FCT – FACULDADE DE CIÊNCIAS E TECNOLOGIA

DMC – DEPARTAMENTO DE MATEMÁTICA E COMPUTAÇÃO

BACHARELADO EM CIÊNCIA DA COMPUTAÇÃO

JUAN CARDOSO DA SILVA - 171257138

GUILHERME DE AGUIAR PACIANOTTO - 181251019

**MATÉRIA SEGURANÇA DA INFORMAÇÃO**

ATIVIDADE 5



**Presidente Prudente, 25/08/2022**

# **INTRODUÇÃO**

Diffie-Hellman foi uma muito bem recebido depois de seu desenvolvimento em 1976 na história de toda criptografia, introduzindo o conceito de *“one way trap door”* como método de compartilhamento de chaves de segurança para ambas as partes envolvidas, sem necessidade de compartilhar o segredo final de ambas as partes.  
Esse algoritmo pode ser considerado como o início da criptografia moderna, depois de sua criação, deu espaço para introdução de muitos outros algoritmos criados, inclusive o RSA, criado dois anos depois da introdução do artigo científico original do Diffie-Hellman.

Apersar de tudo, o Diffie-Hellman apresenta limitações e o seu uso original foi descartado para aceitar outras variantes como DHL(Diffie-Hellman Logarithm Problem), ou DDH(Dicision Diffie-Hellman problem).

Neste artigo foi desenvolvido para entender o algoritmo original e as suas utilidades de aplicações modernas, sendo ele um dos algoritmos bases para toda área de criptografia.

# **FUNCIONAMENTO DO ALGORITMO**

Na área da criptografia, Diffie-Hellman (DH), é utilizado como um método de compartilhamento de chaves, onde uma chave intermediária calculada e trocada entre as pessoas utilizando o algoritmo, cada pessoa calcula depois suas respectivas chaves públicas utilizando a chave intermediária pega.

Com isso é possível calcular a chave final sem a necessidades de trocar elas e arriscar comprometer a segurança dos sistemas envolvidos.

# **UTILIZAÇÕES DO ALGORITMO**

O algoritmo de Diffie-Hellman teve muitas utilidades após sua publicação original, não só contribuiu para geração de algoritmos de criptografia como RSA, como também é utilizado na validação de servidores, proteger chaves privadas em serviços utilizados na internet.

**CONCLUSÃO**

O algoritmo de Diffie-Hellman foi uma marca muito grande na área da criptografia, levando a construção de outros algoritmos e a criação da criptografia moderna e atual, como também o algoritmo é importante para validações e comunicações na rede.

# **REFERENCIAS BIBLIOGRÁFICAS**

[Ueli M. Maurer](https://link.springer.com/article/10.1023/A:1008302122286#auth-Ueli_M_-Maurer); [Stefan Wolf](https://link.springer.com/article/10.1023/A:1008302122286#auth-Stefan-Wolf); **The Diffie-Hellman Protocol**, 2000, p. 1-25 Disponível em: < https://link.springer.com/article/10.1023/A:1008302122286>

THE INTERNET SOCIETY (1999). rfc-editor, 1999. **Diffie-Hellman Key Agreement Method**. Disponível em: < https://www.rfc-editor.org/rfc/rfc2631.html>

Cridland, Dave; **Crypto Show And Tell: The Wonders of Diffie-Hellman-Merkle**, 2018, Disponível em: < <https://dev.to/dwd/crypto-show-and-tell-the-wonders-of-diffie-hellman-merkle-2jah>>

Sampaio, Edsion; **Criptografia e Protocolo Diffie-Hellman**, 2018, Disponível em: < <https://dev.to/dwd/crypto-show-and-tell-the-wonders-of-diffie-hellman-merkle-2jah>>

Wang, Saji; **Basics of Encryption: The Diffie-Hellman key Exchange Explained**, 2022, Disponível em: <<https://dev.to/dwd/crypto-show-and-tell-the-wonders-of-diffie-hellman-merkle-2jah>>

OLIVEIRA, Carla Josefa Gonçalo de; **PROTOCOLO DIFFIE-HELLMAN**, p. 1-55, Disponível em: < <https://repositorio.ifpb.edu.br/handle/177683/1699>>