# Criptografia

# 1. Dois exemplos históricos do uso de criptografia

1. Cifra de Vigenère (século XVI)  
- Desenvolvida por Blaise de Vigenère na França.  
- Usa uma série de cifras de César com base em uma palavra-chave, criando um texto cifrado polialfabético.  
- Considerada por muito tempo “indecifrável” até ser quebrada no século XIX.  
- Esse método foi usado por diplomatas e exércitos para transmitir mensagens confidenciais.  
  
2. Códigos Navais Japoneses na Segunda Guerra Mundial (J.N.-25)  
- O Japão usava um complexo sistema de cifras chamado J.N.-25 para comunicações navais e militares.  
- Era baseado em um código de números substituídos e complementado por cifras adicionais.  
- Quebrado pela equipe americana em Pearl Harbor, contribuindo para a vitória na Batalha de Midway.  
- Esse episódio foi fundamental para mostrar a importância da criptografia na guerra moderna.

# 2. Dois algoritmos de criptografia com chaves simétricas (atuais)

- AES (Advanced Encryption Standard):  
 \* Substituiu o DES (Data Encryption Standard) como padrão do governo dos EUA.  
 \* Utiliza tamanhos de chave de 128, 192 ou 256 bits.  
 \* Usado amplamente em VPNs, HTTPS, discos criptografados, comunicações móveis e aplicativos bancários.  
 \* Considerado seguro até hoje quando implementado corretamente.  
  
- ChaCha20:  
 \* Algoritmo moderno de fluxo, rápido e seguro, muito usado em comunicações móveis e em TLS.  
 \* Desenvolvido como alternativa ao RC4 e ao AES em dispositivos com menos poder computacional.  
 \* Utiliza um contador e uma chave para gerar um fluxo de bits pseudoaleatórios.  
 \* Amplamente empregado em aplicativos como Google Chrome e WhatsApp para segurança de tráfego.

# 3. Dois algoritmos de criptografia com chaves assimétricas (atuais)

- RSA (Rivest–Shamir–Adleman):  
 \* Desenvolvido em 1977 pelos criptógrafos Ron Rivest, Adi Shamir e Leonard Adleman.  
 \* Baseia-se na dificuldade de fatorar grandes números primos.  
 \* Um dos sistemas assimétricos mais usados para troca de chaves, assinaturas digitais e certificados SSL/TLS.  
 \* Ainda amplamente empregado, embora recomenda-se usar chaves grandes (2048 bits ou mais).  
  
- ECC (Elliptic Curve Cryptography):  
 \* Criptografia de curvas elípticas; mais eficiente e segura com chaves menores (ex.: Ed25519).  
 \* Baseia-se em propriedades matemáticas de pontos sobre curvas elípticas.  
 \* Usada em sistemas modernos como Bitcoin, sistemas móveis e certificados digitais.  
 \* Oferece alta segurança com menor consumo de recursos, ideal para dispositivos móveis e IoT.

# Conclusão

A criptografia evoluiu ao longo dos séculos, passando de técnicas manuais simples a sistemas matemáticos altamente sofisticados.  
Hoje, tanto algoritmos simétricos como assimétricos são fundamentais para garantir a segurança digital, protegendo dados pessoais, transações financeiras e comunicações sigilosas.  
O entendimento desses conceitos é essencial para qualquer profissional que atue na área de tecnologia e segurança da informação..