Studi dan Perbandingan Penggunaan Kriptografi Kunci Simetri dan Asimetri pada Telepon Selular

Ratih – NIM: 13503016

Program Studi Teknik Informatika, Institut Teknologi Bandung
Jl. Ganesha 10, Bandung

E-mail : if13016@students.if.itb.ac.id

Abstrak

Makalah ini berisi pembahasan mengenai kriptografi kunci simetri dan asimetri. Kriptografi kunci simetri merupakan salah satu metode kriptografi yang menggunakan kunci yang sama untuk proses enkripsi dan dekripsi, sedangkan kriptografi kunci asimetri atau kunci publik berarti menggunakan kunci yang berbeda untuk proses enkripsi dan dekripsi.

Pada makalah ini juga akan dibahas mengenai struktur keamanan jaringan telepon selular agar dapat memahami bagaimana kriptografi kunci simetri dan asimetri digunakan didalam pengamanan jaringan telepon selular, maupun pada beberapa aplikasi yang ada pada lingkungan selular.

Terakhir, makalah ini akan membandingkan antara kriptografi kunci simetri dan asimetri pada penggunaannya di telepon selular, khususnya pada Global System for Mobile Communications (GSM) untuk mengetahui metode mana yang secara umum lebih baik untuk diterapkan atau untuk mengetahui penerapan seperti apa yang akan memberikan jaminan keamanan lebih baik.

Dengan mempelajari mengenai penggunaan kriptografi kunci simetri dan asimetri pada telepon selular, diharapkan dapat lebih memahami bagaimana sesungguhnya cara kerja pengamanan jaringan komuniksi pada telepon selular. Memahami pula perbedaan penerapan kunci simetri dan asimetri dalam keamanan telepon selular dan pada aplikasi yang berada pada lingkungan selular. Selain itu diharapkan dapat memberi wawasan lebih atas penggunaan kunci simetri dan asimetri dalam kehidupan sehari-hari di dunia nyata.

Kata kunci: kriptografi simetri. kriptografi asimetri/ kunci publik, pengamanan telepon selular, GSM.

1. Pendahuluan

Penggunaan telepon selular dengan *Global System for Mobile Communications* (GSM) telah menjadi bagian yang tak terpisahkan dari kehidupan sehari-hari. Semula telepon selular hanya digunakan sebagai alat untuk berkomunikasi dengan orang lain melalui suara dan teks, namun saat ini kegunaan telepon selular telah berkembang dengan pesat. Telepon selular sudah dapat digunakan untuk mengakses internet dan berbagai aplikasi lainnya.

Pengamanan pada telepon selular berkembang pula seiring dengan perkembangan pada jaringan telepon selular. Meskipun demikian hanya sedikit orang yang menyadari pentingnya pengamanan pada jaringan telepon. Lebih sedikit lagi orang yang mengetahui dan memahami proses pengamanan jaringan telepon. Padahal hal ini merupakan salah satu aspek penting untukk diketahui oleh pengguna telepon selular.

Pendekatan klasik untuk memproteksi informasi yang ditransmisi adalah memberi akses kepada pengirim dan penerima kepada suatu kunci privat. Teknik ini disebut juga kriptografi kunci simetri. Namun, dalam kriptografi kunci simetri, terdapat masalah pengelolaan keamanan dari kunci privat yang tunggal.

Kunci privat harus didistribusikan pada kedua belah pihak, pengirim pesan dan penerima pesan. Mengirim kunci dari pengirim ke penerima melalui saluran publik tidak aman, karena ada kemungkinan kunci disadap selama proses transmisi dilakukan. Oleh karena itu, kunci harus dikirim melalui saluran kedua yang benar-benar aman atau bertemu pada tempat yang ditentukan untuk membagi kunci. Saluran kedua umumnya lambat dan mahal.

Untuk meningkatkan prosedur pengamanan kunci inilah kriptografi asimetri diperkenalkan pada tahun 1976 oleh Diffie dan Hellman. Kriptografi asimetri menggunakan dua kunci yang berbeda, masing-masing untuk enkripsi dan dekripsi. Hal ini memungkinkan pengguna

berkomunikasi secara aman tanpa perlu berbagi kunci rahasia. Nama lain kriptografi simetri adalah kunci publik, sebab kunci untuk enkripsi diumumkan kepada publik sehingga dapat diketahui oleh siapapun, sementara kunci untuk dekripsi hanya diketahui oleh penerima pesan.

Kedua metode inilah yang kemudian digunakan oleh jaringan telepon selular untuk keamanan. Metode mana yang digunakan biasanya tergantung dari penyedia jasa layanan tersebut.

Namun tentunya terdapat kelebihan dan kekurangan pada masing-masing metode kriptografi tersebut. Makalah ini akan mempelajari kelebihan dan kekurangan dari kedua metode tersebut dengan tujuan mengetahui metode mana yang lebih layak diterapkan pada pengamanan telepon selular atau cara seperti apa yang dapat dianggap sebagai penerapan yang optimal.

2. Pengamanan pada Telepon Selular

Pada jaringan internet, terdapat berbagai macam gangguan, antara lain:

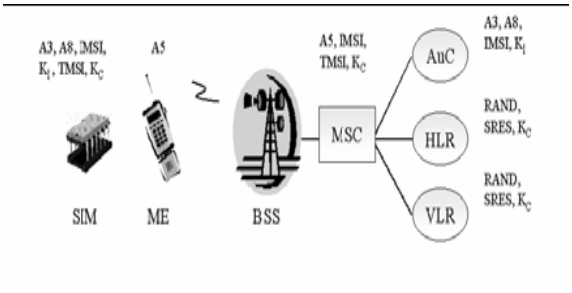
1. *eavesdropping*, kerahasiaan dari informasi terganggu, namun tidak terjadi perubahan pada informasi tersebut.
2. *Tampering*, informasi yang dikirim dirubah atau diganti oleh pihak lain dan kemudian dikirimkan kepada penerima pesan sehingga penerima pesan akan menerima pesan yang salah.
3. *Impersonation*, informasi yang dikirimkan berasal dari orang yang berpura-pura menjadi orang lain.

Dengan adanya kemajuan teknologi selular, internet dapat diakses melaui jaringan telepon selular. Oleh karena itu, seluruh ancaman keamanan yang terjadi pada internet dapat mengancam jaringan telepon selular.

Dibutuhkan pengamanan yang baik untuk menjaga pengguna telepon selular dari ancaman-ancaman tersebut.

2.1. Jaringan Telepon Selular

Sebelum membahas lebih lanjut mengenai pengamanan pada telepon selular, terlebih dahulu akan dijabarkan mengenai jaringan telepon selular agar lebih mudah untuk memahami istilah-istilah yang digunakan.



Gambar 1. Jaringan Telepon Selular

Keterangan singkatan pada gambar:
A3, A5, A8 : algoritma pengamanan
Kc : kunci enkripsi untuk sesi tersebut
Ki: kunci otentikasi individual
RAND: angka random / acak
ME: mobile equipment
BSS: base station subsystem
SIM: subscriber identity module
MSC: mobile service switching center
AuC: authentication center
VLR: visitor location register
HLR: home location register
IMSI, TMSI: international dan temporary mobile subscriber identities

Pada gambar diatas, *mobile station* (MS) berkomunikasi dengan *base station system* (BSS) melalui *radio interface.* BSS terhubung ke *network and switching subsystem* (NSS) dengan berkomunikasi dengan *mobile switching center* (MSC) melalui *A interface*.

MS terdiri dari dua bagian, *subscriber identity module* (SIM) dan *mobile equipment* (ME). SIM dilidungi oleh sebuah *personal identity number* (PIN) yang terdiri dari empat sampai delapan digit angka.

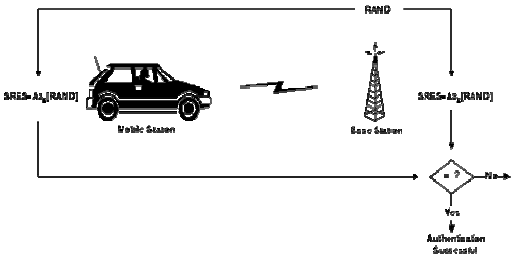
BSS menghubungkan MS dan NSS. BSS terdiri dari dua bagian, yaitu *base transceiver station* (BTS) dan *base station controller* (BSC). BTS terdiri dari *transmitter, receiver,* dan peralatan sinyal yang digunakan secara spesifik pada *radio interface* untuk menghubungi MS.

