UNIVERSIDADE SÃO JUDAS TADEU
SISTEMAS DE INFORMAÇÃO

LARISSA OLIVEIRA DOS SANTOS

UC SISTEMAS COMPUTACIONAIS E SEGURANÇA

São Paulo
2025

ATIVIDADE SOBRE CRIPTOGRAFIA- UC SCS

- **Tipos históricos de criptografia:**

1- Cifra de Jefferson: Criada por Thomas Jefferson, se tratava de discos rotativos com alfabetos, usados para codificar mensagens. Era uma cifra de substituição e foi empregada por Jefferson durante a sua presidência e em momentos de guerra para proteger a comunicação confidencial.

2- Cifra de Enigma: Utilizada pela Alemanha na Segunda Guerra Mundial, foi uma das formas mais complexas de criptografia. A máquina Enigma usava rotores mecânicos para criar códigos extremamente difíceis de decifrar. Sua quebra pelos aliados foi essencial para mudar o rumo da guerra.

- **Algoritmos de Criptografia com Chaves Simétricas utilizados atualmente:**

1- AES (Advanced Encryption Standard): Um dos algoritmos mais utilizados atualmente para criptografia de dados, considerado seguro e eficiente. É amplamente utilizado em transações bancárias, armazenamento de dados e outras aplicações de segurança.

2- DES (Data Encryption Standard): Embora considerado ultrapassado devido ao seu tamanho de chave limitado, o DES foi amplamente utilizado no passado e ainda é encontrado em alguns sistemas legados.

- **Algoritmos de Criptografia com Chaves Assimétricas utilizados atualmente:**

1- RSA (Rivest-Shamir-Adleman): Um dos algoritmos de criptografia assimétrica mais conhecidos, amplamente usado em troca de chaves e assinaturas digitais.

2- ECC (Elliptic Curve Cryptography): Utiliza curvas elípticas para fornecer segurança com chaves menores, tornando-o eficiente para dispositivos com recursos limitados, como smartphones e dispositivos IoT.