BAB II
LANDASAN TEORI

1. Kajian Peneliti Terdahulu

Desain Penelitian yang pertama terkait *simcard cloning* dalam hal ini untuk mengetahui lebih mendalam tentang karakteristik data dan bukti digital pada *simcard*, teknik *imaging, collecting* dan analisis data pada *simcard* maka diterapkan sebuah aktifitas forensika digital dalam sebuah simulasi kasus. Pada simulasi ini diasumsikan telah terjadi pencurian *handphone* dan duplikasi *simcard* oleh si pelaku. Selanjutnya untuk mengecoh penyidik maka *handphone* dan *simcard* asli diletakkan pada satu tempat dan *simcard* hasil *cloning* diaktifkan pada lokasi lain. Melalui *simcard cloning* inilah si pelaku melakukan sejumlah tindak kejahatan. Selanjutnya diasumsikan si pelaku dapat ditangkap dan ditemukan dua barang bukti, satu adalah handphone dan *simcard* yang asli dan yang lain adalah *handphone* dan *simcard* hasil *cloning.* Penyidik diminta untuk melakukan eksplorasi data-data pada *simcard* yang akan akan mendukung upaya pembuktian atas tindak kejahatan yang telah dilakukan. Berdasarkan penelitian diatas dapat ditekankan bahwa *simcard* merupakan sebuah perangkat komunikasi yang sangat dibutuhkan di era digital ini. Dibalik perannya sebagai media komunikasi, *simcard* ternyata juga berpotensi untuk menyimpan barang bukti pada suatu kasus kejahatan atau bahkan *simcard* tersebut adalah juga berfungsi sebagai alat kejahatan. Pada penelitian ini telah dilakukan sejumlah langkah serta ekplorasi terhadap *simcard* menggunakan *Simcard Seizure*. Analisis dilakukan untuk mengetahui beberapa karakteristik data digital yang dapat disimpan dalam *simcard* serta teknik untuk melakukan analisisnya. Untuk barang bukti *simcard*, data digital standar yang dapat dijadikan sebagai inisiasi proses investigasi adalah pada informasi ICCID *(Serial Number),* IMSI *(Subscriber ID),* MSISDN *(Phone Number),*

SMS *(Text Message),* AND *(Dialled Numbers)* dan LND (*Last Dialled Number*). Informasi tersebut dapat dilihat dengan mengenali karakteristik struktur *file* dan nilai heksa *decimal* pada *simcard* yang terbagi menjadi *Master File* (MF), *Dedicated File* (DF), dan *Elementary File* (EF). Bagan yang dihasilkan dari penelitian ini dapat dijadikan sebagai panduan dan pengetahuan praktis bagi investigator digital untuk mengungkapkan kasus-kasus kejahatan yang melibatkan barang bukti *simcard* (Prayudi & Rifandi, 2013).

Sistem keamanan GSM berdasar pada pertukaran data antara HLR (*Home Location Register)* dengan kartu SIM pada MS (*Mobile Station* atau telepon selular). Data yang ditukarkan diatas yaitu Ki, yaitu kunci sepanjang 128 bit yang digunakan untuk membuat 32 bit *response* yang disebut *SRES*, sebagai jawaban dari adanya *random challenge* yang disebut RAND, yang dikirim MSC melalui BTS kepada MS. Selain Ki data yang ditukarkan yaitu Kc, yaitu kunci sepanjang 64 bit yang digunakan untuk mengenkripsi pesan selama diudara antara BTS dengan MS. RAND, SRES yang dibangkitkan berdasarkan adanya RAND dan Ki, serta Kc yang juga dibangkitkan berdasarkan Ki disebut *triplet*, *triplet* tersebut telah dijelaskan dibagian makalah sebelumnya dalam proses autentikasi. Berdasarkan penelitian system keamanan GSM dapat diperoleh penekanan bahwa jaringan GSM melakukan autentikasi pada saat awal melakukan panggilan. Autentikasi pada GSM yaitu menggunakan algoritma A3 dengan kunci Ki dengan metode *Challenge* and *Response.* Autentikasi menggunakan prosedur *Unique Challenge Procedure* dengan *base station* mengenerate nilai 24-bit value dan mentransmisikannya ke *mobile station* di *Authentication Challenge Message.* Banyak kemungkinan untuk melakukan serangan pada sistem keamanan GSM, serangan itu dapat dilakukan pada algoritma A3, A5 maupun A8. Jaringan GSM meskipun dengan sistem keamanan telah diperbaiki dengan sempurna, tetapi masih ada peluang untuk melakukan penyadapan yaitu dengan melakukan skenario sosial *engineering*, yaitu dengan dapat berpura-pura sebagai pegawai operator maupun menyadap panggilan pada jaringan *backbone* operator selullar (Fauzan, 2013).

Ponsel dan perangkat genggam lainnya menggabungkan kemampuan *smartphone* dimana-mana. Selain menempatkan panggilan, ponsel memungkinkan pengguna untuk melakukan tugas-tugas lain seperti pesan teks dan manajemen daftar buku telepon (*phonebook*). Ketika ponsel dan perangkat seluller yang terlibat dalam kejahatan atau kejadian lainnya, spesialis digital forensik memerlukan alat yang memungkinkan pengambilan yang tepat dan cepat. Untuk perangkat yang sesuai dengan standar *Global System for Mobile Communications* (GSM), data tertentu seperti nomor keluar *dial up*, pesan teks, dan buku telepon pada *Subscriber Identity Module* (SIM). Makalah ini memberikan gambaran tentang keadaan perangkat lunak forensik untuk *simcard*. Berdasarkan penelitian terkait keamanan GSM SIM, bahwa forensik perangkat selular adalah bagian dari subyek komputer forensik. Alat pemeriksaan forensik menerjemahkan data ke format dan struktur yang dapat dimengerti oleh pemeriksa dan dapat secara efektif digunakan untuk mengidentifikasi dan memulihkan bukti. Namun, alat memungkinkan ketidakakuratan perangkat menyebabkan alat tidak berfungsi semestinya dalam situasi tertentu sehingga penting *update* alat forensik. Perangkat lunak forensik untuk SIM berada dipertengahan tahap ini namun keterbatasan *update tools forensic* yang menjadi hambatan. Sedangkan alat yang dibahas dalam makalah ini umumnya dilakukan dengan baik dan memiliki fungsi yang disempurnakan dan lebih memadai, versi baru diharapkan untuk meningkatkan dan lebih memenuhi persyaratan investigasi (Jansen & Ayers, 2005).

Sistem GSM telah menjadi sistem yang paling populer untuk komunikasi seluler didunia. Penjahat biasanya menggunakan ponsel GSM, dan oleh karena itu kebutuhan untuk penyelidik forensik untuk memahami bukti dapat diperoleh dari sistem GSM. Makalah ini secara singkat menjelaskan dasar-dasar dari sistem GSM. Item bukti yang dapat diperoleh dari *Mobile Equipment*, SIM dan jaringan inti dieksplorasi. Alat untuk mengekstrak seperti bukti dari komponen sistem yang ada, tetapi ada kebutuhan untuk mengembangkan prosedur forensik yang lebih sehat dan alat-alat untuk mengekstraksi bukti-bukti tersebut.