Bagian yang penting dari BTS adalah *transcoder/ rate adapter unit* (TRAU) yang menyimpan bahasa *encoding/ decoding* yang khusus untuk GSM dan *rate adaption* pada transmisi data. BSC menangani fungsi switching pada BSS, dan berkomunikasi dengan MSC pada NSS. Sebuah BSC dapat terhubung ke beberapa BTS dan menjaga konfigurasi *cell* pada BTS tersebut.

2.2. Keamanan pada Telepon Selular

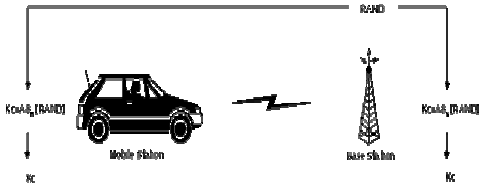
Pada dasarnya ada tiga area keamanan yang ditawarkan oleh GSM, yaitu:

1. Otentikasi pengguna.
   Berkaitan dengan kemampuan sebuah telepon selular untuk membuktikan bahwa ia memiliki akses untuk suatu akun dengan operator. Lebih jelasnya proses otentikasi, dapat dilihat pada gambar dibawah.



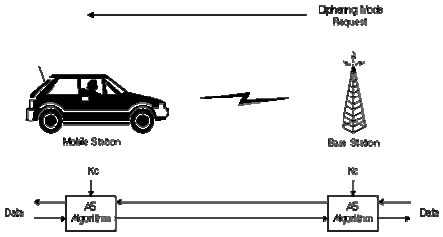
Gambar 2. Mekanisme Otentikasi GSM

2. Kerahasiaan data dan sinyal.
   Dibutuhkan untuk memastikan sinyal dan data pengguna (seperti pesan teks dan komunikasi suara) dilindungi dari penyadap dengan melakukan enkripsi.
   SIM menyimpan algoritma (A8) untuk membangkitkan kunci enkripsi 64-bit (Kc). Kunci enkripsi dihitung dengan menggunakan angka acak (RAND) yang sama dengan yang digunakan pada proses otentikasi untuk algoritma pembangkit kunci (A8) dengan kunci otentikasi individual pelanggan (Ki).
   Kc akan digunakan untuk melakukan enkripsi dan dekripsi data antara MS dan BS. Untuk meningkatkan keamanan, kunci enkripsi tersebut diubah-ubah, membuat sistem lebih resistan dari penyadap. Kunci enkripsi berubah sesuai dengan interval tertentu tergantung pada kebutuhan dan rancangan jaringan dan juga pertimbangan keamanan. Gambar dibawah akan menjelaskan perhitungan dari kunci enkripsi (Kc).



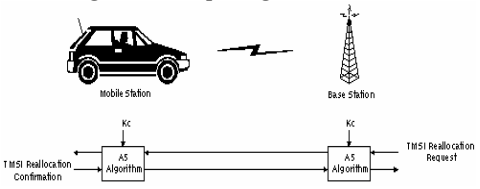
Gambar 3. Mekanisme Pembangkitan Kunci Enkripsi

Dengan cara yang sama seperti proses otentikasi, perhitungan kunci enkripsi (Kc) dilakukan didalam SIM. Oleh karena itu informasi yang dibutuhkan seperti kunci ontentikasi individual milik pelanggan (Ki) tidak boleh diperlihatkan oleh SIM.
Komunikasi suara dan data yang telah terenkripsi antara MS dan jaringan dilakukan oleh algoritma enkripsi A5. Komunikasi yang terenkripsi tersebut diinisialisasi oleh perintah permintaan mode enkripsi oleh jaringan GSM. Setelah menerima perintah ini, MS akan memulai enkripsi dan dekripsi data menggunakan algoritma enkripsi (A5) dan kunci enkripsi (Kc). Gambar dibawah ini akan menjelaskan mengenai mekanisme enkripsi.



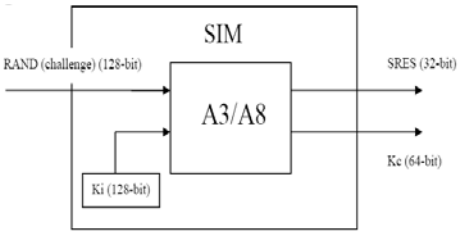
Gambar 4. Mekanisme Inisiasi Mode Enkripsi

3. Kerahasiaan pengguna.
   dibutuhkan untuk memastikan ketika jaringan menghubungi pelanggan tertentu, atau selama proses otentikasi, IMSI (*international mobile subscirber identity*) tidak diperlihatkan secara plainteks (tidak dienkripsi). Hal ini berarti jika seseorang menyadap komunikasi, ia tidak dapat mengetahui ada pengguna selular tertentu di suatu daerah.
   Untuk menjamin kerahasiaan identitas pelanggan, digunakan TMSI (Temporary Mobile Subscriber Identity). TMSI dikirimkan ke MS setelah prosedur otentikasi dan enkripsi selesai. Setelah menerima TMSI, MS akan memberikan konfirmasi penerimaan. TMSI valid untuk area lokasi yang ditentukan. Untuk komunikasi diluar area lokasi awal, selain TMSI dibutuhkan pula *Location Area Identification* (LAI).
   Proses lokasi dan realokasi TMSI digambarkan pada gambar dibawah ini.



Gambar 5. Mekanisme Realokasi TMSK

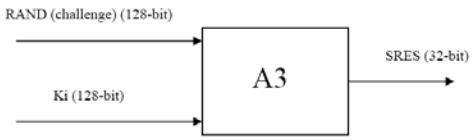
Untuk memenuhi keamanan tersebut diterapkan strategi pengamanan. Pengamanan pada telepon selular GSM terbagi menjadi dua bagian, yaitu otentikasi dan enkripsi. Otentikasi bertujuan mencegah akses yang tidak seharusnya dari tiap MS. Enkripsi digunakan untuk mencegah orang yang tidak berhak untuk turut mendapat informasi.
Lebih lengkapnya mengenai skema otentikasi dan enkripsi sistem GSM dapat dilihat pada lampiran.



Gambar 5. Konsep Otentikasi SIM

Gambar diatas menggambarkan konsep otentikasi pada SIM. Ki adalah ’akar’ dari kunci enkripsi. Ki merupakan angka 128-bit yang dibangkitkan secara acak yang dialokasikan untuk pelanggan tertentu yang menjadi ’bibit’ dari pembangkitan seluruh kunci yang digunakan dalam sistem GSM. Ki harus dilindungi, dan hanya diketahui oleh SIM dan AuC jaringan. Telepon itu sendiri tidak pernah mengetahui Ki, dan hanya memberikan SIM informasi yang dibutuhkan untuk melakukan otentikasi atau membangkitkan kunci untuk enkripsi. Proses otentikasi dan pembangkitan kunci dilakukan oleh SIM, hal ini mungkin karena SIM adalah alat yang dilengkapi dengan *microprocessor*.

Untuk menginisialisasi proses otentikasi, *home system* dari MS membangkitkan 128-bit angka acak yang disebut RAND. Angka ini dikirimkan kepada MS. Dengan menggunakan algoritma, A3, kedua belah pihak, Auc dan MS menggunakan Ki dan RAND untuk menghasilkan *signed result* (SRES). Lebih jelasnya dapat dilihat pada gambar dibawah.

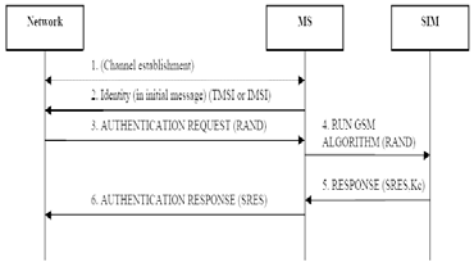


Gambar 6. Proses Komputasi SRES

RAND harus berbeda setiap waktu, karena jika tidak *attacker* dapat melakukan impersonasi dengan mengirimkan SRES yang sama.

SRES yang dibangkitkan oleh MS dikirimkan ke *home system* dan dibandingkan dengan SRES yang dibangkitkan oleh AuC. Jika ternyata tidak sama, permintaan akses akan ditolak. Pada dasarnya algoritma yang digunakan (dalam hal ini A3) tergantung pada penyedia jasa layanan.

Jika permintaan akses oleh MS diterima, sebuah kunci enkripsi Kc dibuat oleh sebuah algoritma, A8, dengan Ki dan RAND sebagai masukan. Algoritma yang digunakan juga tergantung dari jasa penyedia layanan. Setelah *home system* membangkitkan Kc, kunci enkripsi akan dikrimkan ke *visited system*. Kc dan *frame number* dari TDMA yang telah di-encode akan digunakan oleh algoritma A5, untuk melakukan enkripsi dan dekripsi data stream antara MS dan *visited system*.



