

## ABSTRAK

Keamanan kata sandi merupakan aspek penting dalam menjaga integritas dan priviasi data. Kata sandi (*password*) yang kuat umumnya dibentuk dari campuran karakter, angka, serta simbol. Kebanyakan pengguna sulit untuk mengingat *password* yang dibentuk dari campuran karakter, angka, serta simbol. *Password phrase (passphrase)* merupakan *password* yang dibentuk dari gabungan beberapa kata, sehingga cenderung lebih mudah diingat. *Diceware* merupakan salah satu algoritma yang digunakan dalam pembuatan *passphrase*. Namun belum diketahui tingkat kemudahan diingat (*memorability*) dan tingkat kekuatan (*strength*) dari *passphrase* yang dihasilkan oleh algoritma *Diceware* ini. Tujuan dari penelitian ini, melakukan pengukuran *memorability* dan *password strength* dari *passphrase* yang dihasilkan oleh algoritma *Diceware*. *Memorability* diukur dengan menggunakan pendekatan algoritma *Jaro Winkler Distance* dan kekuatan *password* menggunakan tools *library password strength*. Hasil *passphrase* dengan 3 kata yang dihasilkan Algoritma *Diceware* menunjukkan tingkat kemudahan diingat (*memorability*) melalui pendekatan Algoritma *Jaro Winkler Distance* mendapatkan nilai rata-rata 39,47% dan tingkat kekuatan (*Password Strength*) berada pada kategori *medium*. Penelitian ini berhasil menciptakan *generator passphrase* menggunakan algoritma *Diceware* serta mengimplementasikan pengukuran tingkat kemudahan diingat (*memorability*) dengan Algoritma *Jaro Winkler Distance* dan kekuatan kata sandi (*password strength*).

**Kata kunci :** *Diceware, Jaro Winkler Distance, Memorability, Password Strength*