BIO Web of Conferences **97**, 00093 (2024) https://doi.org/10.1051/bioconf/20249700093
ISCKU 2024

Comparing two cryptographic hash algorithms: sha-512 and whirlpool- a case study on file integrity monitoring

Farah Al-Shareefi[1]* *and Zahraa* Al-Barmani[2]
[1,2]Computer Science Department Babylon University, Hilla, Iraq

Abstract. SHA-512 and Whirlpool are two distinct hashing algorithms in the cryptography domain. Although they are different, these methods share some characteristics; such as both of them produce secure digests of the same size. In addition, being increasingly used for sustaining the integrity of confidential files. As a result, it is crucial to explore a method to contrast and compare their performance. This paper presents a comparative analysis of SHA-512 and Whirlpool, in terms of: time consumption, avalanche effect, and resistance to collision. It also investigates their suitability in the context of File Integrity Monitoring. Our results reveal that Whirlpool outperforms SHA-512 in the avalanche effect scenario, whereas a comparable resistance to the collision behavior is exhibited. Regarding time consumption, it is slower than SHA-512. However, this positively reflects its resistance to brute force attacks.