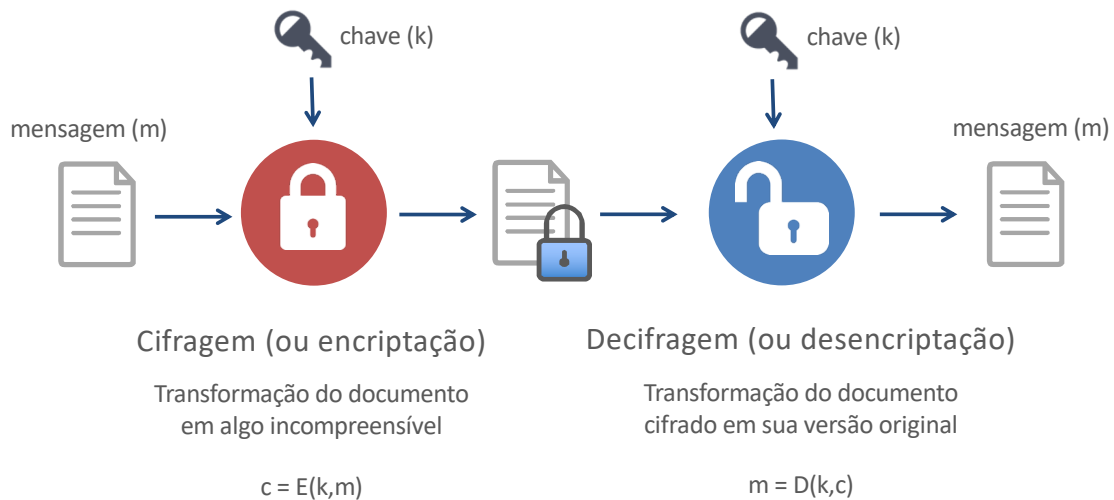


Criptografia

Do grego: *kryptós* (escondido) + *graphein* (escrita)



Aplicações da criptografia



Confidencialidade
Manter as informações privadas



Integridade
Garantir que os dados não foram alterados



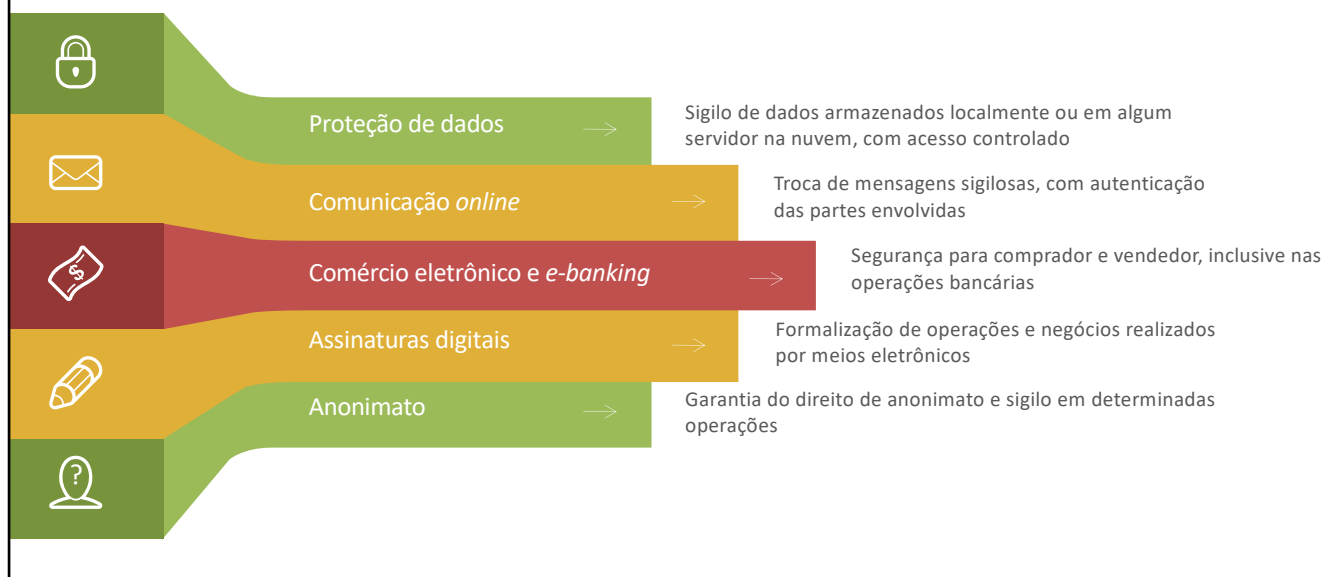
Autenticação
Estabelecer a identidade de um usuário ou sistema



Não-repúdio
Impedir que uma pessoa negue ter feito uma operação ou enviado uma mensagem

Os algoritmos criptográficos realizam uma ou mais operações, mas não todas. Assim, devem ser usados de forma combinada, se necessário.

Exemplos de aplicações



Cifragem

Cifragem é o processo de conversão de um texto claro para um código cifrado.

Decifragem é o processo contrário, de recuperar o texto original a partir de um texto cifrado.

Cifragem

A cifra de substituição é um método de criptografia no qual os símbolos (letras, grupos de letras, números, ...) são substituídas por outros símbolos.

A cifra de transposição é um método de criptografia em que os símbolos são trocados de posição com outros símbolos.