ABSTRAK

Penelitian ini bertujuan untuk meningkatkan keamanan kata sandi dengan menerapkan prehash menggunakan fungsi hash SHA-512 pada algoritma Bcrypt. Penelitian diuji pada dua kategori kata sandi, yaitu yang kurang dari 72 karakter dan yang lebih dari 72 karakter, dengan fokus pada dua jenis serangan, yakni combinatory attack dan dictionary attack. Hasil penelitian menunjukkan bahwa penerapan prehash dengan menggunakan SHA-512 pada Bcrypt mampu mengatasi kedua jenis serangan tersebut.

Selain itu, penelitian ini juga menyoroti bahwa memperpanjang jumlah karakter pada kata sandi dapat memperlambat kecepatan hash yang dibutuhkan untuk memecahkan kata sandi sebanyak 1%. Hal ini menunjukkan bahwa memperpanjang panjang kata sandi adalah strategi efektif untuk meningkatkan keamanan sistem dalam menghadapi serangan brute force.

Hasil eksperimen ini memberikan wawasan berharga dalam pengembangan strategi keamanan kata sandi dan memberikan kontribusi positif dalam upaya melindungi data sensitif dari potensi serangan. Penelitian ini menegaskan bahwa menggabungkan prehash SHA-512 dengan algoritma Bcrypt adalah pendekatan yang kuat dalam meningkatkan keamanan sistem autentikasi.

Kata kunci : ***prehash, SHA-512, Bcrypt, Serangan Kamus, Serangan Kombinatorik***