Proteção de Dados

### **Exemplo 1: Códigos Navais dos EUA na Guerra do Pacífico (1942–1945)**

Durante a Segunda Guerra Mundial, os EUA usaram o famoso **“Código Navajo”**, baseado na língua indígena dos navajos.

* Esse sistema foi crucial nas batalhas contra o Japão, já que era praticamente impossível para os inimigos decifrarem rapidamente.
* A rapidez e a complexidade linguística ajudaram os EUA a manter a vantagem estratégica.
* Esse exemplo é marcante porque mostra como **a língua humana pode ser usada como forma de criptografia**.

### **Exemplo 2: Escítala Espartana (Grécia Antiga, séc. V a.C.)**

Os espartanos utilizavam a **escítala**, um bastão de madeira em que se enrolava uma tira de couro ou pergaminho.

* A mensagem era escrita ao longo do bastão; ao desenrolar, parecia apenas um monte de letras embaralhadas.
* Para ler corretamente, o destinatário precisava ter um bastão do mesmo diâmetro.
* Foi uma das primeiras formas conhecidas de **criptografia de transposição**.

Algoritmos de Criptografia com Chaves Simétricas (mesma chave para cifrar e decifrar):

1- **RSA (Rivest–Shamir–Adleman)**

* Amplamente utilizado em assinaturas digitais, certificados SSL/TLS (navegação segura) e autenticação.
* Baseado na dificuldade de fatorar números primos grandes.
* 2-**ECC (Elliptic Curve Cryptography)**
* Usa propriedades matemáticas de curvas elípticas.
* Mais seguro e leve que o RSA, ideal para dispositivos móveis, IoT e conexões modernas (TLS/HTTPS).

Integrantes

Rodolfo Regis de Souza – RA 825113514

Sergio Rycbzak Junior – RA 825154823

Pietro Oliveira Silva – RA 825113483

Gabriel Souza Santos – RA 825113168