GSM menyediakan otentikasi pengguna dan enkripsi lalu lintas diseluruh antarmuka udara. Hal ini dilakukan dengan memberikan pengguna dan jaringan rahasia bersama, *Called* Ki. Nomor 128-bit ini disimpan pada kartu SIM, dan tidak secara langsung dapat diakses oleh pengguna. Setiap kali ponsel terhubung ke jaringan, jaringan mengotentikasi pengguna dengan mengirimkan nomor acak (*challange*) ke ponsel. SIM kemudian menggunakan algoritma otentikasi untuk menghitung otentikasi token SRES menggunakan nomor acak dan Ki. *Mobile* mengirimkan SRES kembali ke jaringan yang membandingkan nilai dengan SRES independen dihitung. Pada saat yang sama, kunci enkripsi Kc dihitung. Jadi, bahkan jika penyerang mendengarkan lalu lintas udara dapat memecahkan kunci enkripsi Kc, serangan akan menjadi nilai kemungkinan yang kecil, karena kunci ini berubah setiap kali prosedur otentikasi dilakukan. Semua data yang disimpan dapat berpotensi memiliki nilai pembuktian. Namun, sebagian besar *file* mengacu pada internal jaringan bahwa pengguna sendiri tidak pernah melihat data tersebut. Oleh karena itu dibatasi untuk file yang khas atau identik yang merupakan bukti yang relevan pada penggunaan telepon sebagai referensi lebih lanjut.

Berdasarkan penelitian terkait autentikasi Ki dapat diperoleh penekanan bahwa peniruan pelanggan GSM lainnya memang mungkin bagi siapa saja yang dapat mendapatkan kartu pelanggan dan sesuai PIN/PUK. Metode ketiga analisis forensik dari ponsel hanya menggunakan telepon barang bukti untuk mengakses informasi yang tersimpan, Kebanyakan informasi yang tersimpan diponsel dapat diakses dengan menggunakan sistem menu telepon (Jansen & Ayers, 2005). Dalam hal ini telah diamati bahwa beberapa ponsel mengikat informasi yang tersimpan di telepon ke *subscriber identity* pada *simcard*. Dimaksudkan sebagai fitur keamanan untuk mencegah akses ke informasi oleh pengguna yang tidak sah. Sebagai contoh, ponsel Nokia *store log* panggilan keluar dan masuk di telepon. Jika pengguna menghapus kartu SIM dan masukkan kartu lain, *log* ini akan dihapus. Oleh karena itu investigator harus berhati-hati dengan mengeluarkan kartu dari telepon sebelum informasi yang relevan telah diamankan.

GSM adalah dunia sistem terbesar untuk komunikasi *mobile,* juga dasar bagi masa depan sistem UMTS, penting untuk mengenali kebutuhan dalam mempelajari metode dan alat untuk analisis forensik dari sistem GSM. Penyelidikan saat ini dilakukan dengan alat tidak dirancang khusus untuk forensik (kecuali *Cards4Labs*), kedepannya mudah-mudahan akan memungkinkan gambaran penyidik dalam menganalisa isi dari ponsel dan *SIM-card* dengan cara forensik suara. Penelitian lebih lanjut juga diperlukan dalam analisis informasi yang tersimpan di ponsel dan *SIM-card* dikarenakan bahwa sistem GSM mengandung sejumlah besar informasi yang berharga kepada penyidik. Sebagian besar informasi yang tersedia saat ini dan dapat diambil dan memiliki potensi besar untuk digunakan sebagai bukti (Willassen, 2003).

Perangkat *mobile* tumbuh dalam popularitas dan dimana-mana dalam kehidupan sehari-hari, perangkat *mobile* sering rentan dalam keamanan dan privasi. Ponsel, misalnya, telah menjadi target *spam* dan pelecehan. Kadang-kadang, ponsel menjadi media atau alat dalam kasus pidana atau penyelidikan perusahaan. Forensik telepon seluler itu penting untuk penegakan hukum dan penyelidik swasta. Forensik ponsel bertujuan memperoleh dan menganalisis data dalam ponsel, yang mirip dengan komputer forensik. Namun, alat-alat forensik untuk ponsel yang sangat berbeda dari orang-orang untuk komputer pribadi. Salah satu tantangan didaerah ini adalah kurangnya prosedur validasi alat bantu forensik untuk menentukan dan mendeskripsikan barang bukti. Makalah ini menyajikan penelitian awal dalam menciptakan dasar untuk menguji alat forensik. Penelitian ini dilakukan dengan mengisi data uji ke ponsel (baik secara manual atau dengan *Identity Module Programmer*) dan kemudian berbagai alat efektivitas akan ditentukan oleh persentase data uji diambil. Penelitian ini akan meletakkan dasar untuk penelitian lebih lanjut dalam bidang ini. Penelitian ini dapat diperluas lebih lanjut dalam beberapa cara, Pertama, pengguna menggunakan *T-Mobile* kartu SIM standar sehingga jumlah perubahan yang dapat dilakukan terbatas, tes kartu SIM atau *SmartCard* yang dibuka akan memberikan rentang yang lebih besar dari

daerah untuk data yang akan ditulis. Kedua, seorang penulis kartu SIM atau *programmer identity module* untuk menulis langsung ke kartu SIM juga akan memungkinkan rentang yang lebih besar dari *file simcard*. Ketiga, *open source writeSIM* atau identitas programmer modul dan pembaca kartu SIM akan lebih ideal untuk membaca/mendapatkan data dan menulis data sehingga memiliki kemampuan untuk melihat serta memodifikasi kode.

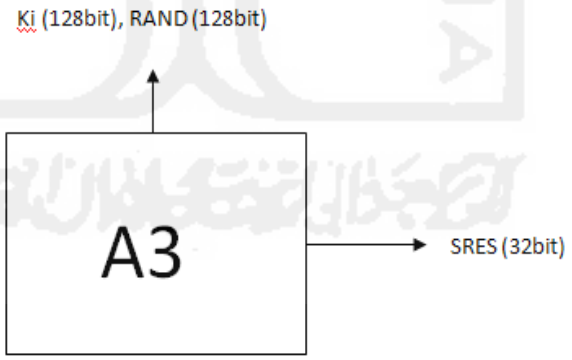
Penelitian ini dibatasi dengan ruang lingkup waktu dan peralatan yang tersedia. Namun, menyediakan cara sederhana untuk memvalidasi alat forensik untuk ponsel. Penelitian ini dapat diperluas lebih lanjut dengan menguji alat forensik ponsel berganda dengan data dasar yang sama. Karena kartu SIM yang digunakan dalam percobaan adalah kartu SIM standar *T-Mobile* yang terkunci, jumlah perubahan dan modifikasi yang terbatas karena perlindungan data penting atau kesalahan menimpa data asli tersebut. Akan lebih menarik jika dapat menguji kartu SIM atau kartu pintar yang tidak terkunci, sehingga akan memberikan rentang yang lebih besar dari daerah untuk data yang akan ditulis(Bhadsavle & Wang, 2009).

