Pontifícia Universidade Católica de Minas Gerais – PUC Minas
Campus de Poços de Caldas
Instituto de Ciências Exatas e Informática – ICEI
Curso de Bacharelado em Ciência da Computação

SEGURANÇA CIBERNÉTICA E CRIPTOGRAFIA DE DADOS

Fundamentos da Criptografia

Prof. Dr. João Benedito dos Santos Junior
Ph.D. in Computing

CRIPTOGRAFIA

Como funciona a criptografia e seus impactos na Segurança Cibernética, principalmente no que se refere a dados e informações

CONCEITO DE CRIPTOGRAFIA

Criptografia (cripto = oculta; grafia = escrita) é caracterizada como a ciência (ou arte) de escrever em códigos cifrados, usando um conjunto de métodos que permite tornar incompreensível uma mensagem (dado ou informação), de forma a permitir que apenas as pessoas autorizadas consigam decifrá-la e compreendê-la.

A palavra **criptografia** tem sua origem no grego e significa escrita oculta. Júlio César escrevia textos criptografados para Cícero e para seus generais, há mais de 2.000 anos. A **Cifra de Cézar** substituía cada letra do texto por outra, deslocada três letras adiante, na ordem alfabética.

A palavra **CESAR** é escrita como **FHVDU**

HISTÓRICO DA CRIPTOGRAFIA

A máquina **Enigma** foi um dos segredos mais bem guardados na **Segunda Grande Guerra**, usada pelos alemães para proteger as comunicações entre os pontos de comando e as embarcações navais.

MOTIVAÇÕES PARA USO DA CRIPTOGRAFIA

CREDIBILIDADE

INTEGRIDADE

Evitar a alteração fraudulenta e/ou a destruição de dados e informações

SIGILO

Proteger dados e informações para que somente pessoas ou processos autorizados consigam utilizá-los

AUTENTICIDADE

Determinar a origem (fonte geradora) de dados e informações

MODELO DE CRIPTOGRAFIA

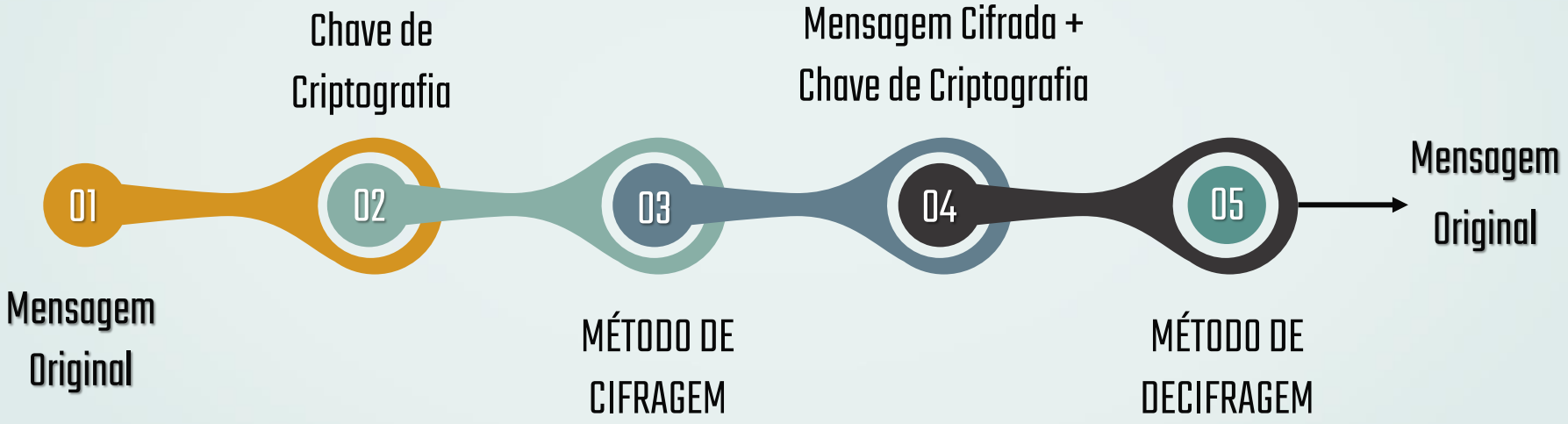
Cifragem

Para cifrar uma mensagem, deve-se usar um método de **cifragem**, que recebe como entrada uma mensagem (dado ou informação) e uma chave de **cifragem**, e produz como resultado uma mensagem cifrada, que pode, então, ser armazenada em um meio qualquer ou transmitida por uma rede de comunicação.

Decifragem

Para decifrar a mensagem, utiliza-se um método de decifragem, que recebe como entrada a mensagem cifrada e uma chave de decifragem, e produz a mensagem original.

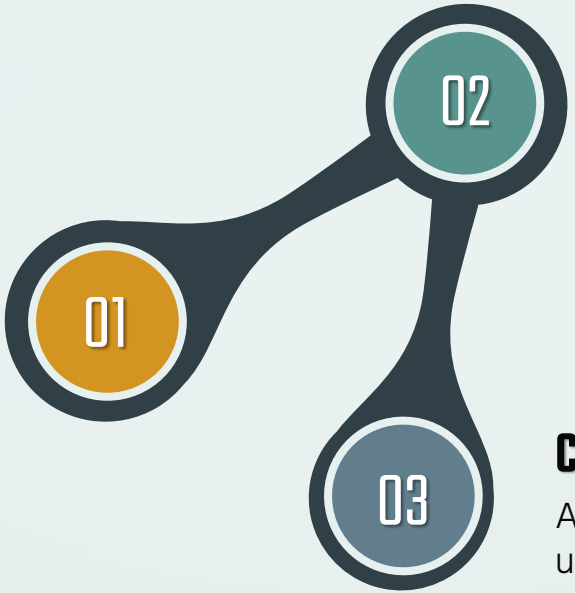
MÉTODO DE CRIPTOGRAFIA E DESCRIPTOGRAFIA



IMPACTOS DA CRIPTOGRAFIA

SEGURANÇA

A criptografia oferece uma camada de segurança para as comunicações interpessoais e entre as mais diversas organizações da sociedade



ANONIMATO

Mensagens criptografadas podem aumentar a sensação de anonimato, o que produz impactos positivos e negativos

CRIMINALIDADE

Algoritmos de criptografia podem ser utilizados a serviço de organizações criminosas, dificultando operações de rastreamento e identificação