O compartilhamento de informação é algo crucial para o desenvolvimento da humanidade, desse modo nós criamos diversas maneiras para compartilharmos informações de modo que não seja compreendida por pessoas indesejadas, um exemplo é a Usada pelos espartanos, consistia em enrolar uma tira de couro ou pergaminho em um bastão de madeira (a escítala). A mensagem era escrita na tira, mas só poderia ser lida corretamente quando enrolada em outro bastão do mesmo tamanho (ex da aula). Outro exemplo histórico importante é o uso dos mensageiros navajos na Segunda Guerra Mundial. Os Estados Unidos recrutaram falantes da língua navajo para transmitir mensagens militares, já que era um idioma desconhecido, fora da comunidade indígena então era praticamente impossível de decifrar pelos inimigos.

Nos dias de hoje, a criptografia evoluiu bastante e é aplicada em diferentes áreas da tecnologia. Entre os algoritmos de chave simétrica, podemos citar o Blowfish, conhecido por sua velocidade e bastante usado em softwares de segurança e aplicações de rede, e o Twofish, sucessor do Blowfish, considerado ainda mais seguro e eficiente.

Já na criptografia de chave assimétrica, além dos mais conhecidos, existem o ECC (Elliptic Curve Cryptography) que é baseado em propriedades matemáticas de curvas elípticas ela oferece o mesmo nível de segurança que o RSA, mas com chaves menores, tornando-o mais eficiente. E também a Multivariate Quadratic cryptographi que usa sistemas de equações quadráticas sobre corpos finos, usados mais para assinaturas digitais.