USJT – UC Sistemas Computacionais e Segurança – Prof. Calvetti - Atividade

NOME: Daniel Silva

ATIVIDADE:

Escolher 2 (dois) exemplos históricos do uso de criptografia não citados neste material; Citar 2 algoritmos de Criptografia com Chaves Simétricas utilizados atualmente; Citar 2 algoritmos de Criptografia com Chaves Assimétricas utilizados atualmente.

PESQUISA:

Exemplos Históricos do Uso de Criptografia

1 - Cítala Espartana (c. 650 a.C.): A cítala espartana consistia em enrolar uma fita de tecido em um bastão de madeira de dada largura. A frase a ser cifrada era escrita na fita no comprimento do bastão, desenrolada e enviada disfarçada (como um cinto por exemplo) e ao chegar ao destino deveria ser enrolada num bastão de mesma largura para que a mensagem fosse decifrada.

2 - Cifra Atbash: é uma criptografia de simples substituição do alfabeto hebraico. Ela consiste na substituição do aleph (a primeira letra) pela tav (a última), beth (a segunda) pela shin (a penúltima), e assim por diante, invertendo o alfabeto usual. Uma decodificação em Atbash para o alfabeto romano seria assim:

Normal: a b c d ... w x y z Código: Z Y X W ... D C B A

Algoritmos de Criptografia de Chave simétrica

1 - AES (Advanced Encryption Standard): É, sem dúvida, o padrão de criptografia simétrica mais usado e recomendado atualmente. Utiliza chaves de 128, 192 ou 256 bits.

2 - Serpent: Um algoritmo de cifra de bloco que também foi um dos finalistas do concurso AES. Utiliza chaves de 128, 192 ou 256 bits e foi projetado para ter uma margem de segurança muito alta.

3 - ChaCha20: Uma cifra de fluxo mais moderna, frequentemente usada em conjunto com o Poly1305 para autenticação (formando o modo **ChaCha20-Poly1305**). Ganhou popularidade como uma alternativa segura e eficiente para o RC4 em protocolos de internet (como TLS).

Algoritmos de Criptografia de Chave Assimétrica

1 - ECC (Elliptic Curve Cryptography): A Criptografia de Curva Elíptica, que usa a estrutura algébrica de curvas elípticas em campos finitos, é o principal concorrente do RSA e está se tornando o padrão preferido devido à sua eficiência. Utiliza chaves significativamente menores (ex: uma chave ECC de 256 bits oferece segurança comparável a um RSA de 3072 bits), tornando-o ideal para dispositivos móveis e ambientes de largura de banda limitada.

2 - Kyber (CRYSTALS-Kyber): Devido à ameaça potencial de computadores quânticos que poderiam quebrar RSA e ECC, essa cifra usa criptografia baseada em reticulados, um campo que emprega estruturas matemáticas complexas, com propriedades geométricas intrincadas que são difíceis de decifrar, até mesmo para computadores quânticos. Ela é altamente eficiente e consome poucos recursos, o que permite sua utilização até em aparelhos com capacidade computacional limitada, como dispositivos IoT, sistemas integrados ou sensores industriais.

BIBLIOGRAFIAS

MEDEIROS, Fávio. **Uma breve história sobre Criptografia**. Disponível em: <https://cryptoid.com.br/criptografia-identificacao-digital-id-biometria/a-historia-da-criptografia/>. Acesso em: 29 set. 2025.

WIKIPEDIA. **Atbash**. Disponível em: <https://pt.wikipedia.org/wiki/Atbash>. Acesso em: 29 set. 2025.

SANTOS, Vitor. **Entendendo o CRYSTALS-Kyber: a resposta à ameaça quântica na segurança digital**. Disponível em: <https://www.protiviti.com.br/cybersecurity/entendendo-o-crystals-kyber/#:~:text=O%20Kyber%20opera%20em%20tr%C3%AAs,chave%20privada%20%C3%A9%20mantida%20confidencialmente.> Acesso em: 29 set. 2025.

DIGICERT. **O que é criptografia de curva elíptica?**. Disponível em: <https://www.digicert.com/pt/faq/cryptography/what-is-elliptic-curve-cryptography#:~:text=O%20que%20%C3%A9%20criptografia%20de%20curva%20el%C3%ADptica%20(ECC)%3F,um%20ponto%20base%20publicamente%20conhecido.>. Acesso em: 29 set. 2025.

ALVES, Josias. **Protocolos Criptográficos Simétricos e Assimétricos: Uma Visão Geral dos Principais Algoritmos**. Disponível em: <https://blog.grancursosonline.com.br/protocolos-criptograficos-simetricos-e-assimetricos-uma-visao-geral-dos-principais-algoritmos/>. Acesso em: 29 set. 2025.