Pada sistem keamanan jaringan GSM, ditemukan beberapa kelemahan yang terjadi pada pengamanan data di luar *link radio*. *Simard Clone* adalah bagian dari masalah keamanan di *Mobile Station*. Beberapa *authentication algorithm simcard* GSM dapat ditembus dengan alat tertentu sehingga seluruh data dalam simcard dapat dipindahkan ke *simcard* lain. Penelitian ini melakukan *cloning simcard* serta menganalisis pengkombinasian metoda kriptografi ECC (*Elliptic Curve Cryptography*) dengan algoritma A3,A5,dan A8 untuk mendapatkan kualitas keamanan yang lebih baik. Analisis untuk menguji performansi metode ECC yang meliputi proses registrasi, *basic call setup*, dan *roaming* dengan menggunakan parameter perbandingan dalam analisis adalah analisis waktu proses, *data rate*, dan pengujian *avalanche effect*. Dari penelitian ini didapatkan bahwa metode ECC hanya dapat dikombinasikan dengan algoritma A3 dan A8 dan efektif mengurangi celah ditembusnya kerahasiaan identitas pelanggan dan proses autentikasi tanpa penambahan waktu proses secara signifikan. Meski terdapat penambahan

jumlah *bit* data yang ditransmisikan, penambahan *data rate* yang terjadi masih dapat ditolerir. Berdasarkan penelitian ini juga didapatkan hasil bahwa metoda ECC tersebut ternyata tidak efektif bila dikombinasikan dengan algoritma A5 disebabkan adanya perbedaan sistem dan prosedur antara keduanya (Hayat, 2014)

Penelitian selanjutnya terkait dengan *simcard* yang telah direview maka akan diteliti lebih lanjut tentang bagaimana *simcard* itu dapat di *cloning*, efek yang timbul bilamana *simcard* telah dikloning, serta menganalisa skema dan metode pengkloningan *simcard*. Selanjutnya akan dibahas lebih lanjut upaya investigasi forensik terhadap barang bukti digital berupa *simcard cloning* dan *simcard* asli dengan metode pencocokan algoritma COM128 A3 RAND dan A8 untuk mendapatkan *Autentication Key* (KI) pada kedua *simcard*. Algoritma Pengkodean GSM terdiri dari Algoritma A3 dan A8, Algoritma A3 adalah algoritma autentikasi dalam model keamanan GSM.

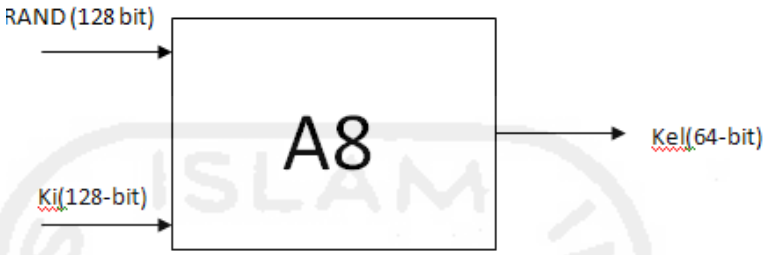
Fungsi A3 adalah untuk membangkitkan *reponse* yang lebih dikenal dengan SRES sebagai jawaban dari *random challenge* yang dikenal dengan RAND. *Sign Response* (SRES) dihitung dengan melihat nilai RAND dan Ki seperti pada Gambar 2.1



Gambar 2.1 Sign Response (SRES) (Briceno M, 1998).

Algoritma A8 adalah algoritma yang berfungsi untuk membangkitkan kunci sesi pada sistem keamanan GSM. Algoritma A8 membangkitkan kunci sesi, Kc, dengan melihat *random challenge*, RAND, yang diterima dari MSC dan kunci

rahasia Ki, yang terdapat pada kartu SIM. Algoritma A8 menagmbil 128 bit masukkan dan membangkitkan 64 bit keluaran. Keluaran sejumlah 64 bit ini merupakan kunci sesi Kc. seperti pada Gambar 2.2



Gambar 2.2 Perhitungan Kunci Sesi (Kc) (Briceno M, 1998).

Hasil yang diharapkan dari penelitian ini berupa gambaran proses investigasi forensik terkait autentikasi *simcard cloning* dengan *simcard* asli menggunakan analisa *Random Number Generator* (RAND) deangan tujuan akhir yaitu memberikan sumbangsi kepada pihak investigator dalam menangani barang bukti tindak kejahatan *mobile phone* dan sejenisnya. Berdasarkan beberapa pengkaji terdahuli terkait simcard dan keamanannya maka dapat klasifikasikan peneliti seperti tampak pada Table 2.1

Tabel 2.1 Tabel Literatur Review

No	Nama	Judul	Uraian Singkat	Hasil Penelitian
1.	Prayudi & Rifandi, 2013	Ekplorasi Bukti Digital pada Simcard	Skema kasus simcard cloning dalam hal ini untuk mengetahui lebih mendalam tentang karakteristik data dan bukti digital pada simcard, teknik imaging, collecting dan analisis data pada Simcard	Ekplorasi simcard & upaya investigasi simcard secara umum
2.	Fauzan, 2013	Studi dan Perbandingan Keamanan GSM dan CDMA	Sistem keamanan GSM berdasar pada pertukaran data antara HLR (Home Location Register) dengan kartu SIM pada MS (Mobile Station) RAND, MSC melalui BTS kepada MS. Ki & Kc yang digunakan untuk mengenkripsi pesan antara BTS dengan MS. RAND, SRES	Autentikasi pada GSM yaitu menggunakan algoritma A3 dengan kunci Ki dengan metode Challenge and Response. Autentikasi menggunakan prosedur Unique Challenge Procedure
3.	Jansen & Ayers, 2005	Forensic Software Tools for Cell Phone Subscriber Identity Modul	Spesialis forensik dalam pengambilan yang tepat dan pemeriksaan cepat data. Untuk perangkat Global System for Mobile Communications (GSM), Makalah ini memberikan gambaran tentang keadaan perangkat lunak forensik untuk simcard	Alat pemeriksaan forensik sebagai penterjemah data ke format dan struktur yang dapat dimengerti oleh pemeriksa dalam mengidentifikasi dan memulihkan bukti digital dengan kelebihan & kekurangannya
4.	Willassen , 2003	Forensics and the GSM mobile telephone system Senior Investigator	Makalah ini secara singkat menjelaskan dasar-dasar dari sistem GSM. Item bukti yang dapat diperoleh dari Mobile Equipment, SIM dan jaringan inti dieksplorasi untuk mengembangkan prosedur forensik yang lebih baik.	Kesimpulannya bahwa peniruan simcard GSM memang mungkin bagi siapa saja yang dapat. Metode analisis forensik masih kontak fisik dengen ponsel untuk mengakses informasi yang tersimpan.
5.	Bhadsavle & Wang, 2009	Validating Tools for Cell Phone Forensics	Makalah ini menyajikan penelitian awal dalam menciptakan dasar untuk menguji alat forensik & diamati bahwa beberapa ponsel dengan informasi yang tersimpan di subscriber identity pada SIM-card tepatnya di store log pada T-Mobile kartu SIM standar	SIM standar T-Mobile yang terkunci, masih memungkinkan perubahan dan modifikasi terkait perlindungan data

Tabel 2.1 Tabel Literatur Review (Lanjutan)

6.	Cynthia Hayat, 2014	Analisis SIM Card Clone Pada IM3 Smart Serta Penggunaan Ellptic Curve Cryptosystem Untuk Meningkatkan Keamanan Jaringan GSM	Penelitian ini melakukan cloning simcard serta menganalisis pengkombinasian metoda kriptografi ECC (Elliptic Curve Cryptography) dengan algoritma A3,A5,dan A8 untuk mendapatkan kualitas keamanan yang lebih baik.	Penelitian ini didapatkan bahwa metode ECC hanya dapat dikombinasikan dengan algoritma A3 dan A8 serta metoda ECC tersebut ternyata tidak efektif bila dikombinasikan dengan algoritma A5 disebabkan adanya perbedaan sistem dan prosedur antara keduanya.
7.	**Nuril Anwar, 2015**	**Forensic Simcard Cloning Menggunakan Algoritma Autentikasi Random Number Generator (RAND)**	**Investigasi Forensik terhadap simcard cloning & simcard asli dengan mencocokkan algoritma COM128 A3 dan A8 untuk mendapatkan Autentication Key (KI) pada simcard**	**Hasil yang diharapkan berupa gambaran proses investigasi forensic terkait autentikasi simcard cloning dengan menganalisa algoritma autentikasi Random Number Generator (RAND)**

2. Landasan Teori

2.1 Umum

Kemajuan teknologi komunikasi dalam penggunaan ponsel berbasis GSM sekarang ini sudah mencapai jumlah yang sangat signifikan dan mulai menimbulkan persoalan-persoalan baru yang tidak pernah ditemui sebelumnya. Persoalan yang muncul sebenarnya bukan pada peralatan ponsel yang sangat pasif dipasaran dari berbagai model, tetapi lebih pada persoalan-persoalan yang menyangkut persoalan harga, kekuatan sinyal, serta fasilitas layanan yang disediakan oleh para operator GSM.

