ANÁLISE COMPARATIVA DO DESEMPENHO DE ALGORITMOS CRIPTOGRÁFICOS ASSIMÉTRICOS EM AMBIENTES VIRTUALIZADOS: AVALIAÇÃO DO RSA *VERSUS* IMPLEMENTAÇÕES BASEADAS EM CURVAS ELÍPTICAS (APOIO UNIP)

Alunos: Kayky Crespo dos Santos e Caio Pacheco de Andrade
Orientador: Prof. Me. André Gomes de Lira Muniz
Curso: Ciência da Computação
***Campus*:** Marquês

A segurança da informação tornou-se um aspecto crítico na infraestrutura tecnológica moderna, com a criptografia assimétrica constituindo um pilar fundamental para proteção de dados sensíveis, autenticação digital e estabelecimento de comunicações seguras. Com o crescimento exponencial da virtualização em *data centers* e computação em nuvem, surge a necessidade crítica de compreender como algoritmos criptográficos se comportam em ambientes virtualizados, onde recursos computacionais são compartilhados e dinamicamente alocados. Esta pesquisa objetivou analisar sistematicamente o desempenho de três famílias principais de algoritmos criptográficos assimétricos: RSA (1024, 2048 e 4096 bits), Ed25519/X25519 baseado na Curve25519, e curvas NIST (P-256, P-384, P-521) em diferentes configurações de hardware virtualizado. A metodologia experimental compreendeu o desenvolvimento de um *framework* de *benchmark* especializado em Python, utilizando a biblioteca *cryptography* para avaliar operações fundamentais, como geração de chaves, assinatura, verificação e troca de chaves. Os experimentos foram conduzidos em máquinas virtuais Oracle VirtualBox com configurações controladas, variando em número de núcleos de CPU (2, 4 e 8) e memória disponível (0,5GB, 1,0GB e 2,0GB) e coletando métricas de tempo de execução, consumo de memória e utilização de CPU. Os resultados

evidenciaram superioridade categórica das implementações baseadas em curvas elípticas sobre o RSA em praticamente todas as métricas avaliadas. O Ed25519/X25519 demonstrou eficiência excepcional, sendo aproximadamente 250 vezes mais rápido que RSA 2048 bits para geração de chaves, com consumo significativamente menor de recursos computacionais. O RSA apresentou limitações substanciais em ambientes virtualizados, especialmente para chaves de maior tamanho, com degradação não linear do desempenho. Esta investigação fornece subsídios técnico-científicos e recomendações práticas para seleção otimizada de algoritmos criptográficos em diferentes contextos, contribuindo para o desenvolvimento de sistemas de segurança computacionalmente eficientes e escaláveis em infraestruturas virtualizadas.