

**SIMULASI SISTEM KEAMANAN JARINGAN  
GSM KHUSUSNYA PADA AUC (AUTHENTICATION CENTER) DENGAN  
MENGUNAKAN VISUAL BASIC 6.0**

**TUGAS AKHIR**

**Diajukan sebagai salah satu syarat  
untuk memperoleh gelar Ahli Madya**

**Oleh**

**LENI FARIANI  
BP: 05 085 041**

**Program Studi Teknik Telekomunikasi  
Jurusan Teknik Elektro**



**POLITEKNIK UNIVERSITAS ANDALAS PADANG  
2008**

## ABSTRAK

Industri Mobile Telecommunication sedang mengalami peningkatan yang pesat dengan bertambahnya jumlah services yang ditawarkan oleh sejumlah network operator dan service provider, yang menyebabkan bertambahnya jumlah pengguna telepon cellular. Sejumlah teknologi baru bermunculan, namun menimbulkan masalah baru dalam hal *security* atau keamanan.

Tugas Akhir ini menjelaskan mengenai mekanisme pengamanan jaringan GSM. Mencakup prosedur- prosedur yang dilakukan untuk pengamanan komunikasi menggunakan jaringan GSM, beserta algoritma yang diterapkan untuk masing – masing prosedur yaitu algoritma A3, A5, dan A8.

Ada beberapa prosedur yang dilakukan dalam pengamanan GSM, mulai dari otentikasi *Personal Identification Number (PIN)*, otentikasi *Mobile Station* oleh jaringan, hingga pembangkitan kunci untuk mengenkripsi data yang ditransmisikan melalui jaringan GSM.

Kata kunci : GSM security, Autentikasi.

# BAB I

## PENDAHULUAN

### 1.1 Latar Belakang

Keamanan informasi dari berbagai macam gangguan merupakan persoalan utama baik pada jaringan kabel atau nirkabel. Keamanan system informasi mencakup keamanan jaringan, keamanan informasi dan *physic* atau peralatannya itu sendiri.

Sistim keamanan dibuat untuk mengatasi masalah *authentication*, *information integrity* dan *identification problem*. *Mobile telephone* atau HP yang memberikan kemudahan dalam berkomunikasi dengan siapa saja dan dimana saja, telah menjadi bagian yang penting dalam proses bisnis dan kehidupan masyarakat.

Persoalan utamanya informasinya mudah disadap, karena menggunakan *signal radio* sebagai saluran transmisinya. Jaringan *Mobile telephone* merupakan persoalan pokok dalam masalah keamanan dikarenakan *cost* yang sangat besar dalam penanggulangannya. Oleh karenanya *securiti* servis sangat dibutuhkan oleh pengguna *Mobile Phone*.

Salah satu solusi yang digunakan untuk mengatasi masalah keamanan dalam system GSM ini adalah dengan menggunakan proses autentikasi. Proses dimana data pelanggan atau informasi tentang pelanggan dapat dirahasiakan dan tidak mudah dipalsukan atau digunakan oleh orang-orang yang tidak berhak.

## 1.2 Tujuan Penulisan

Proposal Tugas Akhir ini bertujuan :

1. Sebagai salah satu syarat kelulusan bagi mahasiswa Telekomunikasi Multimedia Politeknik Negeri Padang.
2. Untuk menerapkan ilmu dan keahlian yang diperoleh selama perkuliahan khususnya mata kuliah Komunikasi Data.
3. Dapat mengetahui proses dalam system keamanan pada jaringan GSM terutama pada AUC (Authentication Center).
4. Sebagai bahan ajar bagi Dosen telekomunikasi khususnya pada mata kuliah system komunikasi bergerak.

## 1.3 Ruang Lingkup

Mata kuliah atau bidang keilmuan yang menunjang tugas akhir ini adalah komunikasi data data, sistem komunikasi bergerak dan program penunjang adalah visual basic.

## 1.4 Batasan Masalah

Dalam penulisan tugas akhir ini pembahasannya meliputi simulasi pada AUC (Authentication Center) yang menggunakan algoritma A3, A5, dan A8 sebagai algoritma autentikasi.

## BAB V

### PENUTUP

#### 5.1 Kesimpulan

Berdasarkan pembahasan yang telah dilakukan maka dapat diambil kesimpulan sebagai berikut:

1. Untuk menjamin aspek keamanan, sistem jaringan GSM (*Global System for Mobile Communication*) menawarkan tiga macam keamanan, yaitu autentifikasi, kerahasiaan data dan sinyal, serta kerahasiaan pengguna.
2. Dalam jaringan GSM Autentikasi terjadi ketika melakukan panggilan ataupun pengiriman data. Autentikasi terjadi untuk memastikan bahwa tidak terjadi pemalsuan pada data pelanggan, sehingga hanya pengguna yang sah saja yang dapat mengakses jaringan GSM.
3. Pada kartu SIM, kunci otentikasi individual dari pengguna juga tersimpan pada pusat otentikasi GSM. Semua orang yang memiliki hak dan kemampuan untuk mengakses pusat otentikasi dapat memperoleh kunci otentikasi dari pelanggan yang valid untuk melakukan impersonasi terhadap pengguna selular tersebut.
4. Algoritma yang digunakan untuk keamanan GSM adalah:
  - a. A3 : untuk otentikasi user.
  - b. A5 : untuk enkripsi pesan.
  - c. A8 : untuk menghasilkan *ciphering key*.

Semua algoritma tidak bersifat publik sehingga kerahasiaan data pelanggan dapat terjaga

## DAFTAR PUSTAKA

1. Gunawan, Uke Kurniawan, Gunadi. *Konsep Teknologi Seluler*. Informatika Bandung. Bandung 2008.
2. Silalahi, Nurain. *Komunikasi Mobile Publik dan Sistem Komunikasi Personal PCS*. PT. Elex Media Komputindo Kelompok Gramedia. Jakarta 2003.
3. Saydam, Gouzali. *Teknologi Telekomunikasi Perkembangan dan Aplikasi*. ALFABETA. April 2005. Bandung
4. Saydam, Gouzali. *Sistem Telekomunikasi*. Djambatan. Jakarta 1993
5. Prasetyo, Didik Dwi. *101 TIP dan TRIK Visual Basic 6.0. Edisi kedua*. PT. Elex Media Komputindo Kelompok Gramedia. Jakarta 2007
6. Prasetyo, Didik Dwi. *101 TIP dan TRIK Visual Basic 6.0*. PT. Elex Media Komputindo Kelompok Gramedia. Jakarta 2006