Harga memang selalu menjadi persoalan utama para pengguna ponsel GSM dimana saja, termasuk di Indonesia. Ini terlihat dari banyaknya jumlah pengguna GSM yang memilih skema pembayaran pre-paid dengan memilih *simcard* isi ulang yang sangat populer. Lebih dari 80 persen *simcard* diberbagai operator GSM di Indonesia adalah para pelanggan yang membayar dimuka dengan pilihan isi pulsa yang variatif. Banyaknya pengguna jasa GSM juga menyebabkan masalah lain, terutama berkaitan dengan kekuatan sinyal dari berbagai *base station* yang terasa mulai sesak dan tidak tertatanya pusat penerima sinyal GSM yang mengakibatkan tidak dapat memperoleh sinyal dikawasan tertentu. Di sisi lain, karena kemajuan teknologi perangkat ponsel sendiri, tidak semua operator GSM memiliki jasa layanan multimedia masa kini seperti GSM, MMS, dan sejenisnya. Karena persoalan ini, banyak pelanggan GSM memiliki lebih dari satu *simcard* dari beberapa operator untuk dapat menikmati berbagai jasa layanan yang tidak dimiliki oleh operator lain.

Sistem Generasi Pertama (Zahara, 2008).

2.2 Generasi Simcard

1) Sistem generasi pertama

Sistem generasi pertama umumnya masih menggunakan teknologi selular analog. Contoh sistem generasi pertama ini adalah NMT

(*Nordic Mobile Telephony*) yang mulai diimplementasikan di Jakarta tahun 1986. AMPS *(Advanced Mobile Phone System)* yang masuk Indonesia sekitar tahun 1991 juga termasuk dalam kategori ini.

Seperti telah dikemukakan sebelumnya pengembangan dari sistem ini adalah dengan menggunakan PIN sebelum melakukan panggilan. Namun demikian sistem ini tetap sangat lemah karena dengan kemajuan teknologi maka sistem *scanner* untuk teknologi ini relatif mudah diperoleh dan algoritma pengacakannya mudah ditemukan sehingga dapat mudah untuk digandakan (kloning).

Fraud yang banyak terjadi pada sistem generasi pertama ini adalah *Kloning* dan *Tumbling*. Kloning dilakukan dengan menggandakan identitas MIN dan ESN pada suatu telepon lain. Identitas MIN dan ESN ini pada awalnya diperoleh dengan melakukan *scanner* pada saat telepon gengam menerima atau melakukan panggilan. *Tumbling* dilakukan dengan cara melakukan modifikasi terhadap konfigurasi rangkaian dalam telepon sehingga telepon memiliki ESN yang berbeda. Melihat banyaknya kemungkinan fraud pada sistem teknologi selular analog maka saat ini teknologi ini mulai banyak ditinggalkan dan beralih kepada sistem dengan teknologi selular digital.

2) Sistem Generasi Kedua

Pada sistem generasi kedua telah menggunakan sistem komunikasi selular digital. Contoh sistem yang dapat dikategorikan sebagai sistem generasi kedua ini adalah sistem GSM, CDMA, PDC dan D-AMPS. Di Indonesia sendiri, sistem yang menjadi kategori ini misalnya adalah Sistem GSM yang dimiliki oleh tiga operator: Telkomsel, Satelindo dan Excelcomindo dan sistem CDMA IS-95 yang dioperasikan oleh Komselindo. Sistem GSM menggunakan model keamanan yang berbeda dibanding sistem CDMA. Pada GSM, model keamanan yang dipakai dikenal dengan nama protokol *Security Triplet*, sedangkan CDMA menggunakan *Shared Secret Data* (SSD).

Seperti pada generasi kedua ini juga terdapat ESN yang di-*set* saat pembuatan dipabrik. Disamping itu juga terdapat pula nomor sebanyak 15 digit yang dikenal dengan *International Mobile Subscriber Identity* (IMSI) yang unik dimana tidak akan sama diseluruh dunia.

Pada sistem GSM, ESN ini lebih dikenal dengan nama *International Mobile Equipment Identifier* (IMEI) yang juga terdiri dari 15 digit. Nomor ini biasanya terdapat pada belakang tempat baterai telepon gengam atau pada nomor kartu garansi.

Selain nomor IMEI tersebut, nomor IMSI juga ditransmitkan. Jika IMEI terletak pada setiap telepon gengam maka IMSI terletak pada setiap kartu *Subscriber Identity Module* (SIM) pada *customer*. SIM ini berisi semua informasi *customer* yang diproteksi dengan *Personal Identification Number* (PIN), juga kunci authentifikasi *customer* (Ki), kunci rahasia yang dihasilkan dengan algoritma (A8) dan algoritma A3 dalam sebuah *Smartcard*. Protokol ini dikenal dengan sebutan *Security Triplet*. *Triplet* yang identik terdapat pada telepon gengam customer dan juga di database sentral telepon bergerak atau *Home Location Register* (HLR).

Algoritma yang dihasilkan dalam telepon gengam adalah algoritma rahasia A5. Algoritma A3, A5 dan A8 juga terdapat dalam *database* jaringan operator GSM. Untuk melakukan autentikasi, semua elemen (SIM, telepon gengam dan *database* GSM) ini diperlukan. Kloning relatif tidak mungkin dapat dilakukan tanpa mengakses *chip* pada SIM karena kode ini relatif tidak mungkin dapat diperoleh melalui *scanner* seperti pada sistem generasi pertama karena algoritma tadi menyebabkan pengacakan informasi. Seperti juga pada sistem GSM, sistem ini relatif tidak mungkin dapat dilakukan kloning dengan melakukan pencurian informasi data SSD, MIN dan ESN melalui udara karena sistem pengacakan dan algoritma digital yang dilakukan, termasuk juga pada kanal suara yang melakukan proses *encryption*.

3) Sistem Generasi Ketiga

Pada sistem generasi ketiga model autentikasi merupakan gabungan kelebihan-kelebihan model keamanan pada generasi sebelumnya. Selain itu juga dengan tambahan *end-to-end security* dan integrasi data. Kelemahan sistem GSM bahwa proses *encryption* hanya dilakukan pada komunikasi melalui udara.

Dengan adanya integrasi sistem komunikasi telepon bergerak dengan komunikasi data, maka metode keamanan yang dipergunakan adalah dengan algoritma *asymmetric cryptographic*. Alasan penggunaan metoda ini adalah karena keamanan ini mengunakan sertifikasi digital (*digital signatures*), penyederhanaan profil menjadi anonim, penyederhanaan distribusi *key* saat *roaming*. Hal ini juga dapat dicapai karena kecenderungan model sekuriti akan menggunakan *chip* yang fisiknya sama seperti kartu pada sistem GSM saat ini. Skenario dengan menggunakan algoritma *asymmetric* ini dengan kecenderungan:

a) Pasangan informasi autentikasi akan dihasilkan dalam telepon dan juga tergantung pada desain keamanan pada *smartcard* (chip).
b) Informasi bit *(key)* pada gengam harus lebih dahulu disertifikasi oleh operator dan disimpan dalam SIM.
c) Semua operator harus memiliki persetujuan bilateral untuk roaming, dan sebuah badan sertifikasi internasional akan diperlukan untuk implementasi sertifikasi secara internasional.

