Analisis Keamanan dan Penerapan Kriptografi pada Sistem *Keyless Entry* Mobil

Pradita Herdiansyah – NIM : 13504073 [1)]

1)Program Studi Teknik Informatika ITB, Jl. Ganesha 10, Bandung, email: if14073@students.if.itb.ac.id

Abstrak *– Kebutuhan akan kemudahan dan meningkatnya kualitas sistem keamanan yang dimiliki oleh kendaraan bermotor, khususnya mobil, telah mendorong para produsen mobil untuk menghasilkan sistem yang disebut keyless entry. Sistem ini berupa sebuah modul kunci yang memiliki transmitter untuk mengirim data kepada modul penerima yang terdapat di dalam mobil sehingga pertukaran data dapat terjadi dalam radius tertentu. Hal ini akan memudahkan pemilik mobil untuk memasuki mobilnya tanpa perlu membuka kunci, karena secara otomatis, dalam radius tersebut, kunci telah terbuka sendiri.*
Ditinjau dari segi keamanan, sistem keyless entry akan menolak untuk mengaktivasi seluruh sistem mobil jika modul kunci tidak terdapat dalam radius yang telah ditentukan. Sistem keyless entry memiliki pasangan yang unik antara satu modul kunci dengan satu modul penerima dalam mobil sehingga tidak memungkinkan terjadi kesalahan tertukarnya transfer informasi antar modul kunci dengan penerimanya pada 2 mobil yang sejenis. Informasi yang akan dipertukarkan secara wireless antara modul kunci dengan penerima di dalam mobil terlebih dahulu dienkripsi dengan menggunakan algoritma KeeLoq. Algoritma ini yang banyak digunakan oleh produsen mobil dalam aplikasi keyless entry pada produk mobil mereka. Namun, meski informasi yang akan dipertukaran telah dienkripsi dengan algoritma KeeLoq tersebut, media transmisi wireless memungkinkan para kriptanalis melakukan kriptanalisis untuk menemukan kunci pada informasi tersebut..

Kata Kunci*:Keyless entry, KeeLoq.*

1. PENDAHULUAN

Perkembangan dunia otomotif dapat diamati dengan munculnya berbagai inovasi yang diaplikasikan pada sebuah mobil. Berbagai fitur yang mungkin tidak terpikirkan sebelumnya sudah mulai banyak diaplikasikan pada berbagai mobil yang dipasarkan kepada masyarakat luas di seluruh dunia. Contoh fitur-fitur inovaif tersebut antara lain *antilock braking system*, *adaptive leveling suspension*, *intelligence key system*, dan lain sebagainya.

Intellegence key system mengizinkan pemilik mobil untuk melakukan personalisasi seluruh setting atau pengaturan yang terdapat pada mobilnya. Pengaturan tersebut dapat dipanggil kembali dengan menggunakan sebuah kunci khusus. *Intelligence key* dalam taraf sederhana biasanya hanya memuat sistem untuk akses ke dalam mobil tanpa kunci yang biasa disebut dengan *keyless entry system*.

Keyless entry system merupakan sistem yang difokuskan pada keamanan dan kenyamanan pemilik mobil sehingga untuk memasuki mobil cukup membuka tuas pintu saja karena dalam radius tertentu, sistem ini akan membuka kunci pintu mobil secara otomatis. Sistem ini sudah mulai banyak digunakan oleh para produsen mobil di dunia dengan menggunakan dasar algoritma KeeLoq.

Belakangan ini, *keyless entry system* sudah tidak sepenuhnya lagi aman karena para kriptografer telah mampu melakukan penyadapan pada data yang ditransmisikan antara modul kunci dengan modul yang terdapat di dalam mobil. Data yang ditransmisikan tersebut disadap dan dianalisis oleh kriptografer sehingga para kriptografer dapat menemukan kunci yang tepat untuk mendekripsinya. Lebih lanjut, kunci yang ditemukan tersebut akan dapat digunakan untuk membangun sebuah sistem modul kunci palsu yang dapat digunakan untuk membuka kunci pintu mobil yang transmisi datanya telah disadap sebelumnya.

Algoritma KeeLoq yang digunakan oleh sebagian besar produsen mobil di dunia perlu mengalami modifikasi atau bahkan diganti untuk meningkatkan keamanan pada *keyless entry system* yang akan digunakan di kemudian hari.

