

MÉTODOS DE CRIPTOGRAFIA EM APLICATIVOS DE MENSAGEM

Calebe dos Santos FARIAS*
Enzo Mateus Garbim LEZO**
Heitor André ZELBATO***
João Pedro Gianini FRANZIN****
Leonardo Capato Vieira LUIZ*****
Fernando PEDROSO*****
Elaine Doro Mardegan COSTA*****

RESUMO

Introdução: A criptografia em aplicativos de mensagens representa uma das principais ferramentas de proteção da privacidade e da segurança digital no cenário atual. Aplicativos como WhatsApp, Signal e Telegram utilizam protocolos de criptografia ponta a ponta. A coleta de dados, a vulnerabilidade a ataques cibernéticos e os avanços da computação quântica colocam em xeque a confiabilidade de métodos criptográficos tradicionais. A necessidade de algoritmos mais robustos e de práticas transparentes no tratamento de dados mostra-se cada vez mais urgente. **Objetivo:** O presente estudo tem como objetivo analisar a eficácia dos métodos de criptografia aplicados em aplicativos de mensagens mais utilizados no mundo e verificar sua importância na proteção da privacidade, na confiabilidade junto aos usuários e na resistência frente às ameaças tecnológicas emergentes. **Metodologia:** Trata-se de uma pesquisa exploratória e descritiva, com abordagem qualitativa, fundamentada em revisão bibliográfica. Foram consultados artigos técnicos, relatórios acadêmicos e materiais especializados, além da análise de protocolos de criptografia, como o Signal Protocol, para compreender seus mecanismos, pontos fortes e limitações. **Resultados:** A análise revelou que, embora protocolos como o Signal se destaquem pela segurança, ainda existem vulnerabilidades ligadas ao armazenamento de métodos, que podem expor informações sensíveis. O Telegram, por meio do MTPProto e dos chats secretos, mostrou alternativas que conciliam velocidade e proteção, mas especialistas afirmam que nenhum aplicativo pode ser considerado totalmente invulnerável. Além disso, a Lei Geral de Proteção de Dados (LGPD) reforça a necessidade de transparência e responsabilidade no uso das informações, tornando a criptografia uma aliada indispensável, mas não suficiente por si só. **Conclusão:** Conclui-se que a criptografia em aplicativos de mensagens é fundamental para garantir a privacidade digital, mas exige constante atualização, monitoramento e integração com políticas de proteção de dados.

Palavras-chave: métodos; criptografia; aplicativos de mensagens; proteção de dados.

* Discente de Tecnologia em ADS do Centro Universitário de Santa Fé do Sul, SP – Unifunec. calebesantofarias@gmail.com

** Discente de Tecnologia em ADS do Centro Universitário de Santa Fé do Sul, SP – Unifunec. enzomasky@gmail.com

*** Discente de Tecnologia em ADS do Centro Universitário de Santa Fé do Sul, SP – Unifunec. heitorzelbato@gmail.com

**** Discente de Tecnologia em ADS do Centro Universitário de Santa Fé do Sul, SP – Unifunec. joaopedrogianinifranzin@gmail.com

***** Discente de Tecnologia em ADS do Centro Universitário de Santa Fé do Sul, SP – Unifunec. Leonardocapato15@gmail.com

***** Docente do Centro Universitário de Santa Fé do Sul, SP – Unifunec. fernando.pedroso2@etec.sp.gov.br

***** Orientadora, Mestre, Docente do Centro Universitário de Santa Fé do Sul, SP – Unifunec. elamardegan@hotmail.com