Gambar 7. Skema Proses Otentikasi

Gambar diatas menerangkan prosedur otentikasi pada telepon selular.

1. Dibutuhkan koneksi antara telepon dan jaringan.
2. Telepon mendaftarkan identitasnya. Seluruh pesan yang ada pada awal koneksi berisi identitas. Jika mungkin, ia akan menghindari mengirimkan IMSI dalam bentuk plainteks.
3. Jaringan mengirimkan pesan *AUTHENTICATION REQUEST* yang berisi RAND.
4. Telepon menerima RAND, dan melewatkannya ke SIM, dalam perintah *RUN GSM ALGORITHM.*
5. SIM akan mengeksekusi algoritma A3 dan mengembalikan SRES ke telepon.
6. Telepon akan melakukan transimisi SRES ke jaringan melalui pesan *AUTHENTICATION RESPONSE.*
7. Jaringan akan membandingkan SRES yang dikirimkan dengan SRES nya sendiri. Jika cocok, transaksi dapat dilanjutkan.

Dengan pengamanan seperti diterangkan diatas, sistem keamanan GSM yang ada sekarang memiliki beberapa kelemahan, yaitu:

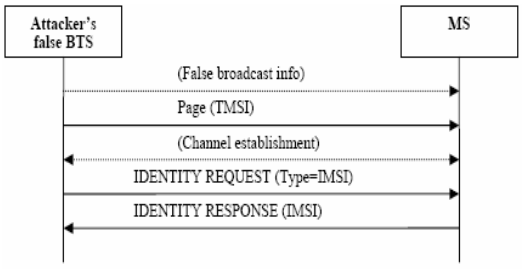
1. Kerahasiaan dari telepon dan pelanggan GSM hanya dijamin pada *radio channel* (interface udara) antara MS dengan BSS. Hal ini memungkinkan adanya penyadap data suara pada infrastruktur dari jaringan GSM (antara BSS dan MSC, HLR, VLR, AuC, dll).
2. Selama kunjungan *inter-domain* dari pelanggan GSM, beberapa parameter otentikasi, seperti kunci enkripsi, dikirimkan dari HLR kepada VLR dalam plainteks. Keamanan dalam komunikasi ini (HLR → ke VLR atau VLR → VLR) tergantung pada keamanan dari transportasi intermediate dari jaringan antara kedua *register* ini. Kebutuhan akan jaringan transportasi yang aman tidak dapat terpuaskan dalam skala yang besar atau global, karena lingkungan jaringan yang bervariasi.
3. Kerahasiaan identitas pengguna dilanggar dengan melakukan transmisi identitas pengguna (IMSI) dalam bentuk yang tidak terlindungi melalui media transportasi jaringan antar *register* GSM.
4. Sebagai tambahan dari 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. Orang yang tidak memiliki otorisasi akhirnya dapat memperoleh dan melalukan dekripsi dari saluran yang terenkripsi pada *radio channel* antara MS dan *base station.*
5. Algoritma keamanan dari GSM (A3, A5, dan A8) semuanya tidak dipublikasikan, algoritma rahasia. Peneliti telah melakukan *reverse-engineered* pada algoritma ini dan mereka telah membuktikan bahwa algoritma ini memiliki beberapa kekurangan dari segi keamanan yang cukup fatal.
6. Pada fase otentikasi GSM, dua parameter yang berhubungan, RAND dan SRES, ditransmisikan pada antarmuka udara dalam bentuk plainteks. Jadi siapapun ’pendengar’ dari antarmuka udara ini dapat melakukan *known plaintext attack* pada pasangan RAND-SRES untuk memperoleh kunci otentikasi.

Kelemahan lain yang tidak berhubungan dengan algoritma atau metode kriptografi namun berhubungan dengan mekanisme GSM antara lain:

1. Jaringan tidak melakukan otentikasi pada telepon
   Ini adalah kesalahan yang paling serius dengan sistem otentikasi GSM. Prosedur otentikasi yang dideskripsikan diatas tidak mengharuskan jaringan untuk membuktikan ia mengetahui Ki, atau otentikasi dalam konteks apapun pada telepon.
   Hal ini memungkinkan penyerang untuk menyiapkan *base station* palsu dengan *Mobile Network Code* yang sama dengan jaringan pelanggan. Karena inisiasi prosedur otentikasi diserahkan pada kerahasiaan jaringan, jaringan yang palsu mungkin saja memilih untuk tidak melakukan otentikasi sama sekali, atau hanya mengirimkan RAND dan mengacuhkan tanggapan yang diberikan. Jaringan yang palsu tidak perlu melakukan aktivasi enkripsi.
2. Umumnya, impelementasi dari A3/A8 memiliki kekurangan (*narrow pipe*).
   Impelementasi yang paling umum dari algoritma A3 dan A8 biasanya digabungkan pada satu algoritma, COMP128, yang akan membangkitkan kunci 64-bit, Kc, dan SRES 32-bit dari masukan 128-bit RAND dan 128-bit Ki.
   Algoritma seperti ini memiliki kelemahan yang cukup serius, yang terletak pada nilai masukan RAND yang dipilih secara hati-hati akan menyediakan informasi yang cukup untuk menentukan Ki dari kurang dari jumlah angka ideal percobaan (*brute force* dari nilai 2^{128}). Kelemahan ini ada karena pada putaran kedua dari algoritma, terjadi *narrow pipe* (seperti keluaran byte individual yang dikelompokkan menjadi grup-grup yang terdiri dari 4 byte pada putaran kedua hanya bergantung pada grup unik yang terdiri dari 4 byte masukan (dua diantaranya adalah Ki, dan dua lagi adalah RAND)) oleh karena itu *collision attack* dapat dilakukan.
3. Implementasi dari A3/A8 memiliki kekurangan-adanya pengurangan kekuatan kunci enkripsi Kc.
   Implementasi umum dari A3/A8, COMP128 memiliki ”kekurangan” lain, namun kekurangan ini lebih merupakan kekurangan yang disengaja.
   Ketika mebangkitkan Kc 64-bit, setidaknya 10 bit dari Kc akan selalu

diatur agar bernilai 0. Hal ini tentunya akan mengurangi kekuatan dari algoritma enkripsi data sampai 54 bit (pengurangan biasanya merupakan faktor dari 1024), tidak perduli algoritma enkripsi apa yang digunakan.
Pengurangan kekuatan yang disengaja ini juga ada pada algoritma yang dipilih, COMP128-2.

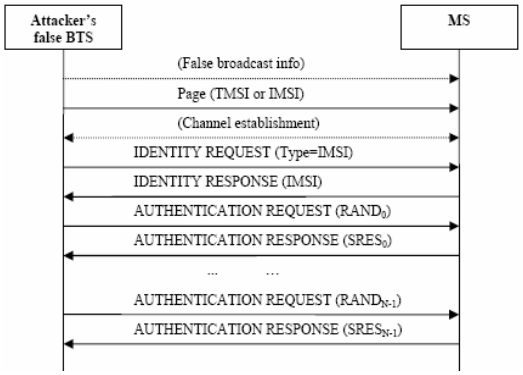
4. Kelemahan pada mekanisme kerahasiaan identitas pelanggan.
Seperti telah dijelaskan sebelumnya, spesifikasi GSM telah menghindari telepon dapat diacu atau diidentifikasi oleh dirinya sendiri pada plainteks melalui IMSI.
Hal ini seharusnya mencegah adanya penyadap yang mendengarkan pada tahap plainteks awal dari komunikasi radio untuk menyadari bahwa ada pelanggan tertentu pada area tersebut (dan apa yang mereka lakukan,jenis komunikasi yang dilakukan dapat diketahui pada saat sebelum enkripsi, seperti SMS, *Video call*, dll).
Oleh karena itu, jika jaringan dapat menghubungi penggunanya dengan TMSI dan menjaga basis data pada VLR agar dapat memetakan antara TMSI ke IMSI.
Jika jaringan tiba-tiba kehilangan jejak dari TMSI tertentu, dan karena itu tidak dapat menentukan siapa pengguna tersebut, jaringan harus meminta pada pengguna IMSI milik pengguna tersebut melalui koneksi radio, menggunakan mekanisme *IDENTITY REQUEST* dan *IDENTITY RESPONSE*.
Jelas saja, koneksi tidak dapat dienkripsi jika jaringan tidak memiliki informasi mengenai identitas pengguna, karena itulah IMSI harus dikirim dalam bentuk plainteks.



