**UNIVERSIDADE SÃO JUDAS**

**CIÊNCIA DA COMPUTAÇÃO**

Felipe Cadena

**SISTEMAS COMPUTACIONAIS E SEGURANÇA**

**Proteção de dados**

**SÃO PAULO**

**2025**

Interface gráfica do usuário

O conteúdo gerado por IA pode estar incorreto.

**Criptografia:** É a técnica de transformar informações em códigos para protegê-las contra acessos não autorizados. Ela usa algoritmos para embaralhar os dados, tornando-os ilegíveis sem uma chave de descriptografia.

**1° Camellia:**

A Camellia foi desenvolvida no final dos anos 1990 pela NTT (Nippon Telegraph and Telephone Corporation) e Mitsubishi Electric como uma alternativa forte ao AES. Ela foi projetada para ser altamente segura e eficiente tanto em hardware quanto em software.

Ele opera em blocos de 128 bits, com chaves de 128, 192 ou 256 bits, sendo comparável ao AES em segurança e desempenho.

**Características principais:**

Forte resistência contra-ataques criptoanalíticos

Eficiente para **hardware** e **software**

Usado em segurança de redes, armazenamento e comunicação segura

Camellia foi padronizado por organizações como a ISO/IEC e está presente em protocolos como TLS e OpenSSL.

* **Criptografia Simétrica** – Usa a mesma chave para criptografar e descriptografar.
* **Tamanhos de chave** – Suporta **128, 192 e 256 bits**.
* **Estrutura Feistel Modificada** – Baseado em uma rede Feistel com 18 rodadas (para 128 bits) ou 24 rodadas (para 192/256 bits).
* **Alta Segurança** – Projetado para resistir a ataques criptográficos conhecidos.
* **Eficiência** – Desempenho otimizado para software e hardware, sendo usado em dispositivos embarcados.
* **Padronização** – Reconhecido por organizações como a **ISO/IEC e a CRYPTREC**.

**2º TWOFISH**

O Twofish é um algoritmo de criptografia simétrica desenvolvido por Bruce Schneier e sua equipe na Counterpane Labs em 1998. Ele foi projetado como um sucessor do Blowfish e participou da competição para escolher o AES (Advanced Encryption Standard).

* **Chave Simétrica** – Usa a mesma chave para criptografia e descriptografia.  
   Suporta chaves de **128, 192 e 256 bits**.
* **Estrutura Feistel Modificada** – Baseado em uma rede de Feistel com 16 rodadas.
* **Velocidade** – Eficiência considerável tanto em software quanto em hardware.
* **Segurança Alta** – Nenhum ataque prático conhecido que quebre sua segurança.
* **Uso de S-Boxes Dinâmicas** – Personalizadas com base na chave, dificultando ataques.
* **Matriz MDS (Maximum Distance Separable)** – Maximiza a difusão dos bits.
* **Cadeias de Chaves Rápidas** – Possui um processo eficiente de expansão de chaves.

**2 algoritmos de Criptografia com Chaves Assimétricas utilizados**

**1º** **Cramer–Shoup** é um **criptossistema de chave pública (assimétrico)** que oferece **segurança contra-ataques de texto-cifrado escolhido adaptável** (IND-CCA2), um nível de segurança mais forte do que o RSA tradicional.

Ele foi desenvolvido por **Ronald Cramer** e **Victor Shoup** em **1998** como uma melhoria sobre o ElGamal.

**2º O criptosistema McEliece** é um dos primeiros esquemas de criptografia de chave pública, proposto por Robert McEliece em 1978. Ele se baseia na teoria de códigos de correção de erros e é considerado um dos poucos algoritmos seguros contra ataques de computadores quânticos, tornando-se uma alternativa viável ao RSA e ECC para o futuro.