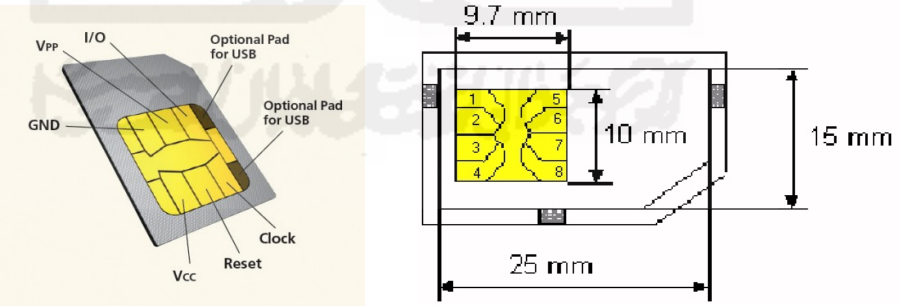
Beberapa yang tergolong pada algoritma *asymmetric cryptographic* diantaranya adalah Algoritma RSA dan Algoritma DSA, dan *Algoritma Elliptic Curve Crytosystems* (ECC) (Irhana, 2000). Secara umum dapat ditabelkan masing-masing model keamanan dari masing sistem generasi di atas dapat dilihat pada Tabel 2.2

Tabel 2.2 Model Keamanan Per-Generasi (Irhana, 2000)

Parameter	**Generasi 1st**	**Generasi 2nd**	**Generasi 3rd**
Signaling, Voice dan Data	Tidak ada	Tinggi: dilakukan pengacakan (encryted)	Tinggi: dilakukan pengacakan (encryted)
Lokasi, user ID	Tidak ada	Sedang: menggunakan IMSI	Tinggi: dengan sistem anonymity
Kloning	Mudah dikloning	Tidak mungkin	Tidak mungkin
Penyadapan melalui udara	Mudah	Susah	Susah

2.3 Simcard

Subscriber Identification Module (SIM) Bagian penting lain dari sistem *baseband* adalah *Subscriber Identity Module* (SIM) yang merupakan *smartcard* kriptografi dan dikeluarkan oleh *provider* seperti tampak pada Gambar 2.3. SIM berlaku dalam ROM nya, selain sistem operasi, algoritma keamanan untuk autentikasi dan pembangkitan kunci Kc.



Gambar 2.3 Model Simcard (Velazco, 2015)

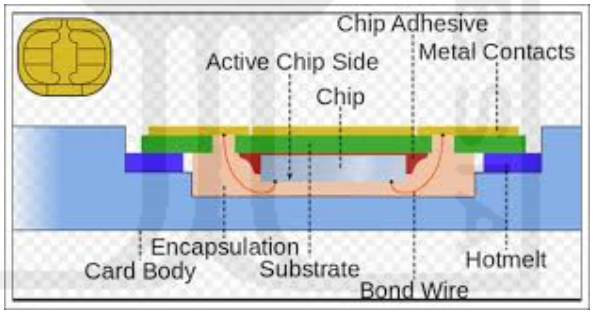
Simcard telah dibuat lebih kecil selama bertahun-tahun mengikuti fungsi independen atas perkembangan perangkat selular. Format antar *simcard*

diantaranya yaitu *Full-size* SIM diikuti oleh *mini-SIM*, *micro-SIM*, dan *nano-SIM*. Masing-masing *simcard* memiliki ukuran seperti tampak pada Tabel 2.3

Tabel 2.3 Simcard Sizes (Velazco, 2015)

SIM card	Introduced	Standard reference	Length (mm)	Width (mm)	Thickness (mm)	Volume (mm^3)
Full-size (1FF)	1991	ISO/IEC 7810:2003, ID-1	85.60	53.98	0.76	3511.72
Mini-SIM (2FF)	1996	ISO/IEC 7810:2003, ID-000	25.00	15.00	0.76	285.00
Micro-SIM (3FF)	2003	ETSI TS 102 221 V9.0.0, Mini-UICC	15.00	12.00	0.76	136.80
Nano-SIM (4FF)	early 2012	ETSI TS 102 221 V11.0.0	12.30	8.80	0.67	72.52
Embedded-SIM		JEDEC Design Guide 4.8, SON-8	6.00	5.00	<1.00	<30.00

Diantara model simcard dan ukuran simcard komponen elektronika juga terdapat dan melekan pada device simcard utama. Komponen yang berpengaruh terhadap penyimpanan data-data didalamnya meliputi seperti pada Gambar 2.4



Gambar 2.4 Komponen Simcard (Velazco, 2015)

Di dalam EEPROM yang memegang data untuk memberikan anonimitas, yaitu *International Mobile Subscriber Identity* (IMSI) dan *Temporary Mobile Subscriber Identity* (TMSI) dan Ki rahasia, yang bersama dengan penyedia seperti ekstrak data dan kunci rahasia yang dapat memungkinkan seorang penyerang untuk membuat kartu SIM kloning.

Perangkat *mobile* atau tepatnya perangkat lunak yang berjalan diatasnya dapat dibatasi untuk bekerja hanya dengan SIM kartu yang memenuhi persyaratan tertentu. Hal ini umumnya disebut *SIM Lock*.

Misalnya ponsel dapat terbatas pada penggunaan kartu milik jaringan operator tertentu dapat disebut *Net Lock*, atau negara tertentu. Paling diprioritaskan berupa kunci untuk kartu SIM individu yang sematkan bersama-sama dengan telepon. Karena minat yang besar dari pengguna akhir *(end user)* dalam menghilangkan pembatasan ini dapat diartikan memiliki nilai kemungkinan tinggi untuk serangan tersebut.

Aspek lain adalah bahwa komunikasi antara kartu SIM dan perangkat *mobile* tidak dienkripsi. Hal ini memungkinkan penyerang dengan akses fisik ke perangkat untuk menerapkan "*man in the middle attack*", misalnya menyalah gunakan fungsi *Toolkit* SIM Aplikasi seperti pengiriman SMS.
Keamanan dari GSM, Dalam hal ini dijelaskan layanan keamanan GSM lebih terinci. Informasi lebih lanjut untuk tujuan keamanan dapat ditemukan diantaranya adalah *Authentication*, kerahasiaan dan anonimitas (Pagliusi2002).

Authentication dalam GSM jaringan mengotentikasi MS *Mobile Station*, namun MS tidak mengotentikasi jaringan. Ide pokok utamanya adalah bahwa jaringan mengirimkan 128 Bit nomor acak dengan MS. MS diminta untuk mengirim SRES respon dari algoritma A3 dengan parameter RAND dan Ki kembali ke jaringan. SRES menjadi yang pertama 32bit algoritma COMP128, yang dijalankan pada SIM. Setelah MSC menerima respon dari MS (*Mobile Station*)cek hasilnya dan, jika benar, MS yang dianggap berhasil dikonfirmasi. Jadi keamanan otentikasi didasarkan pada rahasia Ki dan bahwa tidak mungkin untuk menurunkan Ki dari satu atau banyak RAND dan pasangan SRES, karena pada saat ini tidak ada enkripsi yang disediakan dan penyerang mampu menyadap komunikasi.