2. LANDASAN TEORI

2.1. Keyless Entry System

Keyless entry merupakan suatu sistem yang memberikan kemudahan bagi pemilik mobil untuk dapat masuk ke dalam mobilnya tanpa perlu membuka kunci seperti pada umumnya mobil yang beredar selama ini. Sistem ini dapat dikatakan sebagai pengembangan dari sistem alarm mobil yang juga sudah banyak digunakan oleh masyarakat pada umumnya.

Cara kerja alarm mobil konvensional adalah transmisi sinyal dari modul kunci yang dipegang oleh pemilik mobil dikirimkan kepada modul alarm yang terpasang

di dalam mobil. Proses transmisi yang terjadi dipicu oleh aksi dari pemilik mobil yang menekan tombol yang terdapat pada modul kunci yang dipegang bersama kunci mobilnya. Informasi dari modul kunci ditransmisikan pada frekuensi tertentu yang telah diatur sehingga modul kunci dengan modul di dalam mobil berada pada frekuensi yang sama.

Keyless entry memiliki cara kerja yang kurang lebih sama dengan cara kerja alarm seperti pada umumnya. Kelebihannya, terletak pada modul kunci yang dipegang oleh pemilik mobil selalu mentransmisikan gelombang pada frekuensi tertentu. Jika seseorang membawa modul kuncinya mendekati mobilnya dalam radius tertentu yang terjangkau oleh modul sistem yang terdapat di dalam mobil, maka data yang ditransmisikan oleh modul kunci akan dapat diterima oleh modul di dalam mobil sehingga kunci mobil akan terbuka dengan sendirinya. Sebaliknya, jika pemilik mobil meninggalkan mobilnya tanpa mengunci pintu terlebih dahulu, maka pada radius jarak tertentu pemilik beserta modul kuncinya menjauhi mobilnya, kunci mobil akan terkunci dengan sendirinya.

Proses transmisi data yang dikirimkan dari modul kunci kepada modul penerima yang terdapat di dalam mobil dienkripsi terlebih dahulu. Sesampainya di modul penerima yang terdapat di dalam mobil, data yang terenkripsi akan didekripsi kembali sehngga proses verifikasi autentifikasi data dapat dilakukan. Apabila proses dekripsi menghasilkan kesesuaian antara modul kunci dengan modul di dalam mobil, maka aksi lanjutan yakni membuka kunci mobil dapat dilakukan oleh sistem. Setiap mobil memiliki pasangan yang unik dengan modul kunci yang disertakannya di dalam penjualan sehingga meskipun ada dua atau lebih mobil dengan tipe yang sama persis, tidak dapat saling bertukar kunci antara satu dengan yang lainnya. Oleh karena itu, setiap terjadi kehilangan atau kerusakan pada modul kunci sistem *keyless entry*, pemilik mobil harus segera menghubungi dealer terdekat untuk melakukan reset ulang pada modul kunci maupun modul pada mobilnya sehingga kunci yang digunakan tetap sesuai dan tetap unik antar 1 mobil dengan mobil lain yang sejenis di dunia.

2.2. Algoritma KeeLoq

KeeLoq merupakan algoritma kriptografi yang digunakan oleh sebagian besar produsen mobil yang menggunakan sistem *keyless entry* sebagai fitur pada mobil-mobil yang dihasilkan dan dijual kepada masyarakat. KeeLoq merupakan algoritma kriptografi yang berbasis cipherblock. Algoritma ini ditemukan oleh Willem Smit, PhD yang bekerja di Nanoteq Pty Ltd (Afrika Selatan) di pertengahan tahun 1980-an. Algoritma tersebut dijual kepada Microchip Technology Inc. pada tahun 1995. Microchip Technology inilah yang mendistribusikan teknologi *keyless entry* dengan algoritma KeeLoq tersebut sehingga banyak digunakan oleh para produsen mobil di dunia. Produsen tersebut antara lain Chrysler, Daewoo, Fiat, GM, Honda, Toyota, Volvo, dan lain sebagainya.

Enkripsi pada algoritma KeeLoq dilakukan pada setiap 32-bit blok plainteks untuk menghasilkan 32-bit kode acak yang disebut *hopping code*. Initialization vector sebesar 32-bit ditambahkan dengan metode XOR pada tiap-tiap blok yang dieksekusi. KeeLoq cipher menerima kunci 64 bit dan melakukan enkripsi tiap blok 32 bit dengan mengeksekusi tiap-tiap bit tunggalsebanyak 528 putaran.

