**UNIVERSIDADE SÃO JUDAS TADEU – USJT**

**SISTEMAS COMPUTACIONAIS E SEGURANÇA**

Eduardo Cecilio Alves Santos – **RA:824224719**

Ian Bastos Leme de Moraes – **RA:825111187**

Kauan Camargo – **RA: 825141414**

Lucas Tosta Piola – **RA:825137169**

Victor Gonçalves Volpi **/ RA: 825117218**

Wagner Quispe Espinal – **RA:823154959**

**Segurança em Sistemas Computacionais**

" Criptografia: Exemplos Históricos e Aplicação de Chaves Simétricas e Assimétricas”

SÃO PAULO – SP

2025

### ****Criptografia: Evolução e Aplicações Modernas****

#### **Exemplos Históricos do Uso da Criptografia**

**Cifra de Atbash** – Usada na antiga Mesopotâmia, substituía cada letra da mensagem por sua equivalente invertida no alfabeto. Era um método simples, mas eficaz para ocultar informações.

**Os Papéis de Zimmerman** – Durante a Primeira Guerra Mundial, uma mensagem codificada enviada pela Alemanha ao México foi interceptada e decifrada pelos britânicos, influenciando a entrada dos EUA no conflito.

#### **Algoritmos de Criptografia com Chaves Simétricas**

**Twofish** – Evolução do Blowfish, oferece alta segurança e é utilizado em diversas aplicações, como sistemas de armazenamento e proteção de arquivos.

**RC4** – Algoritmo de fluxo usado em protocolos antigos como WEP e TLS, mas atualmente considerado inseguro devido a vulnerabilidades descobertas.

#### **Algoritmos de Criptografia com Chaves Assimétricas**

**DSA (Digital Signature Algorithm)** – Usado para gerar assinaturas digitais, garantindo a autenticidade e integridade de documentos eletrônicos.

**Post-Quantum Cryptography** – Conjunto de algoritmos em desenvolvimento para resistir a ataques de computadores quânticos, como o Kyber e Dilithium.

**Exemplos Históricos do Uso da Criptografia**

**Cifra de Atbash:**

Mensagem original: "SEGREDO"

Mensagem cifrada: "HVITWVW" (as letras são substituídas pela inversa no alfabeto: A↔Z, B↔Y, etc.)

**Os Papéis de Zimmerman:**

Durante a Primeira Guerra Mundial, o governo alemão enviou um telegrama secreto ao México propondo uma aliança contra os EUA. Os britânicos interceptaram e decodificaram a mensagem, influenciando a entrada dos EUA na guerra.

**Algoritmos de Criptografia com Chaves Simétricas:**

Twofish (Exemplo de uso em proteção de arquivos)

Arquivo: "relatorio.pdf"

Chave secreta: a9f8b7c6d5e4

Arquivo criptografado: "relatorio\_encrypted.pdf"

RC4 (Exemplo de uso em redes Wi-Fi antigas - WEP)

Uma rede Wi-Fi com criptografia WEP usava RC4 para proteger dados, mas ataques modernos conseguem quebrar essa proteção em minutos.

**Algoritmos de Criptografia com Chaves Assimétricas:**

DSA (Exemplo de assinatura digital de documentos)

Um usuário assina um contrato digitalmente com DSA, garantindo que o documento não foi alterado. Chave pública: Usada para verificar a assinatura.

Chave privada: Usada pelo remetente para assinar o documento.

Post-Quantum Cryptography (Proteção contra-ataques quânticos)

Bancos e governos estão testando algoritmos como Kyber e Dilithium para proteger dados contra futuros computadores quânticos, que podem quebrar criptografias atuais.

Eduardo Cecílio Alves Santos – **RA:824224719**

Ian Bastos Leme de Moraes – **RA:825111187**

Kauan Camargo – **RA: 825141414**

Lucas Tosta Piola – **RA:825137169**

Victor Gonçalves Volpi **/ RA: 825117218**

Wagner Quispe Espinal – **RA:823154959**

**Segurança em Sistemas Computacionais**

“Criptografia: Exemplos Históricos e Aplicação de Chaves Simétricas e Assimétricas”

Trabalho apresentado a Universidade São Judas Tadeu – USJT como requisito para conclusão do trabalho de Sistemas Computacionais e Segurança

Orientador: Prof. Robson Calvetti

SÃO PAULO - SP

2025