Gambar 8. Serangan Pemalsuan BTS

Jika digabungkan dengan kekurangan yang sebelumnya, jaringan tidak harus melakukan otentikasi pada telepon, seorang penyerang dapat menggunakan ini untuk memetakan TMSI kepada IMSI-nya. Penyerang dapat melakukan ini dengan cara menirukan *Base Station* yang sah dari jaringan pelanggan, dan menghubungi pelanggan tersebut melalui IMSI-nya. Pelanggan telepon kemudian akan melakukan koneksi radio, dan penyerang dapat dengan mudah mengirimkan pesan *IDENTITY REQUEST (Identity Type = IMSI)* pada pengguna, dan telepon kemudian akan menjawab dengan IMSI.

5. *Cracking* Ki melalui udara
Jika beberapa kekurangan diatas digabungkan, dapat menghasilkan serangan yang lebih serius lagi.
Dengan menirukan jaringan GSM yang sah, penyerang dapat menggunakan prosedur otentikasi beberapa kali dengan memanfaatkan kelemahan pada COMP128.
Untuk dapat melakukan ini, penyerang akan menirukan *Base Station* yang sah dengan kode jaringan selular yang sama dengan jaringan pelanggan. Setelah itu mengirim pesan kepada telepon selular, dapat melalui IMSI (atau TMSI), untuk melakukan koneksi radio kepada pelanggan.
Setelah koneksi berhasil dilakukan, jika telepon dihubungi melalui TMSI, IMSI dapat dengan mudah diketahui dengan mengirimkan pesan *IDENTITY REQUEST* kepada telepon, telepon harus membalas pesan tersebut.
Setelah itu, penyerang dapat menyimpan RAND yang telah dipilih dengan menggunakan kelemahan yang terdapat pada algoritma COMP128 dan mendaftarkannya pada telepon melalui pesan *AUTHENTICATION REQUEST* (menirukan jaringan yang sah meminta telepon untuk melakukan otentikasi). Telepon, sebagaimana seharusnya, akan mengembalikan SRES. Penyerang kemudian akan mengulangi permintaan otentikasi berulang kali, mengumpulkan SRES sampai ia memperoleh informasi yang cukup untuk mendapatkan Ki.
Setelah Ki dan IMSI diketahui, penyerang dapat menirukan pengguna, dan membuat dan menerima telepon dan SMS atas nama pengguna, atau bisa juga digunakan untuk menyadap telepon tersebut.
Serangan ini dapat dilakukan pada semua telepon GSM, tanpa adanya akses terlebih dahulu pada telepon (atau bahkan mengetahui IMSI), TMSI acak dapat diperoleh dengan memonitor saluran radio.



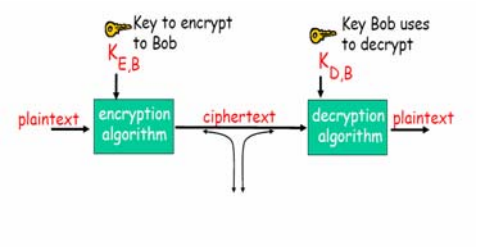
Gambar 9. Serangan Pemalsuan BTS (2)

6. Enkripsi yang dilakukan setelah FEC.
   pada sistem GSM, seperti semua sistem komunikasi dijital radio, *forward error correction* (FEC) digunakan pada jaringan radio untuk membantu koreksi dari *error* yang disebabkan gangguan atau sinyal yang lemah.
   FEC bekerja dengan cara menambahkan *redundancy* pada aliran data, maka menambahkan jumlah bit yang harus dikirimkan.
   Permasalahan pada GSM adalah enkripsi yang dilakukan setelah FEC, berarti aliran bit yang redundan tadi ikut di XOR ditambahkan pada aliran enkripsi, berarti pola *redundancy* yang telah diketahui dapat membantu untuk serangan kriptanalisis.
7. Kekurangan pada algoritma A5/1 dan A5/2
   Alex Biryukov, Adi Shamir dan David Wagner mendemonstrasikan bahwa algoritma A5/1 dapat dipecahkan dalam waktu kurang dari satu detik pada beberapa PC (namun dibutuhkan tabel besar yang telah dihitung sebelumnya, berjumlah sekitar 2^{36} byte atau 64 giga).
   Serangan ini mengeksploitasi kekurangan yang terdapat pada algoritma ketika menyimpan tabel ini menggunakan kombinasi apa yang telah dipelajari melalui analisis statistik dari status yang telah dilalui algoritma.
   A5/2 adalah versi yang dengan sengaja dibuat lebih lemah daripada A5/1, yang telah dibuktikan juga memiliki kelemahan.

3. Penerapan Kriptografi Kunci Simetri

3.1. Kriptografi Kunci Simetri

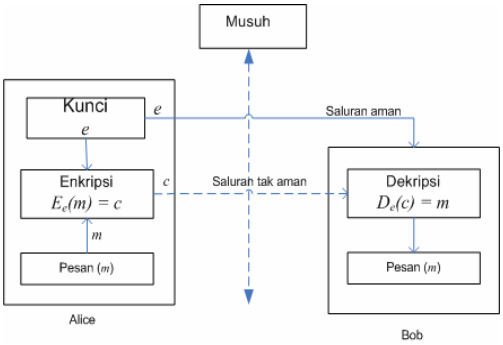
Kriptografi kunci simetri berarti menggunakan kunci yang sama untuk proses enkripsi maupun dekripsi. Pada prosesnya, pengirim pesan dan penerima pesan harus saling berbagi kunci rahasia tersebut.



Gambar 10. Skema Kriptografi Simetri

Pada gambar diatas, Alice ingin mengirim pesan pada Bob. Kunci yang digunakan Alice untuk mengenkripsi pesan yang akan dikirim sama dengan yang digunakan oleh Bob untuk mendekripsi pesan yang ia terima.

Proses pengiriman pesan berlangsung seperti yang tertera pada gambar, pertama-tama plainteks akan dienkripsi dengan kunci enkripsi menghasilkan cipherteks yang akan dikirimkan pada Bob. Cipherteks yang diterima oleh Bob akan didekripsi menggunakan kunci yang sama (Ke,b = Kd,b) atau seperti yang digambarkan oleh gambar dibawah ini.



Gambar 11. Komunikasi menggunakan Kriptografi Simetri

Algoritma simetri memiliki banyak macam, berdasarkan bit yang dienkripsi dapat dibagi menjadi dua kategori:

1. *Cipher* aliran (*stream cipher*). Algoritma kriptografi beroperasi pada plainteks/ cipherteks dalam bentuk bit tunggal, yang dalam hal ini rangkaian bit dienkripsikan/didekripsikan bit per bit.
2. *Cipher* blok (*block cipher*). Algoritma kriptografi beroperasi pada plainteks/ cipherteks dalam bentuk blok bit, yang dalam hal ini rangkaian bit dibagi menjadi blok-blok bit yang panjangnya sudah ditentukan sebelumnya. Misalnya panjang blok adalah 64 bit, maka itu

berarti algoritma enkripsi memperlakukan 8 karakter setiap kali penyandian (1 karakter = 8 bit falam pengkodean ASCII).

Pada *cipher* blok, rangkaian bit-bit plainteks dibagi menjadi blok-blok bit dengan panjang sama. Enkripsi dilakukan terhadap blok bit plainteks menggunakan bit-bit kunci (yang ukurannya sama dengan blok plainteks). Algoritma enkripsi menghasilkan blok cipherteks yang berukuran sama dengan blok plainteks. Dekripsi dilakukan dengan cara yang serupa seperti enkripsi.

Banyak algoritma yang memanfaatkan kunci simetri, yang telah banyak digunakan antara lain adalah DES (Data encryption Standard), rijndael, blowfish, IDEA, GOST, dll.

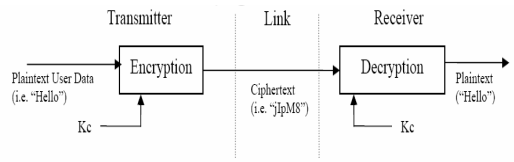
Kriptografi kunci simetri memang pada umumnya lebih mudah untuk diterapkan karena hanya menggunakan satu kunci. Algoritma yang digunakan pun sama, hanya membalikkan fungsinya saja. Namun pada kenyataannya kriptografi kunci simetri sulit untuk diterapkan pada pengiriman pesan, karena melibatkan distribusi kunci.

Pada aplikasi yang hanya melibatkan satu pihak, seperti enkripsi file untuk disimpan pada suatu komputer tentu tidak menjadi masalah, namun jika digunakan untuk menjaga keamanan jaringan yang melibatkan dua pihak atau lebih, hal ini dapat menimbulkan masalah.

Masalah keamanan kunci tentu dapat dijaga dengan menyediakan saluran khusus, namun hal ini menimbulkan masalah baru yaitu biaya. Saluran khusus tentunya mahal dan tidak efisien.