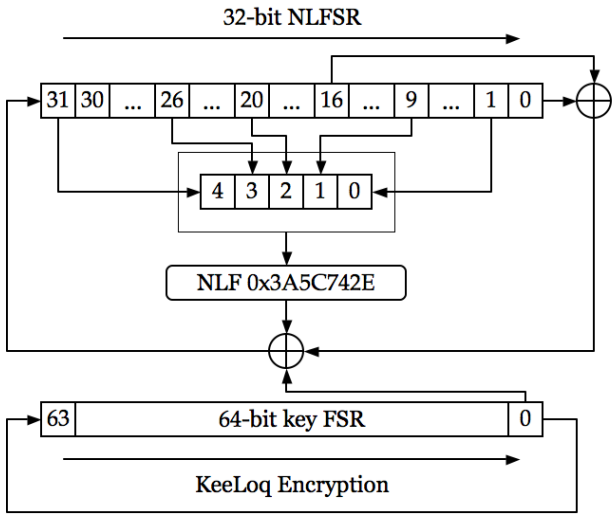
Jika setiap blok plainteks tersebut dibagi menjadi 5 bagian (sebut saja A,B,C, D, E), maka dapat dikatakan fungsi dekripsi dan enkripsi yang digunakan adalah sebagai berikut:

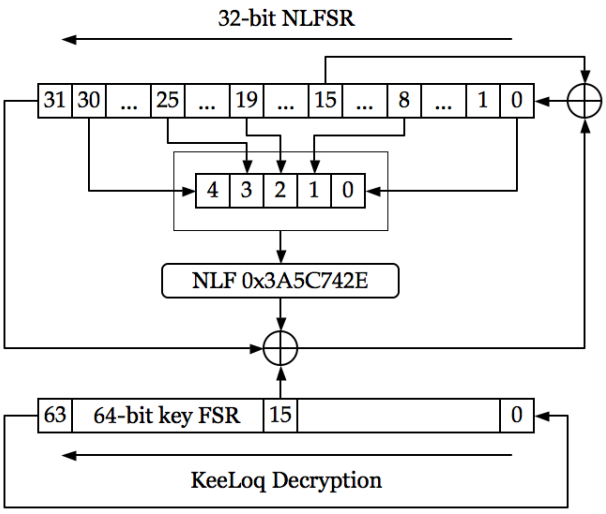
F(A,B,C,D) : D xor E xor AC xor AE xor BC xor BE xor CD xor DE xor ADE xor ACE xor ABD xor ABC

Input tiap bagian untuk enkripsi adalah bit ke-1, ke-9, ke-20, ke-26, dank e-31

Input tiap bagian untuk dekripsi adalah bit ke-0, ke-8, ke-19, ke-25, dan ke-30

Output yang dihasilkan dikombinasikan (xor) dengan bit ke 0 dan 16 untuk enkripsi, dan bit ke 31 dan 15 untuk dekripsi.





3. HASIL DAN PEMBAHASAN

3.1. Analisis Keamanan Keyless Entry System dengan Algoritma KeeLoq

Para kriptanalis (dalam konteks ini mungkin bisa disebut sebagai para pencuri mobil) menangkap transmisi komunikasi data yang terjadi antara modul kunci dengan modul yang terdapat di dalam mobil. Sebagaimana layaknya prinsip kriptografi pada umumnya, data atau pesan yang dikirimkan dari modul kunci ke modul penerima yang ada di dalam mobil sudah diacak menjadi cipherteks menggunakan suatu kunci dengan algoritma KeeLoq tersebut. Apabila data yang ditransmisikan didapatkan oleh kriptanalis dan kriptanalis mencoba mencari kemungkinan kunci yang sesuai secara *brute force*, maka ada sekitar 18 milyar kunci yang mungkin digunakan untuk sebuah pasangan mobil dengan kuncinya. Produsen mobil akan memberikan kunci yang berbeda pada setiap mobil yang dihasilkannya yang menggunakan *keyless entry*. Jumlah sebanyak 18 milyar tersebut diperkirakan tidak akan terlampaui oleh jumlah produksi mobil di dunia yang sama jenisnya sehingga dapat dipsatikan bahwa setiap mobil yang sama jenisnya memiliki kunci yang unik pada sistem *keyless entry* yang dimilikinya. Demikian pula dengan kemungkinan reset atau generating kunci baru untuk berbagai kasus yang mungkin terjadi seperti pemilik kehilangan kunci mobilnya atau kunci mobil yang juga menjadi modul *keyless entry* tersebut mengalami kerusakan. Sekali kriptanalis berhasil menemukan kunci untuk dekripsi pada suatu mobil, maka kriptanalis dapat berpura-pura sebagai pemilik mobil dan membuka kunci mobil tanpa merusaknya sedikitpun.

