**HENRY GAVA SALVAIA - 825122158  
PEDRO HENRIQUE - 824224330  
KAMILLY - 82513794  
JOÃO PEDRO - 824222452**

### 

### **ATIVIDADE DE SISTEMAS COMPUTACIONAIS E SEGURANÇA**

Professor(a): [Robson Calvetti]  
 Data de Entrega: [03/04/2025]

### 

### **RESUMO**

Este trabalho apresenta uma análise sobre os principais sistemas de criptografia, abordando exemplos históricos e algoritmos modernos. O objetivo é compreender a evolução dos mecanismos de segurança e sua aplicação nos dias atuais.

### 

### **1. INTRODUÇÃO**

A segurança da informação é um aspecto essencial para a proteção de dados sigilosos. Ao longo da história, diversos métodos criptográficos foram desenvolvidos para garantir a confidencialidade das informações. Este trabalho analisa a evolução da criptografia, abordando desde os primeiros sistemas até os algoritmos modernos.

### 

### **2. EXEMPLOS HISTÓRICOS DO USO DA CRIPTOGRAFIA**

#### 

#### **2.1 Escítala Espartana**

#### **Os espartanos usavam um bastão chamado escítala para enviar mensagens secretas. Um pedaço de couro ou papiro era enrolado no bastão, e a mensagem era escrita. Quando desenrolado, parecia uma sequência aleatória de letras, sendo legível apenas ao ser enrolado em um bastão de mesmo diâmetro.**

#### 

#### **2.2 Código de Navajo**

Durante a Segunda Guerra Mundial, o exército dos EUA usou a língua dos nativos Navajos como um código para comunicações militares. Como a língua não tinha escrita formal e era desconhecida pelos inimigos, isso criou um sistema criptográfico altamente seguro.

Pontos-chave:

* Considerado um dos códigos mais seguros da história
* Criado por nativos americanos Navajo recrutados pelo exército
* Nunca foi decifrado pelos inimigos

### **3. ALGORITMOS DE CRIPTOGRAFIA COM CHAVES SIMÉTRICAS**

Os algoritmos simétricos utilizam a mesma chave para criptografar e descriptografar os dados, sendo mais rápidos e eficientes. No entanto, exigem que as partes compartilhem a chave de maneira segura.

#### 

#### **3.1 AES (Advanced Encryption Standard)**

O AES é um dos algoritmos mais utilizados atualmente para proteger dados sigilosos. Ele opera com chaves de 128, 192 ou 256 bits, garantindo alto nível de segurança.

**Usado em:**

* Transações bancárias online
* Wi-Fi seguro (WPA2)
* Proteção de arquivos e senhas

#### **3.2 Blowfish**

O Blowfish é um algoritmo simétrico desenvolvido para ser rápido e seguro, permitindo chaves de até 448 bits. É amplamente utilizado na proteção de dados sensíveis.

**Usado em:**

* Ferramentas de criptografia de senhas (bcrypt)
* Segurança de redes e VPNs

### **4. ALGORITMOS DE CRIPTOGRAFIA COM CHAVES ASSIMÉTRICAS**

Diferente da criptografia simétrica, a criptografia assimétrica utiliza um par de chaves:

* **Chave pública:** usada para criptografar a informação
* **Chave privada:** usada para descriptografar a informação

Isso aumenta a segurança e elimina a necessidade de compartilhar uma chave secreta.

#### **4.1 RSA (Rivest-Shamir-Adleman)**

O RSA é amplamente utilizado para assinaturas digitais e criptografia de dados. Sua segurança se baseia na dificuldade de fatorar números primos grandes.

**Usado em:**

* Certificados digitais (SSL/TLS)
* Assinaturas digitais
* Proteção de e-mails

#### **4.2 ECC (Elliptic Curve Cryptography)**

A criptografia de Curvas Elípticas (ECC) proporciona um nível de segurança semelhante ao RSA, mas com chaves menores, tornando-a mais eficiente.

**Usado em:**

* Criptografia para dispositivos móveis
* Blockchain e criptomoedas
* Certificados de segurança modernos

### **5. CONCLUSÃO**

A evolução da criptografia demonstra sua importância para a proteção de informações sensíveis. O uso de algoritmos modernos garante segurança e confiabilidade em diversas aplicações.