3.2. Kriptografi Kunci Simetri pada Telepon Selular

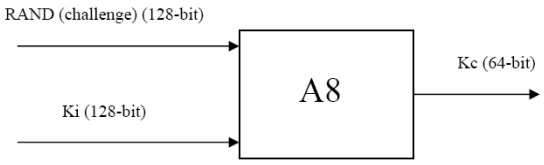
Selain proses otentikasi, jaringan juga melakukan enkripsi. Sistem GSM saat ini menggunakan kriptografi simetri untuk proses eknkripsi. Data yang dienkripsi menggunakan algoritma yang dibangkitkan dari kunci enkripsi, Kc. Kc juga yang dibutuhkan untuk melakukan dekripsi data oleh algoritma dekripsi.



Gambar 12. Proses Enkripsi

Gambar diatas menggambarkan konsep enkripsi pada jaringan telepon selular. Kc harus secara teratur berubah, untuk berjaga-jaga jika pada akhirnya Kc dapat ditebak. Metode untuk mendistribusikan Kc ke telepon terkait erat dengan prosedur otentikasi yang telah didiskusikan sebelumnya.

Kapanpun algoritma A3 dieksekusi (untuk membangkitkan SRES), algoritma A8 juga dieksekusi (pada kenyataannya SIM akan menjalankan keduanya secara bersamaan). Algoritma A8 menggunakan RAND dan Ki sebagai masukan untuk membangkitkan kunci enkripsi 64-bit, Kc, yang kemudian disimpan pada SIM dan dapat dibaca oleh telepon. Jaringan juga akan membangkitkan Kc dan mendistribusikannya ke BTS yang menangani koneksi.

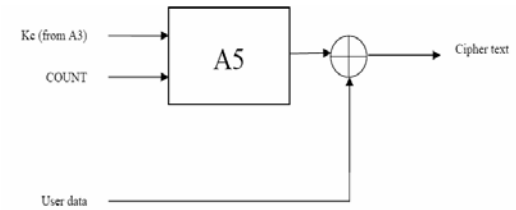


Gambar 13. Pembangkitan Kc

Kapanpun, jaringan dapat meminta telepon untuk memulai enkripsi data (setelah diotentikasi) menggunakan Kc yang telah dibangkitkan sebelumnya.

Jaringan dapat memilih beberapa algoritma untuk digunakan, selama telepon mendukung algoritma yang dipilih (hal ini diindikasikan kepada jaringan sebelumnya dalam pesan *classmark*, yang menjelaskan spesifikasi dari kemampuan telepon).

Algoritma enkripsi dijalankan dengan membangkitkan aliran dari data biner (*cipher block*), dimana modulo-2 ditambahkan (XOR) dengan data pengguna, untuk membuat teks yang terenkripsi yang ditransmisikan melalui udara. Data dapat dienkripsi dengan melakukan XOR pada data yang telah diterima dengan *cipher block*, dimana seharusnya sama dengan plainteks jika Kc yang digunakan sama.



Gambar 14. Enkripsi pada telepon

Algoritma yang digunakan juga berasal dari nilai COUNT, yang berasal dari angka frame TDMA, diterapkan secara sekuensial untuk setiap 4.615 ms frame GSM.

Selain penerapannya pada enkripsi pada system GSM, kunci simetri juga dikembangkan untuk suatu protocol jaringan selular yang dibahas secara lengkap pada [7].

4. Penerapan Kriptografi Kunci Asimetri

4.1. Kriptografi Kunci Asimetri

Kriptografi kunci simetri dibuat untuk menyelesaikan masalah distribusi kunci pada kriptografi kunci simetri. Kriptografi ini diusulkan oleh Diffie dan Hellman. Kriptografi kunci asimetri atau kunci publik menggunakan kunci yang berbeda untuk enkripsi dan dekripsi.

Kriptografi kunci publik menggunakan sepasang kunci kriptografi yang terhubung secara matematis. Jika kunci yang satu digunakan untuk enkripsi pesan, maka hanya kunci pasangannya yang dapat melakukan dekripsi terhadap pesan tersebut. Mengetahui salah satu kunci, bukan berarti dapat mengetahui kunci pasangannya dengan mudah.

Pada sistem kriptografi kunci publik terdapat:

1. Kunci publik.
   Kunci yang memang akan diumumkan pada publik. Kunci ini didistribusikan dengan bebas dan dapat dilihat oleh semua orang.
2. Kunci privat yang berhubungan (dan unik).
   Kunci ini merupakan kunci yang hanya diketahui oleh pemilik kunci. Tidak untuk didstribusikan kepada semua orang. Kunci privat dapat membuktikan bahwa seseorang merupakan orang yang benar-benar memiliki akses.

Kriptografi kunci publik dapat dianalogikan seperti kotak surat yang terkunci dan memiliki lubang untuk memasukkan surat. Kotak surat diletakkan di depan rumah pemiliknya. Setiap orang dapat memasukkan surat ke dalam kotak tersebut, tetapi hanya pemilik kotak yang dapat membuka kotak dan membaca surat didalamnya karena ia yang memiliki kuncinya.

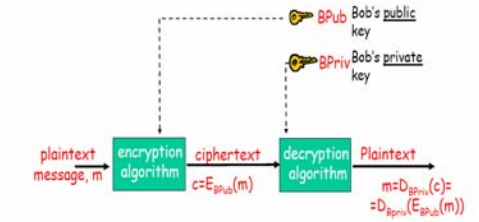
Keuntungan kriptografi kunci publik ada dua. Pertama, tidak ada kebutuhan untuk mendistribusikan kunci privat sebagaimana pada kriptografi kunci simetri. kunci publik dapat dikirim ke penerima melalui saluran yang sama dengan saluran yang digunakan untuk mengirim pesan. Perhatikan bahwa saluran untuk mengirim pesan umumnya tidak aman. Kedua, jumlah kunci dapat ditekan. Untuk berkomunikasi secara rahasia dengan banyak orang tidak perlu kunci rahasia sebanyak jumlah orang tersebut. Cukup membuat dua buah kunci, yaitu kunci publik bagi para koresponden untuk mengirim pesan, dan kunci privat untuk mendekripsi pesan. Berbeda dengan kriptografi kunci simetri dimana jumlah kunci yang dibuat adalah sebanyak jumlah pihak yang diajak berkorespondensi.

Jika kekuatan kriptografi kunci simetri terletak pada panjang kuncinya yang membutuhkan usaha sangat besar untuk menemukan kunci, maka kriptografi kunci publik kekuatannnya terletak pada sulitnya memecahkan masalah matematis seperti pemfaktoran dan logaritma diskrit. Kriptografi kunci publik mempunyai aplikasi yang lebih luas daripada kriptografi kunci simetri, yaitu menjaga kerahasiaan, otentikasi, dan pertukaran kunci.

Kriptografi kunci publik menyediakan jaminan keamanan dengan menyediakan cara untuk menjamin:

1. Enkripsi (*no eavesdropping*), memungkinkan penyembunyian informasi yang akan dikirimkan antara dua pihak. Pengirim pesan akan melakukan enkripsi sebelum pesan dikirimkan, dan penerima pesan harus melakukan dekripsi sebelum dapat membaca pesan tersebut. Informasi atau pesan yang dikirimkan tidak dapat diakses oleh pihak lain.
2. Integritas (*tamper detection*), memungkinkan penerima pesan untuk memastikan tidak ada pihak ketiga yang merubah pesan selama pesan dikirimkan.
3. Otentikasi, memungkinkan penerima pesan untuk memverifikasi asal pesan.
4. *Non-repudiation*, mencegah pengirim pesan untuk mengaku bahwa ia tidak pernah mengirimkan pesan tersebut.

Konsep kriptografi kunci publik sederhana. Seperti telah dijelaskan diatas, pada kriptografi kunci publik, setiap pengguna memiliki sepasang kunci, satu kunci untuk enkripsi dan satu kunci untuk dekripsi. Skema dibawah menggambarkan kriptografi kunci asimetri milik Bob.



