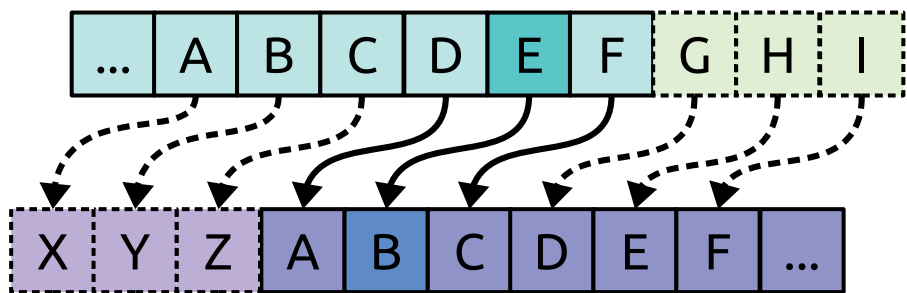


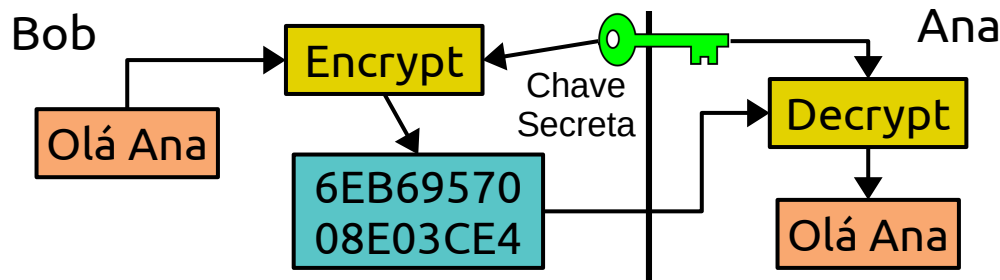
Criptografia (do grego antigo: κρυπτός, romanizado: kryptós "escondido, secreto"; e γράφειν, graphein, "escrever"), é a prática e o estudo de técnicas para comunicação segura na presença de comportamento adversário.

De maneira mais geral, a criptografia trata da construção e análise de protocolos que evitam que terceiros ou o público leiam mensagens privadas.



Acredita-se que as cifras de deslocamento do alfabeto tenham sido usadas por Júlio César há mais de 2000 anos. Este é um exemplo com $k = 3$. Em outras palavras, as letras do alfabeto são deslocadas três em uma direção para criptografar e três na outra direção para descriptografar.

Criptografia de chave simétrica, em que uma única chave é usada para criptografar e descriptografar.



Criptografia de chave pública, em que diferentes chaves são usadas para criptografar e descriptografar.

