BAB 1
PENDAHULUAN

1.1 Latar Belakang

Pada zaman modern ini jaringan GSM telah menyebar luas di seluruh dunia dan dipakai pada telepon selular mayoritas masyarakat pada zaman ini. Adapun pengertian *Global System for Mobile Communication* disingkat GSM adalah sebuah teknologi komunikasi selular yang bersifat digital. Teknologi GSM banyak diterapkan pada komunikasi bergerak, khususnya telepon genggam. Teknologi ini memanfaatkan gelombang mikro dan pengiriman sinyal yang dibagi berdasarkan waktu, sehingga sinyal informasi yang dikirim akan sampai pada tujuan. GSM dijadikan standar global untuk komunikasi selular sekaligus sebagai teknologi selular yang paling banyak digunakan orang di seluruh dunia. Saat ini keamanan komunikasi dalam jaringan GSM terbilang cukup aman karena menggunakan standar enkripsi A5/1.

Akan tetapi, menurut [7] yang mengatakan bahwa algoritma A5/1 memiliki kelemahan serius didalam keamanan komunikasi datanya. Oleh karena itu, akan dibuat suatu proyek akhir yang mempunyai tujuan untuk analisis kelemahan dari keamanan algoritma A5/1 yang digunakan oleh jaringan GSM.

Dari suatu *Encrypted* Burst nantinya akan didapatkan XoR'ed burstnya, burst tersebut akan dicari kunci chiper-nya dengan menggunakan *software* bernama Kraken. Tersambung dengan *Harddisk External* 4 *Terabyte* sebagai tempat *master file*-nya yaitu *Rainbow Table*. Cara ini digunakan untuk melakukan analisis kelemahan keamanan data komunikasi GSM. Dikarenakan data komunikasi merupakan hal yang sangat penting bagi pemakai jaringan GSM.

1.2 Rumusan Masalah

Adapun perumusan masalah dari paparan latar belakang tersebut adalah sebagai berikut.

1. Bagaimana cara melakukan *convert rainbow table* ke dalam program Kraken?
2. Bagaimana cara konfigurasi kraken untuk mencari kunci chiper data komunikasi GSM?

1.3 Tujuan

Adapun tujuan dari proyek akhir ini adalah sebagai berikut.

1. Dapat melakukan *convert rainbow table* ke dalam program Kraken.
2. Dapat melakukan konfigurasi Kraken untuk mencari kunci chiper data komunikasi GSM.

1.4 Batasan Masalah

Adapun batasan masalah dalam pembahasan proyek akhir ini adalah sebagai berikut.

1. Tidak membahas lebih jauh tentang algoritma A5/2 dan A5/3.
2. Tidak membahas lebih jauh tentang RTL-SDR.
3. Tidak membahas lebih jauh tentang autentikasi pada GSM.
4. Tidak membahas lebih jauh tentang penangkapan sinyal GSM.
5. Tidak membahas lebih jauh tentang *decoding* data komunikasi GSM.
6. Hanya membahas tentang keamanan data komunikasi GSM.
7. Hanya membahas pencarian kunci chiper data komunikasi GSM.

1.5 Definisi Operasional

Berikut ini adalah definisi operasional dari sistem yang akan dibuat pada proyek akhir ini.

1. GSM

Global System for Mobile Communication (GSM) awalnya berasal dari singkatan *Grupe Special Mobile* yang memiliki pengertian sebuah teknologi komunikasi seluler yang bersifat digital.

2. Rainbow Table

Rainbow Table adalah *precomputed table* yang digunakan untuk mengembalikan fungsi kriptografi *hash*. Umumnya digunakan untuk *crack hash* kata sandi.

3. Kunci Chiper

Kunci Chiper (Kc) adalah kunci yang digunakan dalam algoritma enkripsi A5/1 untuk menulis dan menguraikan data yang sedang dikirim pada suatu komunikasi. Kc digunakan untuk enkripsi dan juga dekripsi. Kc ini hanya boleh diketahui oleh ponsel dan jaringan.

4. Burst

Burst adalah format informasi yang ditransmisikan selama satu *time slot* TDMA. Informasi ditumpangkan pada satu time slot pada frame TDMA melalui *Air Interface* yang biasa disebut Burst (pemecahan). Burst yang normal mengandung paket 57 bit dari data *encrypted message* atau *voice*.

1.6 Metode Pengerjaan

1. Studi Literatur

Pencarian referensi dan sumber – sumber untuk mempelajari konsep dan teori yang berkaitan dengan GSM dan enkripsi pada GSM. Hal ini dilakukan sebagai landasan untuk analisis kebutuhan sistem dan implementasi sistem yang akan dibangun.

2. Analisis Kebutuhan Sistem

Landasan konsep dan teori yang telah dilakukan pada tahap studi literatur digunakan untuk menganalisis kebutuhan sistem kemudian mengimplementasikan sistem dari hasil analisis kebutuhan ini.

3. Implementasi dan Pengujian Sistem

Untuk implementasi sistem yang akan dibangun, dilakukan dengan instalasi perangkat – perangkat lunak pada sistem. Kemudian dilakukan pengujian dari implementasi sistem yang sebelumnya telah dilakukan. Pada tahapan ini dilakukan pengujian *rainbow table*, XoR *keystream* dengan *encrypted* burst, *crack* XoR'ed burst dan pencarian *chiper key* pada mesin virtual. Hal ini dilakukan untuk memastikan sistem yang telah dibuat dapat berjalan dengan baik.

4. Penyusunan Laporan

Pada tahap terakhir ini, dilakukan dokumentasi dan penyusunan laporan dari semua proses tahapan yang telah dilakukan.

1.7 Jadwal Pengerjaan

Tabel 1- 1 Jadwal pengerjaan proyek akhir

No.	Kegiatan	Maret 2017				April 2017				Mei 2017				Juni 2017				Juli 2017			
		1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
1	Studi Literatur																				
2	Analisis Kebutuhan Sistem																				
3	Implementasi dan Pengujian sistem																				
4	Penyusunan Laporan																				