**Criptografia**

Enigma- Criada durante a segunda guerra mundial, para enviar mensagens codificadas.

* A máquina enigma ultilizava uma série de rotores para alterar as letras de uma mensagem de maneiras complexas. (Alemanha nazista que usou).

Scytale- Vem da Grécia antiga, usada pelos militares espartanos, para enviar mensagem codificadas.

* É uma forma de cifra que consiste em um bastão (geralmente de madeira) e uma tira de pergaminho ou couro. A tira de pergaminho era enrolado ao redor do bastão e a mensagem era escrita ao longo do bastão, de modo que só seria legível quando o pergaminho fosse novamente enrolado no mesmo bastão.

**Chaves Simétricas**

RC4- É um algoritmo de cifra de fluxo simétrica, utilizado em protocolos como SSL/TLS e WEP. Ele usa uma chave de comprimento variável e gera um fluxo de chave para criptografar dados. Embora seja rápido e simples, suas vulnerabilidades de segurança resultam em sua descontinuação em favor de algoritmos mais seguros, como o AES.

Blowfish- É um algoritmo de criptografia simétrica. Sua chave de comprimento variável (32 a 448 bites) e foi uma alternativa ao DES. É usado em aplicações que exigem criptografia rápida e leve.

**Chave Assimétrica**

Kyber- é um algoritmo de criptografia baseado em redes, projetado para ser seguro contra ataques de computadores quânticos. Ele é um dos candidatos da criptografia pós-quântica, com o objetivo de proteger dados em um cenário onde os computadores quânticos possam quebrar algoritmos tradicionais como RSA e ECC. Ele é usado principalmente para troca segura de chaves, ajudando na geração e distribuição de chaves secretas mesmo frente a ataques quânticos, sendo eficiente e seguro para os desafios computacionais futuros.

Paillier- Um sistema de criptografia assimétrica baseado em teoria de números que é particularmente útil em cenários onde a operação de adição de valores criptografados (homomorfismo) é importante. Ele permite fazer operações de soma em dados criptografados sem precisar descriptografá-los.