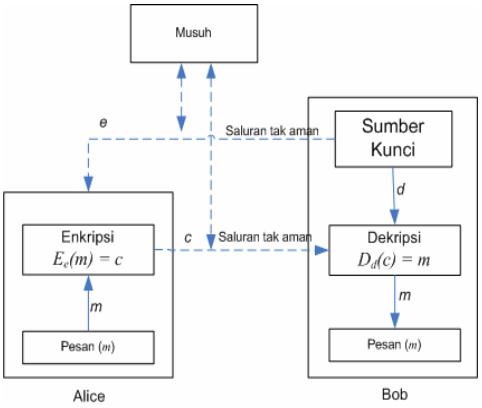
Gambar 15. Skema Kriptografi Asimetri

Misalkan E adalah fungsi enkripsi dan D adalah fungsi dekripsi. Misalkan (Bpub, Bpriv) adalah pasangan kunci untuk enkripsi dan dekripsi sedemikian sehingga

$$E_{Bpub}(m) = c \text{ dan } D_{Bpriv}(c) = m$$

Untuk suatu plainteks m dan cipherteks c. kedua persamaan ini menyiratkan bahwa dengan mengetahui e dan c, maka secara komputasi hamper tidak mungkin menemukan m. Asumsi lainnya, dengan mengetahui e, secara komputasi hampir tidak mungkin menurunkan d. Ee digambarkan sebagai pintu kolong *(trapdoor*) satu arah dengan d adalah informasi *trapdoor* yang diperlukan untuk menghitung fungsi inversinya, D, yang dalam hal ini membuat proses dekripsi dapat dilakukan.

Konsep diatas menjadi penting bila kriptografi kunci publik digunakan untuk mengamankan pertukaran pesan dari dua entitas yang berkomunikasi.



Gambar 16. Komunikasi menggunakan Kriptografi Asimetri

Gambar diatas memperlihatkan perbedaan mendasar sistem asimetri dengan sistem simetri. Bob mengirim kunci publik, e, untuk enkripsi kepada alice melalui saluran yang tidak perlu aman (*unsecure channel)*.

Aplikasi atau penerapan kriptografi kunci public dapat dibagi menjadi tiga bagian:

1. Kerahasiaan data
   Seperti pada kriptografi kunci simetri, kriptografi kunci publik dapat digunakan untuk menjaga kerahasiaan data (*provide confidentiality/ secrecy*) melalui mekanisme enkripsi dan dekripsi. Contoh algoritma untuk aplikasi ini adalah *RSA, Knapsack, Rabin, ElGamal, Elliptic Curve Cryptography* (ECC).
2. Tanda tangan digital
   Tanda-tangan digital (*digital signature*) dengan menggunakan algoritma kriptografi kunci-publik dapat digunakan untuk membuktikan otentikasi pesan maupun otentikasi pengirim (*provide authentication*). Contoh algoritmanya untuk aplikasi ini adalah RSA, DSA, dan ElGamal.
3. Pertukaran Kunci
   Algoritma kriptografi kunci-publik dapat digunakan untuk pengiriman kunci simetri (*session keys*). Contoh algoritmanya adalah RSA dan Diffie-Hellman.

Beberapa algoritma kriptografi kunci-publik dapat digunakan untuk ketiga macam kategori aplikasi (misalnya RSA), beberapa algoritma hanya ditujukan untuk aplikasi spesifik (misalnya DSA untuk *digital signature*).

4.2. Kriptografi kunci Asimetri pada Telepon Selular

Beberapa hal dibawah ini merupakan contoh penggunaan kriptografi kunci publik pada kasus lingkungan selular.

1. *Secure Browsing*
   Open Mobile Alliance (OMA, yang lebih dulu dikenal sebagai WAP Forum) telah melakukan spesifikasi versi *wireless* dari IETF *transport layer security* (protokol TLS), yang dikenal sebagai WTLS, untuk mengamankan *mobile browsing.* WTLS menyediakan saluran yang aman antara telepon selular dan *WAP gateway*, bagaimanapun, tidak dapat memenuhi kebutuhan untuk keamanan *end-to-end* pada jaringan data. Versi selanjutnya dari WAP (2.0) mengadopsi protokol TLS didalam spesifikasi WAP Transport Layer end-to-end Security. Protokol TLS memungkinkan kemanan end-to-end selama *browsing* internet dengan cara:
   a. memungkinkan *web server* dan *client* (telepon selular) untuk melakukan otentikasi satu sama lain dan membuat koneksi yang terenkripsi. Otentikasi menjadi bagian dari proses *handshake*, dimana kriptografi kunci publik digunakan untuk menyediakan

otentikasi yang mutual dan perjanjian pembagian kunci.

b. Ketika proses *handshake* telah berhasil, data aplikasi ditukarkan dengan aman melalui enkripsi kunci simetri menggunakan kunci yang telah dijanjikan.

2. Akses ke jaringan perusahaan (*enterprise network*)

   Salah satu keunggulan dari jaringan *wireless* 2,5 G dan 3G adalah memungkinkan peralatan selular untuk mengeksekusi aplikasi korporat, seperti *email*, pengiriman file, CRM, dan lain-lain. Hal ini meningkatkan kebutuhan akan aplikasi *client Virtual Private Network* (VPN) yang dapat menyediakan layer jaringan yang aman antara peralatan selular dan *corporate gateway* (atau server tujuan). *Client* VPN dapat diimplementasikan pada beberapa lapisan yang berbeda, dimana implementasi yang paling dominan adalah pada lapisan *internet protocol* (IP), menggunakan *IETF Internet Protocol Security* (IPsec). Ipsec melindungi pertukaran antara lapisan pada jaringan, menyediakan asal data otentikasi, kerahasiaan data, perlindungan *replay* dan integritas data. Ipsec menggunakan PKI sebagai bagian dari protokol *Internet Key Exchange* (IKE), yang memfasilitasi manajemen kunci otomatis. IKE menangani pertukaran parameter keamanan sebelum komunikasi diadakan. IKE juga memungkinkan server VPN untuk melakukan otentikasi pada peralatan selular menggunakan sertifikat pengguna. VPN telah menjadi motif yang kuat bagi perusahaan untuk membangun PKI yang bekerja sama dengan *certificate authority* (CA) untuk membentuk tanda-tangan dijital. Setelah infrasturktur ini ditempatkan untuk pengguna pada jarak jauh, tentunya dapat melayani pengguna pada jarak jauh secara *wireless* juga.

3. Otentikasi pembayaran secara *mobile*

   Kriptografi kunci publik dipertimbangkan sebagai arsitektur yang cocok untuk *mobile commerce* dan perbankan. Ilustrasi yang paling cocok untuk pernyataan ini adalah spesifikasi *Visa Three Domain Secure*(3-D Secure). Arsitekturnya berdasar pada kemampuan untuk melakukan otentikasi pada pemegang kartu pada jarak jauh dengan mekanisme yang telah ditentukan sebelumnya, dimana data yang dibutuhkan dikumpulkan selama proses enrolment berlangusng. Spesifikasi *3-D Secure Wireless Authentication Scenarios* memberikan beberapa metode otentikasi yang sesuai dengan lingkungan *wireless*, termasuk pembagian rahasia, tanda tangan, dan *biometric*. Skenario yang paling aman adalah tanda-tangan yang bergantung pada kriptografi kunci publik.

4. Kontrol untuk akses (*access control*)

   Telepon selular dengan kemampuan kriptografi kunci publik juga dapat digunakan sebagai alat otentikasi untuk sistem kontrol akses, berdasarkan mekanisme aksi-reaksi (*challenge-response*), dimana telepon menerima aksi dari *server* dan memberikan reaksi. Mekanisme seperti ini mungkin memang didasarkan pada penggunaan algoritma simetri atau asimetri. Algoritma simetri memerlukan inisialisasi dari telepon secara rahasia, spesifik untuk tiap aplikasi, yang kadang menjadi *impractical*. Kebalikan dari algoritma asimetri yang hanya membutuhkan *server* untuk memperoleh sertifikat pengguna untuk validasi tanda-tangan. Grup *Mobile Electronic Transaction* (MeT) mengerjakan protokol otentikasi lokal yang disebut *Personal Transaction Protocol* (PTP) yang memungkinkan pengguna untuk melakukan otentikasi sendiri pada lokasi retail, tempat pengumpulan tiket, *workstation*, dll. Menggunakan telepon selular.

5. Tanda-tangan dijital pada transaksi *mobile*

   Tanda tangan dijital membuat kriptografi kunci publik menjadi alat yang paling dapat digunakan untuk aplikasi sehari-hari, menjadi metode yang paling dapat diandalkan untuk otentikasi dan *non repudiation*. Tanda-tangan dijital diharapkan dapat menjadi dasar aplikasi bisnis pada telepon selular, karena tanda tangan dijital telah digunakan untuk menandatangani berbagai transaksi, digunakan pula dalam berbagai perbankan *online* dan aplikasi pembayaran.

   Konsep baru dalam transaksi selular adalah *actionable alerts*. *Actionable alerts* berarti ketika penyedia jasa selular mengirimkan pesan kepada pengguna telepon selular, pengguna telepon selular tersebut akan menanggapinya dengan *alert.* Versi yang aman dari aplikasi *actionable alerts*, berdasarkan pada tanda-tangan dijital dan enkripsi, memungkinkan bank untuk memfasilitasi platform selular untuk transaksi perbankan yang aman.

