

## DAFTAR GAMBAR

2.1	Perbandingan Ukuran Kunci Publik pada Kriptografi Asimetrik. . . . .	7
2.2	Grafik Kurva Elips. . . . .	8
2.3	Pertukaran kunci ECDH [1]. . . . .	9
2.4	Goa Ali Baba. . . . .	12
3.1	Alur penelitian. . . . .	14
3.2	Skema erancangan autentikasi ECC berbasis <i>Fiat-Shamir</i> . . . . .	16
3.3	Skema perancangan autentikasi ECDH-HMAC. . . . .	17
4.1	Grafik rata-rata waktu komputasi algoritma autentikasi. . . . .	21
4.2	Grafik rata-rata waktu komputasi algoritma autentikasi. . . . .	22
4.3	Grafik delay algoritma ECC berbasis <i>Fiat-Shamir</i> . . . . .	24
4.4	Grafik delay algoritma ECDH-HMAC. . . . .	24
4.5	Grafik rata-rata <i>delay</i> algoritma autentikasi. . . . .	24
4.6	Grafik rata-rata <i>delay</i> algoritma autentikasi. . . . .	26
4.7	Grafik penggunaan memori algoritma ECC berbasis <i>Fiat-Shamir</i> . . . . .	27
4.8	Grafik penggunaan memori algoritma ECDH-HMAC. . . . .	28
4.9	Grafik rata-rata penggunaan memori algoritma autentikasi. . . . .	29
4.10	Grafik rata-rata penggunaan memori algoritma autentikasi. . . . .	30
4.11	Grafik rata-rata <i>communication cost</i> pada algoritma autentikasi. . . . .	31
4.12	Grafik rata-rata <i>communication cost</i> pada algoritma autentikasi. . . . .	32