3.2. Modifikasi yang Mungkin Dilakukan Terhadap Aplikasi Keyless Entry dengan Menggunakan Algoritma KeeLoq

1. Menerapkan batasan toleransi kesalahan request. Analogi yang digunakan serupa dengan batasan request yang biasa diterapkan pada beberapa homepage yang memerlukan username dan password untuk autentifikasi. Pada umumnya, jika pengunjung web memasukkan pasangan username dan password yang salah sebanyak, misalnya, 3 kali, maka pengunjung tersebut tidak dapat melakukan autentifikasi kembali dalam rentang waktu tertentu, misalnya setengah jam.

   Metode ini sepertinya dapat diaplikasikan pada sistem *keyless entry* sehingga para kriptanalis yang mencoba memecahkan kunci enkripsi-dekripsi yang digunakan pada sebuah mobil dapat terhambat. Kriptanalis mau tidak mau harus menghentikan seluruh kegiatannya selama durasi yang ditentukan karena modul yang teradapat di dalam mobil tidak mengirimkan sinyal request apapun selama beberapa waktu demi alasan keamanan tersebut.

   Pemilik kendaraan yang sebenarnya, seharusnya tidak mengalami halangan apapun dalam membuka kunci mobilnya. Modul kunci resmi yang dimiliki oleh pemilik yang sebenarnya akan selalu mengirimkan data yang tepat dan sesuai dengan request yang dikirimkan oleh modul yang terdapat di dalam mobil. Jika ternyata pengguna tidak dapat membuka kunci mobilnya dengan menggunakan kunci sebenarnya yang dimilikinya, maka hal itu dapat dijadikan indikasi awal. Indikasi bahwa telah terjadi penyusupan pada sistem *keyless entry* pada mobilnya, dengan catatan seluruh komponen penunjang sistem tersebut berjalan dengan baik dan normal. Komponen pendukung itu antara lain sumber daya (baterai) pada masing-masing modul yang digunakan dalam keadaan normal.

2. Peningkatan keamanan yang mungkin dilakukan pada kinerja sistem *keyless entry* dapat memanfaatkan request-respon pencocokan ID yang dilakukan antara modul yang terdapat di dalam mobil dengan modul yang terdapat pada kunci yang dibawa oleh pemilik mobil.

   Sistem *keyless entry* yang saat ini ada bekerja dengan metode yakni ketika pengguna beserta modul kunci yang dimilikinya berada dalam radius tertentu yang dapat dijangkau oleh modul yang terdapat di dalam mobil, maka transmisi data antara kedua modul langsung terjadi. Prinsip pencocokan ID diusulkan agar proses transmisi data tdak langsung dilakukan setiap kali ada respon yang dikirimkan dari

modul kunci yang dimiliki pemilik mobil untuk menjawab request yang dikirimkan oleh modul yang ada di dalam mobil.

Proses pencocokan ID diawali dengan transmisi ID oleh modul dalam mobil dalam setiap request yang dilakukan. Modul kunci kemudaian akan mencocokkan dengan ID yang tersimpan di dalam memori modul kunci, apabila sesuai, maka pengiriman data dari modul kunci dapat dilakukan, sebaliknya, jika ID yang dikirimkan tidak sesuai, maka data tidak dikirimkan. ID yang dimiliki setiap kendaraan yang sama jenisnya sekalipun juga dapat dibedakan antara satu dengan yang lainnya.