GSM didefinisikan menjadi sangat fleksibel dan standar diseluruh dunia dan dengan demikian memungkikan, bahwa MS perlu mengotentikasi ke PLMN. Provider ini tidak mengetahui rahasia bersama Ki dan karena itu tidak dapat mengotentikasi SIM. Untuk mengatasi keterbatasan hanya mampu menggunakan jaringan penyedia itu sendiri. GSM mendefinisikan *triplet* sebagai mekanisme untuk memungkinkan jaringan apapun untuk

otentikasi SIM. Hal ini terjadi melalui *(triplet)*. Sebuah *triplet valid* terdiri dari tantangan RAND dan SRES yang respon utamanya dipengaruhi oleh kunci sesi Kc. Semua penyedia jaringan saling mengutamakan peran RAND dan SRES sehingga produksinya sudah termasuk *include* bersamaan dengan Ki (Egners, Rey, Schmidt, Schneider, & Wessel, 2012).

2.4 Cloning Simcard

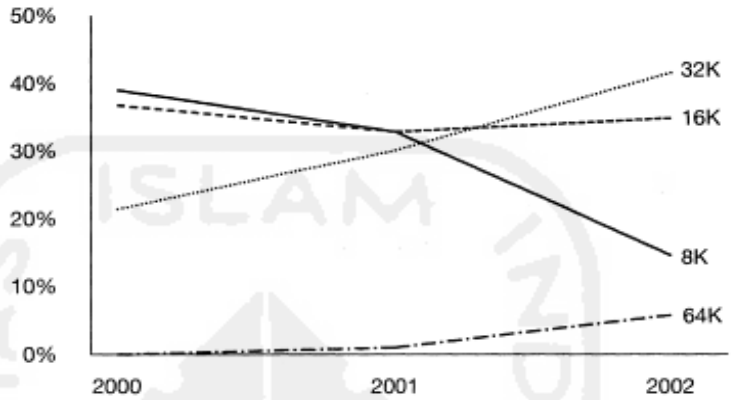
Ketika mencari arti kloning dalam sebuah kamus dapat dinyatakan sebagai membuat replika yang tepat atau bayangan cermin dari pemain pengganti subjek, subjek dapat berupa hidup hal atau non-hidup jadi disini dapat mempertimbangkan telepon seluler atau s*imcard*. Jadi *simcard cloning* adalah menyalin identitas satu *simcard* seluler ke *simcard* seluler lain. *Simcard cloning* illegal di Negara India, banyak orang ditahan karena melakukan hal semacam ini, saat ini banyak operator gsm di India yang melakukan "*surveillance techniques"* untuk mendeteksi orang yang melakukan peng-kloningan. *Simcard* berisi dua kode rahasia atau *"keys"* (imsi *value* dan ki *value*) agar operator dapat mengidentifikasi *simcard* tersebut serta autentikasi *costumer*. Kode ini berkaitan dengan nomor *mobile* yang disimpan didatabase operator. Berdasarkan *key* rahasia ini jugalah operator dapat mengetahui biling/transaksi para pelanggannya. Sekarang yang akan dilakukan adalah mengekstrak dua *key* rahasia tersebut dari sim target dan membenamkan programnya pada *smartcard* kosong atau dikenal dengan sebutan *wafer*. Karena autentikasi operator masih berdasarkan *key* rahasia tadi maka dapat mengelabui operator sehingga operator berpikir bahwa itu adalah *simcard* original yang merupakan salah satu kelemahan pada teknologi GSM. *Simcard* mana yang dapat diklone, *simcard* diproduksi dengan basis 3 alogaritma COMP128v1, COMP128v2 and COMP128v3 dan faktanya adalah bahwa 70% *simcard* yang dipakai sekarang adalah COMP128v1.

Mayoritas penyedia jasa layanan seluler masih menggunakan kartu SIM GSM dengan authentication algorithm COMP128-1 (COMP128v1).

Pada bulan April 1998, SDA *(Smartcard Developer Association*) dan dua orang peneliti dari ISAAC *(Internet Security, Applications, Authentication and Cryptography)* U.C. Berkeley mendapati bahwa *authentication algorithm* COMP128-1 ini ternyata dapat dengan mudah diakali. Hanya membutuhkan 50.000 hingga 150.000 lebih percobaan *"chosen-challenge and response attack"* untuk mendapatkan nilai Ki yang panjangnya 128 bit. Jika nilai Ki ini sudah berhasil diperoleh, proses *cloning* adalah pekerjaan yang sangatlah mudah. Tinggal memasukkan nilai Ki ke kartu *smartcard* yang sudah dilengkapi dengan STK emulasi kartu SIM.

Kartu SIM tersedia dalam berbagai kapasitas data, dari 8 KB sampai dengan 128 KB namun, dari berbagai kapasias memori *simcard* yang telah ada pada generasi *simcard* 32 KB hingga 128 KB yang lebih banyak beredar dipasaran. Semua memori *simcard* memungkinkan menyimpan maksimal 250 kontak telepone untuk disimpan di *simcard*, dengan memori 32 KB memiliki ruang untuk 33 Kode Jaringan Mobile (MNC) atau *"identity network"*, 64 KB versi memiliki ruang untuk 80 perusahaan telekomunikasi multinasional. *Simcard* sendiri dipesan oleh provider telekomunikasi seperti Three, Indosat, Telkomsel dan XL kepada pihak pembuatnya *Philips, Hitachi, ST Microelectronics* dan *simcard* ini dalam keadaan kosong belum diisi apapun. Kapasitas simpannya pun beragam mulai dari 8 KB - 128 KB. Setelah provider menerima maka *simcard* kosong ini akan diserahkan kepada perusahaan yang akan melakukan pengisian program dan data ID pada *simcard* dengan isian yang disesuaikan kapasitasnya. *Simcard* pasca pengisian program data pelanggan masih *idle* dan belum aktif, begitu sampai ke tangan pengguna maka begitu dipasang dan dinyalakan maka program pada *simcard* ditambah program aplikasi pada telepon akan melakukan *searching* jaringan awal, jika telah ditemukan barulah melakukan komparasi dengan *database* yang ada di provider, dari sini pengguna awal mulai melakukan registrasi setelah itu barulah *simcard* diaktifkan oleh mesin yang ada di provider selular. Kebijakan setiap perusahaan telekomunikasi bahwa setiap

pembelian *simcard* baru untuk komunikasi verbal diwajibkan untuk mengisikan data-data diri pelanggan. Grafik penggunaan *simcard* dengan kapasias memori dapat dilihat pada Gambar 2.5



	2000	2001	2002
8K	40%	34%	15%
16K	38%	34%	36%
32K	22%	31%	43%
64K	0%	1%	6%

Gambar 2.5 Grafik Penggunaan Simcard Per-Generasi

Berdasarkan grafik penggunaan *simcard* terkait memori yang melekat didalamnya berperan dalam *simcard cloning* menentukan keberhasilan kloning itu sendiri semakin besar memori yang terdapat pada *simcard* asli maka semakin lama pula proses *crack* Ki algoritma A8 pada *simcard*. Implementasi *authentication algorithm* COMP128-1 ini membuka peluang bagi pihak-pihak yang kreatif dengan melahirkan produk *cloning* kartu SIM GSM. Produk ini terdiri dari perangkat keras yang digunakan untuk menempatkan kartu SIM GSM, perangkat lunak untuk melakukan proses pembacaan dan penulisan kartu SIM GSM, dan satu kartu SIM GSM kosong yang dapat menampung empat, delapan, dua belas, atau bahkan enam belas nomor sekaligus.

