)

Após a pandemia, passou a ser possível a emissão online do Certificado Digital. As AR ainda existem, mas como uma opção.

Quem emite o Certificado Digital é a autoridade certificadora. A AR existe para fazer a validação do documento.



Este material foi elaborado pela equipe pedagógica do Gran Concursos, de acordo com a aula preparada e ministrada pelo professor Jeferson Bogo Severino.

A presente gravação tem como objetivo auxiliar no acompanhamento e na revisão do conteúdo ministrado na videoaula. Não recomendamos a substituição do estudo em vídeo pela leitura exclusiva deste material.