Untuk mencegah kriptanalis mendapatkan ID yang dikirimkan oleh modul yang berada di dalam mobil setiap awal request, perlu dilakukan penanganan tersendiri. Ada 2 buah ID berbeda yang dikirimkan dalam 2 format yang berbeda pula. ID pertama dikirimkan dalam format painteks dan ID yang kedua dikirimkan dalam bentuk cipherteks yang hasil enkripsi dengan bilangan acak. Bilangan acak yang digunakan dapat memanfaatkan metode pembangkitan bilangan acak yang sesuai. Modul kunci yang menerima request dari modul yang ada di dalam mobil melakukan pencocokan terlebih dahulu terhadap ID pertama yang dalam bentuk plainteks. Apabila ID plainteks yang dikirimkan sesuai dengan ID pertama yang dimiliki modul kunci yang tersimpan dalam memori modul kunci, maka modul kunci mulai melakukan dekripsi terhadap cipherteks yang dikirimkan kepadanya. Jika hasil dekripsi cipherteks juga sesuai dengan ID kedua yang dimiliki modul kunci, maka modul kunci baru mengirimkan data kepada modul penerima yang ada di dalam mobil dengan menggunakan kunci yang berbeda. Dengan metode tambahan respon-request di awal transmisi data diharapkan akan menyulitkan kinerja kriptanalis karena harus mencari tahu terlebih dahulu ID yang digunakan dalam komunikasi data antara kedua modul. Apabila ID tersebut tidak dapat ditemukan oleh kriptanalis, maka modul penerima yang terdapat di dalam mobil tidak menerima informasi autentifikasi yang tepat mengenai modul kunci yang seharusnya berkomunikasi dan bertukar data dengannya. Secara otomatis, transmisi data lebih anjut tidak dapat terjadi.

3. Untuk mempersulit kinerja kriptanalis, sebenarnya pesan atau kunci yang dikirimkan bisa ditingkatkan ukurannya sehingga lebih panjang. Namun, hal ini sepertinya bukan suatu cara yang baik karena penyimpanan pesan dalam ukuran besar pada modul kunci maupun modul dalam mobil membutuhkan memori dan sumber daya yang lebih besar. Selain itu, semakin panjang bit-bit yang digunakan, maka waktu yang dibutuhkan untuk proses autentifikasi sebelum membuka kunci pintu membutuhkan waktuyang lebih lama. Hal ini akan membawa dampak pada kenyamanan pengguna dalam berinteraksi dengan mobilnya.

4. KESIMPULAN

Sistem *keyless entry* merupakan sistem yang membantu pemiliknya agar lebih nyaman dalam berinteraksi dengn mobilnya karena tidak lagi perlu membuka kunci pintu secara knvensional. Untuk membuka dan mengunci pintunya, pemilikm beserta modul kunci mobilnya cukup mendekat dan menjauh dari radus tertentu sehingga terjadi transmisi data antara modul kunci yang dibawa pemilik dengan modul penerima yang terdapat di dalam mobil.

Sistem *keyless entry* yang banyak beredar saat ini umumnya menggunakan algoritma KeeLoq yang telah ditemukan pada tahun 1980-an. Kelemahan sistem *keyless entry* terletak pada transmisi data yang terjadi secara *wirelesss* dapat disadap oleh para kriptanalis dan algoritma KeeLoq yang digunakan akan dapat dicari kunci enkripsi-dekripsinya.

Usulan yang mungkin dilakukan untuk meningkatkan keamanan sistem *keyless entry* dengan menggunakan algoritma KeeLoq antara lain:

1. Menerapkan batas toleransi kesalahan pada request sehingga kriptanalis yang mencoba untuk menggunakan kunci yang salah akan terhambat. Penerapannya misalnya setiap respon yang diberikan oleh modul kunci mengalami kesalahan 3 kali berturut-turut akan terjadi kondisi *no response* dimana modul penerima di dalam mobil tidak mau menerima respon apapun dalam waktu, misalnya, 15 menit.
2. Penggunaan metode request respon dengan ID ganda dengan format ID ysng berbeda yaitu plainteks dan cipherteks yang dienkripsi dengan bilangan acak.
3. Memperpanjang pesan atau kunci yang digunakan. Namun hal ini akan membawa dampak pada performansi sistem secara umum karena membutuhkan sumberdaya (baterai, memori) dan waktu proses yang lebih besar.

DAFTAR REFERENSI

[1] Munir, Rinaldi, *Diktat Kuliah IF5054 Kriptografi*, Sekolah Teknik Elektro dan Informatika Institut Teknologi Bandung, 2006

[2] Alrabady, Ansaf Ibrahem, Syed Masud Mahmud. *Analysis of Attack Against the Security of Keyless Entry Systems for Vehicles and Suggestions for Improved Designes*. IEEE. 2005
[3] http://redtape.msnbc.com
[4] http://www.carforumisfits.com