Dois exemplos históricos do uso de criptografia

a) Escítala Espartana – Grécia Antiga (cerca de 500 a.C.)
Os espartanos utilizavam um bastão de madeira chamado escítala para enviar mensagens secretas.
A mensagem era escrita em uma tira de couro ou tecido enrolada ao redor do bastão.
Quando desenrolada, ficava embaralhada e ilegível.
Somente quem tivesse um bastão de mesmo diâmetro conseguiria decifrar o conteúdo.
Esse método utilizava a técnica de transposição, rearranjando as letras do texto.

b) Telegrama Zimmermann – Primeira Guerra Mundial (1917)
A Alemanha utilizava códigos criptografados para estabelecer comunicações militares e diplomáticas.
O famoso Telegrama Zimmermann foi interceptado e decifrado pelos britânicos, revelando uma tentativa de aliança com o México contra os Estados Unidos.
A quebra dessa criptografia influenciou decisivamente a entrada dos EUA na guerra, mostrando a importância estratégica da criptoanálise.

2 Dois algoritmos de criptografia com chaves simétricas usados atualmente

a) AES – Advanced Encryption Standard
É o algoritmo mais utilizado no mundo atualmente.
É rápido, seguro e usado em sistemas financeiros, redes Wi-Fi (WPA2 e WPA3), VPNs, dispositivos móveis e governos.

b) 3DES – Triple Data Encryption Standard
Evolução do antigo DES.
Ainda presente em sistemas financeiros e bancários legados.
Utiliza três rodadas de criptografia para aumentar a segurança.

3 Dois algoritmos de criptografia com chaves assimétricas usados atualmente

a) RSA – Rivest, Shamir e Adleman
Usado em certificados digitais, HTTPS, assinaturas digitais e proteção de dados na Internet.
Baseia-se na dificuldade de fatorar grandes números primos.

b) ECC – Elliptic Curve Cryptography (Criptografia de Curvas Elípticas)
Oferece maior segurança com tamanhos de chave menores que o RSA, sendo muito eficiente.
É amplamente usado em dispositivos móveis, IoT e aplicativos como WhatsApp e Signal.