**Atividade: Criptografia – Exemplos Históricos e Algoritmos Atuais**

**1. Dois Exemplos Históricos do Uso da Criptografia**

**a) Escítala Espartana (Grécia Antiga – cerca de 500 a.C.)**  
A escítala era um instrumento usado por espartanos para enviar mensagens criptografadas. Consistia em um bastão de madeira onde uma faixa de couro ou papiro era enrolada. A mensagem era escrita ao longo do bastão. Quando desenrolada, ela parecia um texto sem sentido. Apenas quem tivesse um bastão do mesmo diâmetro poderia enrolar a faixa e ler a mensagem corretamente.

**b) Código Navajo (Segunda Guerra Mundial)**  
Durante a Segunda Guerra Mundial, os Estados Unidos utilizaram membros da tribo navajo como “code talkers”. Eles falavam em navajo para transmitir mensagens militares, utilizando ainda codificações internas na língua. O idioma navajo não era escrito nem conhecido pelos inimigos, o que o tornou um método de criptografia altamente eficaz e impossível de ser decifrado na época.

**2. Dois Algoritmos de Criptografia com Chaves Simétricas Utilizados Atualmente**

**a) AES (Advanced Encryption Standard)**  
É o algoritmo de criptografia simétrica mais utilizado atualmente. Foi adotado pelo governo dos EUA e é amplamente usado para proteger dados em aplicações comerciais e governamentais.

**b) Blowfish**  
É um algoritmo de chave simétrica projetado para substituir o DES. Ele é rápido, seguro e de domínio público, sendo utilizado em diversos sistemas e aplicações de software.

**3. Dois Algoritmos de Criptografia com Chaves Assimétricas Utilizados Atualmente**

**a) RSA (Rivest–Shamir–Adleman)**  
É um dos algoritmos assimétricos mais conhecidos e utilizados. Baseia-se na dificuldade de fatoração de números primos grandes e é utilizado em sistemas de troca de chaves, assinaturas digitais e criptografia de dados.

**b) ECC (Elliptic Curve Cryptography)**  
Utiliza curvas elípticas para gerar chaves mais curtas com a mesma segurança que RSA, tornando-o ideal para dispositivos com recursos limitados. É bastante usado em aplicações móveis, IoT e criptomoedas.