ABSTRACT

Password security is an important aspect in maintaining data integrity and privacy. Strong passwords are generally formed from a mixture of characters, numbers and symbols. Most users find it difficult to remember passwords that are formed from a mixture of characters, numbers and symbols. A password phrase is a password formed from a combination of several words, so it tends to be easier to remember. Diceware is one of the algorithms used in creating passphrases. However, the level of memorability and strength of the passphrase generated by the Diceware algorithm is not yet known. The aim of this research is to measure the memorability and password strength of passphrases generated by the Diceware algorithm. Memorability is measured using the Jaro Winkler Distance algorithm approach and password strength using the password strength library tool. The results of the 3-word passphrase produced by the Diceware Algorithm show the level of memorability through the Jaro Winkler Distance Algorithm approach, getting an average value of 39.47% and the level of strength (Password Strength) is in the medium category. This research succeeded in creating a passphrase generator using the Diceware algorithm and implementing memorability measurements using the Jaro Winkler Distance Algorithm and password strength.

***Keys**: Diceware, Jaro Winkler Distance, Memorability, Password Strength*