# Abstraksi

Metoda kriptografi yang dipakai untuk penyandian suara pada sistem telepon seluler GSM (*Global System for Mobile Communication*) adalah dengan menggunakan algoritma kriptografi A5. Algoritma A5 merupakan jenis algoritma simetri dimana kunci yang dipakai untuk proses enkripsi dan dekripsi sama. Algoritma A5 dibagi menjadi A5/1, A5/2, dan Versi terbarunya yaitu A5/3.

Pada tugas akhir ini disimulasikan dan dinalisis algoritma kriptografi A5/2 untuk membuktikan kemampuan dari system kriptografi algoritma A5 tersebut, dengan cara menganalisa tingkat distribusi keacakan atau presentase perubahan bitnya, lama dan performansi proses, dan avalanche effect. Untuk hasil avalanche effect ini akan akan dibandingkan dengan hasil avalanche efect pada algoritma A5 dengan ECC ECC (Elliptic Curve Cryptography).

**Kata kunci** : *Cryptography, GSM (Global System for Mobile Communications, A5, A5/2, A5 with ECC, Avalanche effect.*

**Hypotesis :** Sistem keamanan GSM menggunakan kriptografi algoritma A5/2 merupakan versi lemah dari algoritma A5 yang disebabkan struktur internal algoritma tidak kompleks, dan Algoritma A5 dengan ECC merupakan algoritma yang digunakan untuk mengatasi kelemahan tesrebut.