   Berdasarkan konsep tersebut, transaksi *procurement* yang lain, dapat diamankan dengan melibatkan tanda-tangan dijital, dimana pengguna telepon selular

menandatangani dokumen seperti kontrak, NDA, MOU, RFP, dll.

6. *Messaging*
   Kriptografi kunci publik juga dapat digunakan untuk mengamankan pesan selular lain, seperti *Short Message Service* (SMS) atau aplikasi *email wireless* menggunakan *S/MIME (Secure/ Multipurpose Internet Mail Extension)*, sebuah spesifikasi untuk pengiriman *email* yang aman dalam format MIME.
7. Otentikasi konten
   Penandaan kode (*Code Signing*) adalah teknologi yang penting dalam peralatan selular yang memungkinkan aplikasi untuk melakukan *download* melalui udara, seperti Java Applets. Hal ini diperlukan, untuk alat tersebut, sebagai penjamin keamanan dari kode yang di-*download*. Pemilik atau penyedia kode dapat menyediakan semacam jaminan dengan cara menanda-tangani secara dijital kode tersebut, dengan tanda-tangan dijital melalui XML, Java API, atau antarmuka lainnya. Telepon memegang salinan yang dapat dipercaya dari kunci publik orang yang menandatangani kode tersebut, untuk melakukan verifikasi tanda-tangan pada kode tersebut sebelum menggunakannya. Penandatanganan kode memang tidak bisa menjamin bahwa kode tersebut aman untuk digunakan, namun paling tidak dapat menjamin bahwa kode tersebut memang dibuat oleh orang yang menandatangani kode tersebut dan belum dimodifikasi oleh pihak lain yang tidak berhak.
8. ID dijital
   ID dijital mengidentifikasi pemegangnya untuk berbagai tujuan, seperti izin mengemudi (SIM), jaminan kesehatan, polis asuransi, dll. ID dijital diimplementasikan dalam bentuk *credentials* pengguna dan sertifikat yang berhubungan. ID dijital dibuat dan ditandatangani secara dijital oleh pihak berwajib yang berkaitan, tergantung pada tujuannya. Ketika digunakan untuk peralatan *wireless*, ID dijital tersimpan pada peralatan tersebut. Dan dapat dikirimkan (misalnya jika ingin mengganti peralatan selular), dapat pula menggunakan kartu, atau media perantara lainnya.
9. *Digital Rights Management* (DRM)
   Konten *multimedia* (musik, *e-book*, video, dll) didimpan, didistribusikan, dan dikonsumsi dengan niat dijital, sehingga timbul kebutuhan untuk manajemen *digital right* untuk melindungi hak hokum dari pemiliknya.
   Misalnya untuk protokol *end-to-end* dari distribusi data musik dari penyedianya, melalui alat pemutar (telepon selular), ke kartu penyimpanan, didefinisikan pada spesifikasi *Universal Distribution with Access Control-Media Base* (UDAC-MB), dan diadopsi oleh konsorsium musik keitaide. UDAC-MB menggunakan enkripsi dari *license key* yang *content specific*, untuk distribusi media, untuk dibaca pada alat yang berhubungan. UDAC-MB menggunakan kriptografi kunci publik untuk enkripsi perizinan (termasuk kunci untuk media yang dienkripsi), yang dilewatkan dari *server* perizinan untuk alat permutar. Kriptografi kunci publik memungkinkan pengiriman kunci secara aman, dimana kunci simetri tidak dapat diterapkan, karena ia membutuhkan seluruh *server* perizinan dan alat-alat pemutar untuk berbagi kunci rahasia (*secret key).*
   Asosiasi *MultiMediaCard* mengusulkan untuk mengadopsi *MultiMediaCard* (MMC) sebagai standard global dan terbuka untuk memori yang *removable* dan *non-volatile*. Spesifikasi MMC mendefinisikan antarmuka antara kartu (yang digunakan untuk penyimpanan) dan alat yang digunakan. *Secure MultiMediaCard* (Secure-MMC) merupakan MMC dengan fitur kriptografi yang ditambahkan, dan tempat penyimpanan yang aman untuk kunci, digunakan untuk mendukung manajemen hak dijital. Secure-MMC menggunakan kriptografi kunci-publik dengan tujuan untuk pengiriman perizinan konten yang aman, dan juga digunakan untuk skema pertukaran yang berbasis PKI. Telepon selular digunakan sebagai alat pemutar, membutuhkan ekstraksi konten perizinan secara asimetri dan kemudian mendekripsi isi dari konten untuk dimainkan secara simetri untuk pelanggan.

Selain penggunaan untuk aplikasi-aplikasi diatas, kriptografi kunci publik digunakan untuk otentikasi pada sistem telepon selular. Banyak penemuan atau algoritma baru yang memanfaatkan kriptografi berbasis kunci publik yang diajukan untuk membuat pengguna telepon selular lebih terjamin keamanannya.

5. Perbandingan Kriptografi Kunci Simetri dan Asimetri

Perbandingan mendasar antara kriptografi simetri dan asimetri dapat langsung dibandingkan tanpa menerapkannya.

Kelebihan kriptografi kunci simetri:

1. Algoritma kriptografi simetri dirancang sehingga proses enkripsi / dekripsi membutuhkan waktu yang singkat.
2. Ukuran kunci simetri relatif pendek. Algoritma kriptografi simetri dapat digunakan untuk membangkitkan bilangan acak.
3. Algoritma kriptografi simetri dapat disusun untuk menghasilkan cipher yang lebih kuat.
4. Otentikasi pengirim pesan langsung diketahui dari cipherteks yang diterima, kearena kunci hanya diketahui oleh pengirim dan penerima pesan saja.

Kelemahan kriptografi kunci simetri:

1. Kunci simetri harus dikirim melalui saluran yang aman. Kedua entitas yang berkomunikasi harus menjaga kerahasiaan kunci ini.
2. Kunci harus sering diubah, mungkin pada setiap sesi komunikasi.

Kelebihan kriptografi kunci publik:

1. Hanya kunci privat yang perlu dijaga kerahasiannya oleh setiap entitas yang berkomunikasi (tetapi, otentikasi kunci publik tetap harus terjamin). Tidak ada kebutuhan mengirim kunci privat sebagaimana pada kriptografi kunci simetri.
2. Pasangan kunci publik/ kunci privat tidak perlu diubah, bahkan dalam periode waktu yang panjang.
3. dapat digunakan untuk mengamankan pengiriman kunci simetri.
4. Beberapa algoritma kunci publik dapat digunakan untuk memberi tanda tangan digital pada pesan.

Kelemahan kriptografi kunci publik:

1. Enkripsi dan dekripsi data umumnya lebih lambat daripada sistem simetri, karena enkripsi dan dekripsi menggunakan bilangan yang lebih besar dan melibatkan operasi perpangkatan yang besar.
2. Ukuran cipherteks lebih besar daripada plainteks (bisa dua sampai empat kali ukuran plainteks).
3. Ukuran kunci relatif lebih besar daripada ukuran kunci simetri.
4. Karena kunci publik diketahui secara luas dan dapat digunakan setiap orang, maka cipherteks tidak memberikan informasi mengenai otentikasi pengirim.
5. Tidak ada algoritma kunci publik yang terbukti aman (sama seperti *block cipher*). Kebanyakan algortima mendasarkan keamanan pada sulitnya memecahkan persoalan-persoalan aritmetik (pemfaktoran, logaritmik, dsb) yang menjadi dasar pembangkitan kunci. Kriptografi kunci publik juga tidak aman dari serangan *man-in-the-middle-attack*. Orang di ”tengah” mengintersepsi komunikasi lalu berpura-pura sebagai salah satu pihak yang berkomunikasi untuk mengetahui informasi rahasia.

Selain kelebihan dan kekurangan dari masing-masing metode, pada penerapannya pada jaringan telepon selular, kedua metode juga memiliki kelebihan dan kekurangannya masing-masing. Bukan berarti dengan adanya kriptografi kunci-publik, kriptografi kunci privat dapat tergantikan.

Penggunaan kriptografi kunci privat dan kunci publik biasanya saling melengkapi agar mencapai hasil yang optimal.

Protokol keamanan berbasi kunci privat atau kunci simetri yang dideskripsikan pada [7], memiliki kelebihan dan kekurangan sebagai berikut:

1. Protokol yang ditawarkan tidak memberikan solusi untuk kerahasiaan panggilan telepon didalam infrastruktur padat dari jaringan selular.
2. Setelah otentikasi pertama dari pengguna telepon selular pada area VLR baru, disediakan sebuah identitas sementara dan berubah-ubah untuk dipakai. Hal ini melindungi kerahasiaan identitas pengguna kecuali pada saat pertama kali pengguna berinteraksi dengan domain yang asing.
3. Pada protocol yang ditawarkan, kunci rahasia milik pengguna disimpan pada jaringan asal (*home network*) seperti pada GSM.
4. Algoritma yang digunakan pada protokol ini dianggap sudah diterima dan dikenal, seperti DES dan MD5.