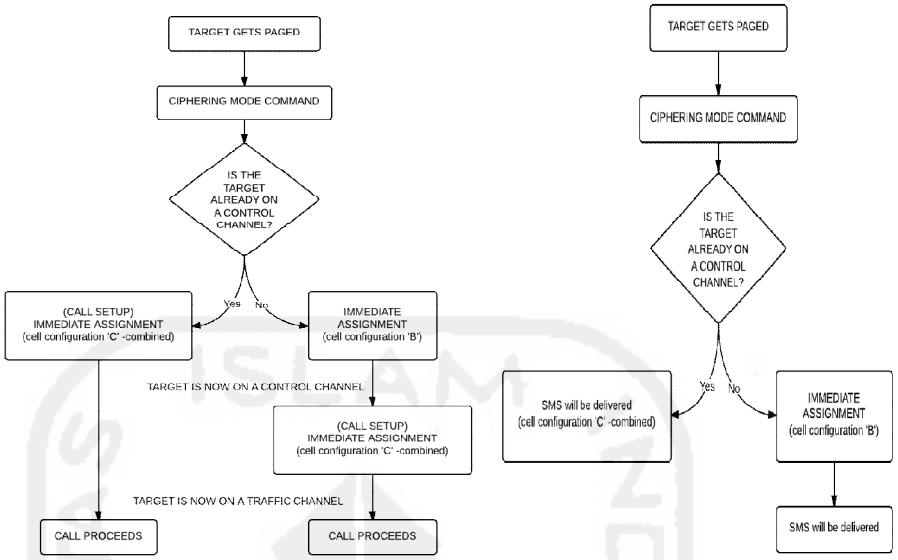
Perangkat yang dibutuhkan untuk melakukan *cloning* kartu SIM GSM ini adalah satu perangkat *reader/writer* kartu SIM GSM dan perangkat lunak yang tepat untuk melakukan scanning nilai Ki. Perangkat *reader/writer*

yang dihubungkan pada serial port RS-232 komputer pribadi (personal computer) ini dapat dibuat sendiri dengan harga yang terjangkau. Diagram skematik yang dibuat oleh Dejan Kaljevic ini dapat dengan mudah dibuat oleh mereka yang memiliki ketrampilan merakit rangkaian elektronika (R. Rao, Rohatgi, & Scherzer, 2002).

2.5 Attacks on GSM Security

Sistem keamanan GSM berdasar pada pertukaran data antara HLR *(Home Location Register)* dengan kartu SIM pada MS *(Mobile Station* atau telepon selular). Data yang ditukarkan diatas yaitu Ki, yaitu kunci sepanjang 128 bit yang digunakan untuk membuat 32 bit *response* yang disebut SRES, sebagai jawaban dari adanya *random challenge* yang disebut RAND, yang dikirim MSC melalui BTS kepada MS. Selain Ki data yang ditukarkan yaitu Kc, yaitu kunci sepanjang 64 bit yang digunakan untuk mengenkripsi pesan selama diudara antara BTS dengan MS. RAND, SRES yang dibangkitkan berdasarkan adanya RAND dan Ki, serta Kc yang juga dibangkitkan berdasarkan Ki.

Prinsip kerja cloning dapat dilihat dari Gambar 2.6, menurut (Tomcs, 2013) dalam *report page "The big GSM write-up how to capture, analyze and crack GSM"* bahwa *flowchart* atau alur proses terjadinya pembajakan sebuah telekomunikasi terjadi bilamana pengguna dianggap lalai dalam menggunakan alat komunikasinya sehingga memungkinkan tindak kejahatan berupa penyadapan ataupun pengkloningan pembicaraan maupun sms.



Gambar 2.6 Phone dan SMS Control Channel (Tomcs, 2013)

Proses autentikasi dimulai dengan adanya MS *sign on* MSC *(Mobile Service Switching Center)* melalui BTS dengan mengirim identitas, kemudian MSC meminta *triplet* kepada HLR, lalu HLR memberi HLR kepada MSC. MSC mengirim RAND kepada MS, kemudian MS menghitung SRES dengan algoritma A3 menggunakan RAND yang diterima dan Ki yang terdapat pada SIM. Setelah itu MS mengirim SRES kepada MSC. MSC menerima SRES, lalu mencocokkan SRES dengan SRES dari *triplet* dari HLR (HLR dapat menghitung SRES dari RAND yang HLR buat, karena HLR mengetahui semua Ki pada SIM).

Setelah proses autentikasi selesai, MS membangkitkan kunci sesi, Kc, dengan algoritma A8 berdasarkan pada *challenge* dari MSC dan Ki. Begitu juga pada BTS yang berfungsi sebagai sarana komunikasi dengan BTS, menerima Kc dari MSC, sehingga proses komunikasi udara antara BTS dengan MS terenkripsi.

Setiap *frame* dienkripsi dengan *keystream* yang berbeda. *Keystream* ini dibangkitkan dengan algoritma A5. Algoritma A5 diinisialisasi dengan Kc dan jumlah frame yang akan dienkripsi, kemudian membangkitkan *keystream* yang berbeda untuk setiap *frame.* Ini berarti

suatu panggilan dapat didekripsi jika penyerang mengetahui Kc dan jumlah dari *frame*. Kc yang sama digunakan selama MSC belum mengautentikasi MS lagi.

Serangan terhadap Keamanan GSM, Ada banyak kemungkinan serangan terhadap keamanan GSM dan itu adalah wajar, bahwa GSM tidak memenuhi persyaratan keamanan yang tinggi. Sebagian besar serangan timbul dari algoritma yang lemah yang digunakan dan beberapa kelemahan arsitektur. Sebagian besar serangan yang telah dijelaskan hanya berupa teoritis, menunjukkan bahwa tujuan keamanan yang dijanjikan penydia jasa dapat dikompromikan. Alasan untuk itu adalah pada pembatasan hukum satu sisi melarang serangann tersebut, dan disisi lain bahwa serangan dijelaskan masih sangat kompleks. Namun baru-baru beberapa serangan telah diterbitkan, yang dikerahkan dilingkungan laboratorium dan menunjukkan bahwa karya teoritis adalah benar, dalam hal ini memberikan gambaran tentang serangan yang berbeda pada sistem keamanan GSM.

Serangan terhadap COMP128, adalah masih digunakan untuk kedua autentikasi dan sesi pembangkitan kunci. Jadi setiap serangan terhadap COMP128 segera akan diulas fitur dan keamanan GSM tersebut. Selanjutnya COMP128 tidak pernah mempublikasikan sehingga ada tidak ada *review* oleh masyarakat terkait kriptografi seperti keamanan lainnya yang terkait algoritma. *Goldberg* dan *Briceno* COMP128 mengungkapkan demikian menentukan kunci Ki rahasia dengan mengirimkan 160.000 angka acak melalui pembaca kartu SIM ke SIM dan mengamati SRES dikembalikan oleh SIM. Jumlah 160.000 tanggapan, tetapi pelaku dapat me-*mount* serangan sekitar delapan jam. Jumlah ini waktu untuk beberapa skenario yang ditentukan. Dampak dari serangan ini akan lebih tinggi. *Goldberg* dan *Briceno* menemukan, bahwa serangan yang sama juga dapat dilakukan melalui udara dengan dipalsukannya BTS. Ini berarti, bahwa penyerang bahkan tidak perlu memiliki akses fisik ke Kartu SIM untuk melakukan serangan. Selama serangan udara tentunya mengambil lebih

banyak waktu, tetapi yang 160.000 tanggapan tantangan yang dibutuhkan tidak perlu harus dikontrol dalam satu sesi, namun dapat dikumpulkan periode yang lebih lama. Pengukuran menunjukkan, bahwa selama serangan udara membutuhkan sekitar tiga belas jam SRES konstan. Hal ini wajar dikarenakan Ki tidak pernah berubah. Karena SIM tidak ada yang berbeda dari *smartcard* setiap kemungkinan serangan dibidang ini berdampak pada sistem keamanan GSM (Goldberg, Wagner, & Green, 1999).

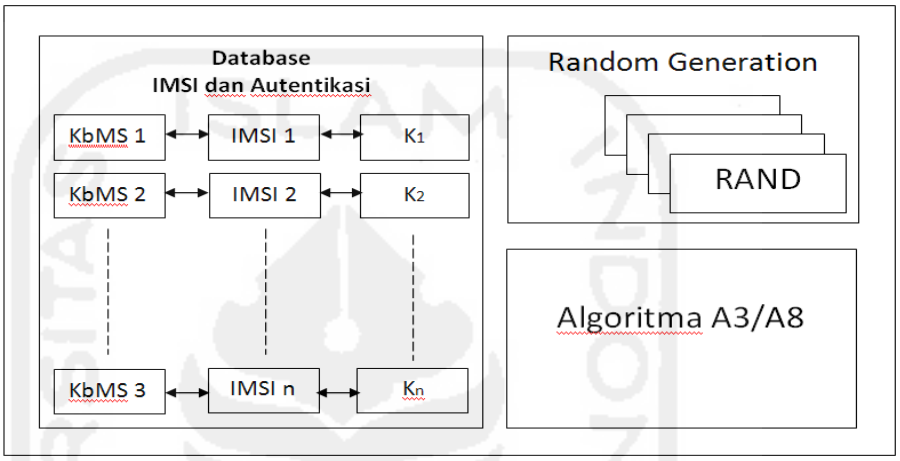
(R. Rao J. , Rohatgi, Scherzer, & Tinguely, 2002) menggambarkan bagaimana melalui serangan terhadap beberapa implementasi COMP128 kunci Ki rahasia dapat terungkap, dengan mengeksploitasi kerentanan dalam pelaksanaan tabel pencarian COMP128. Jumlah yang dibutuhkan permintaan untuk respon dari SIM tergantung pada bagaimana permintaan yang dipilih. Dampak dari serangan dijelaskan sangat besar, karena kunci rahasia Ki terungkap dan dengan setiap tindakan atau usaha pencegahan keamanan *simcard* yang memungkinkan untuk mengkloning kartu SIM.

2.6 Pentest Simcard Cloning

Kesan bahwa hampir mustahil untuk menyalin *simcard* ternyata dapat ditepis dengan sebuah penelitian terkait hal tersebut. *Simcard* identik dengan *Smartcard*, yaitu keamanan adalah bagian dari *simcard* itu sendiri walaupun keamanan mutlak tidak dapat diketahui, pertanyaannya adalah apakah biasa sejenis *simcard* atau disebut juga *smartcard* dikloning sedemikian rupa sehingga dapat merugikan otoritas pribadi milik pelanggan selullar.

Autentication key (disebut sebagai Ki dalam terminologi GSM), merupakan bagian dari IMSI dan nomor ESN Dari hal ini, hanya private key dan ‘Ki’ dilindungi serta terdapat pada kartu SIM. Sedangkan *Private Key* tidak pernah meninggalkan *simcard*. A3-algoritma yang digunakan sebagai algoritma *checksum*, setidaknya pelaksanaan dapat dikenal sebagai COMP128. Dengan test *trial-and-error*, dengan memberi inputan yang

berbeda untuk *simcard* dan mengamati respon, untuk selanjutnya ditambahkan pula database *public key* pelanggan (KbMS) yang digunakan Sehingga ketika proses autentikasi berlangsung, IMSI yang diterima oleh jaringan dikorelasikan dengan dua database yaitu Ki dan KbMS seperti tampak pada Gambar 2.7 (Montaque, 2001).



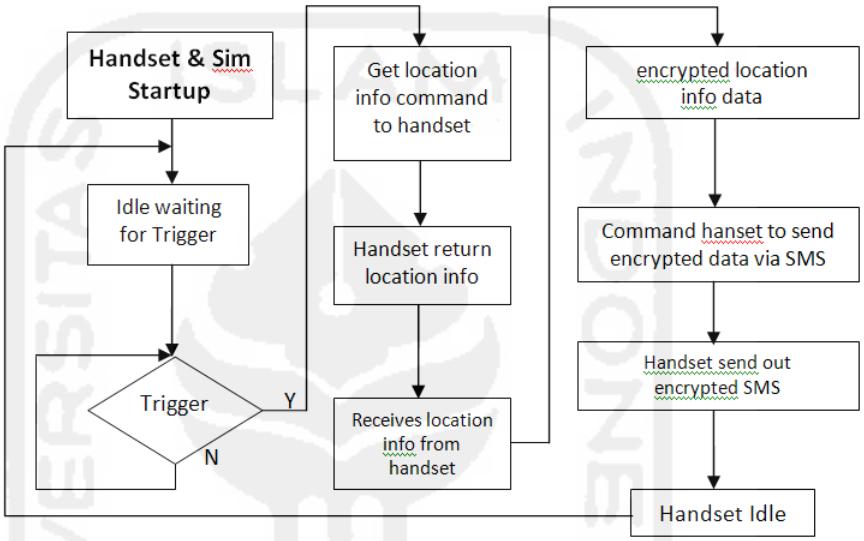
Gambar 2.7 Skema Pantest Simcard Cloning (Montaque, 2001).

A3 COM128 adalah algoritma dalam *simcard*, yang digunakan untuk mengenkripsi *simcard* terhadap piranti selullar, keduanya algoritma *checksum* merupakan hasil dari perhitungan KI A3 COM 128 dapat diperoleh dari :

1. Mengetahui respon terhadap jaringan selullar pasca *simcard* dikloning?
2. Bagaimana mengakumulasi autentikasi respon dan menghitung kunci enkripsi KI?
3. A3 COM128 dan A8 COM128. Apakah dapat memodifikasi algoritma atau hanya mendistribusikan kartu SIM diubah serta memodifikasi AUCs *(Authentication Center).* Apakah dilakukan secara *real* terhadap *simcard* asli dan hasil kloning?
4. Bagaimana lalu lintas dari ponsel pengguna ke *base station* bilamana *simcard* masih terenkripsi meskipun *simcard* telah dikloning?

2.7 Flowchart Pentest Simcard Cloning

(Agency, 2014) Flowchart Pentest dalam hal ini akan dijelaskan cara pengujian *simcard* sebagai barang bukti digital pasca terjadi *cloning* sehingga diketahui respon terhadap jaringan antara *simcard* asli terhadap *simcard* hasil *cloning* tampak seperti Gambar 2.8



Gambar 2.8 Flowchart Pantest Simcard Cloning (Agency, 2014)

Berdasarkan Gambar 2.8 diatas dapat disimpulkan bahwa penggunaan *simcard* dapat dilakukan saat *simcard* tersebut dalam status *idle* atau tidak digunakan, sehingga si pelaku dapa leluasa dalam mengakses *simcard* beserta kemampuannya identik dengan *simcard* asli. Pengujian tingkat keberhasilan *cloning* diketahui dengan memberikan *signal network* penyedia jasa telekomunikasi untuk selanjutnya mengetahui respon jaringan apakah berjalan sebagaimana *simcard* asli dalam memperoleh layanan baik panggilan *(call)*, pesan text (sms) dan akses data internet *(browsing)* ke penyedia layanan jaringan selular.