Protokol otentikasi dan pertukaran kunci dengan basis kriptografi kunci publik yang dideskripsikan pada [9] memiliki beberapa kelebihan dan kekurangan sebagai berikut:

1. *End-to-end privacy* antara dua pengguna telepon selular yang sedang berkomunikasi terlindungi.
2. Tidak ada protokol yang didefinisikan untuk melakukan komunikasi yang aman antara jaringan asal (*home network*) dan jaringan asing (*foreign network*) pusat otentikasi.
3. Sertifikat dijital yang didefinisikan pada protokol ini termasuk identitas pengguna dalam bentuk plainteks.
4. Karena sistem ini menggunakan teknik kriptografi kunci publik, tidak perlu menyimpan kunci privat dari pengguna pada basis data jaringan.
5. Protokol ini menggunakan algoritma yang telah diterima dan dikenal seperti DES dan MD5.
6. Solusi yang ditawarkan tidak mengikutsertakan asumsi apapun mengenai keamanan dari jaringan.

Untuk lebih jelasnya, berikut adalah perbandingan usulan penerapan kunci public dan kunci privat pada jaringan selular GSM:

Celah keamanan pada arsitektur GSM	Protokol berbasis kunci privat	Protokol berbasis kunci-publik
Kurangnya mekanisme enkripsi pada infrastruktur *fixed* pada jaringan GSM.	X	V
Kebergantungan keamanan pada media perantara pada jaringan antara pasangan VLR dan HLR.	V	X
Pelanggaran pada kerahasiaan identitas pengguna.	V	X
Penyimpanan informasi yang sensitif pada *register* jaringan.	X	V
Penggunaan dari algoritma yang tidak dipublikasikan.	V	V

Tabel 1. Perbandingan Keamanan Kriptografi Simetri dan Asimetri

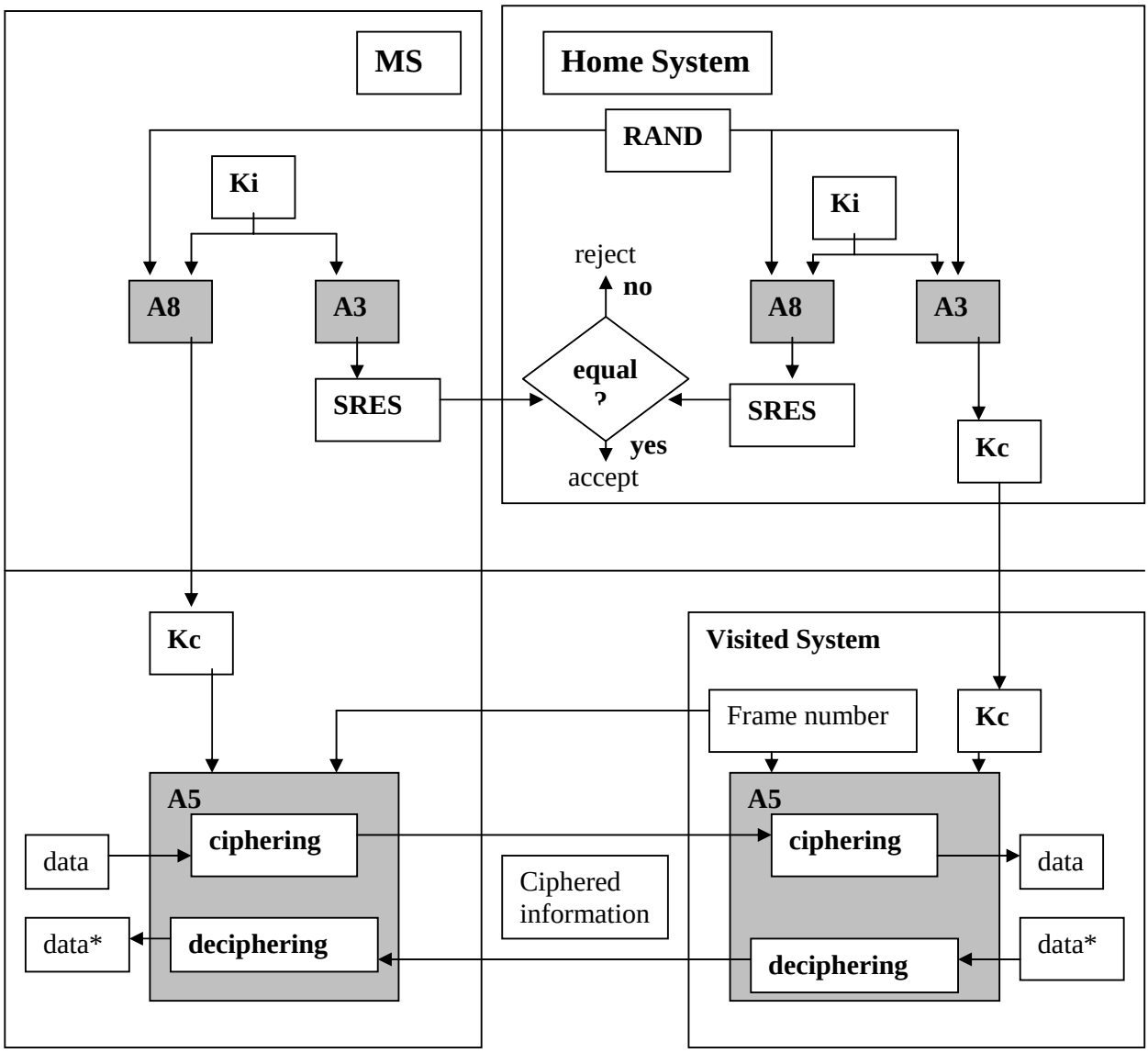
Keterangan:
V: menandakan adanya solusi dari celah keamanan.
X: menandakan tidak adanya solusi dari celah keamanan.

6. Kesimpulan

Kesimpulan yang dapat diambil dari pembahasan pada makalah ini adalah:

1. Penggunaan kriptografi kunci publik tidak dapat dikatakan telah menggantikan keberadaan kriptografi kunci simteri karena tetap saja ada beberapa macam aplikasi yang perlu atau lebih baik menggunakan kriptografi kunci simetri.
2. Penerapan kunci simetri pada telepon selular lebih kepada enkripsi data yang dikirimkan sementara penerapan kunci publik lebih kepada proses otentikasi.
3. Penerapan kunci simetri pada telepon selular tidak dapat diterapkan sendiri, karena pada umumnya digunakan perantara antara jaringan asal (*home network*) dan pusat otentikasi. Seluruh informasi yang sensitif dikirimkan dalam bentuk terenkripsi melalui perantara jaringan ini.
4. kriptografi kunci publik untuk distribusi kunci rahasia yang digunakan.
5. Penerapan yang paling baik adalah menggunakan keduanya, baik kriptografi kunci publik maupun kriptografi simetri. Keduanya saling melengkapi dan digunakan pada proses yang berbeda pada telepon selular.
6. Penerapan kriptografi kunci publik pada lingkungan selular amat banyak dan bermanfaat pula untuk menjaga hak pada konten multimedia dengan tanda-tangan dijital.

Lampiran


MS
Home System
RAND
Ki
Ki
reject
no
A8
A3
A8
A3
equal
?
SRES
SRES
Kc
yes
accept
Kc
Visited System
Frame number
Kc
A5
A5
ciphering
ciphering
data
data
Ciphered
information
data*
deciphering
deciphering
data*

Daftar Pustaka

[1] C. Park. (1997). On Certificate Based Security Protocols for Wireless Mobile Comm. Systems.

[2] Discretix (2002)
http://www.discretix.com
Tanggal akses: 21 November 2006 pukul 16.00

[3] Herzberg, Amir. (2001). Introduction to Network Security.

[4] Intro_pki.pdf
www.articsoft.com
Tanggal akses: 21 November 2006 pukul 16.30

[5] Li, Yi-Bing et al. (2001). Wireless and Mobile Network Architectures.

[6] Munir, Rinaldi. (2004). Bahan Kuliah IF5054 Kriptografi. Departemen Teknik Informatika, Institut Teknologi Bandung.

[7] R. Molva, et al. (1994). Authentication of Mobile Users.

[8] Wikipedia (2006)
http://www.wikipedia.org