IMPLEMENTASI *ADVANCED ENCRYPTION STANDARD (AES)* PADA SISTEM KUNCI ELEKTRONIK KENDARAAN BERBASIS SISTEM OPERASI ANDROID DAN MIKROKONTROLER ARDUINO

Adimas Fiqri Ramdhansya[1)], **Endro Ariyanto**[2)], **Hilal Hudan Nuha**[3)]
[1,2,3)]Fakultas Informatika, Universitas Telkom
Jl. Telekomunikasi No. 1, Terusan Buahbatu, Bandung
adi31059@gmail.com[1)], endroa@telkomuniversity.ac.id[2)], hilalnuha@gmail.com[3)]

Abstrak
Selama ini untuk menghidupkan kendaraan seseorang harus menggunakan sebuah kunci, sehingga untuk mengakses banyak kendaraan harus digunakan banyak kunci yang berbeda. Namun jika *handphone* dijadikan kunci elektronik, tentunya semua kunci tersebut tidak dibutuhkan lagi, karena satu *handphone* dapat mewakili kunci tersebut. Pada penelitian ini, sistem kunci elektronik menggunakan *handphone* sebagai kunci, dan sebuah mikrokontroler Arduino pada kendaraan sebagai penerima kontrol. Komunikasi antara *handphone* dan mikrokontroler menggunakan *bluetooth*. Komunikasi dengan *bluetooth* tersebut belum didukung dengan keamanan yang kuat. Bahkan ada yang menyatakan bahwa dukungan keamanan pada *bluetooth* sudah berhasil dipecahkan dan diserang. Oleh karena itu, penelitian ini dibuat untuk melengkapi aspek keamanan kunci elektronik dengan mengimplementasikan *Advanced Encryption Standard (AES)* dengan panjang kunci 128 bit, 192 bit, dan 256 bit. Hasil yang diperoleh dari penelitian ini adalah meningkatnya dukungan aspek keamanan yang diperoleh dari implementasi AES. Setelah dilakukan pengujian, total waktu eksekusi maksimum sistem kunci elektronik kendaraan yang telah dibuat sebesar 385 ms pada jarak 20 m. Lama waktu tersebut masih lebih rendah dibanding batas kenyamanan pengguna yaitu di bawah 1000 ms (Nielsen, 1993), sehingga sistem layak untuk diterapkan.

Kata Kunci: *AES, kunci elektronik, keamanan Bluetooth, mikrokontroler Arduino*

Abstract
As long as a person want to turn the vehicle they must use a key, so as to access a lot of vehicles to be used a lot of different keys. However, if the mobile phone used as an electronic key, of course all the keys are not needed anymore, because the phone can represent the key. In this research, the electronic lock system using mobile phone as a key, and an Arduino microcontroller to control the vehicle as a receiver. Communication between mobile and microcontroller using bluetooth is not secure. One of them is that bluetooth communication not yet supported with strong security. In fact there are states that the bluetooth security has been successfully broken and attacked. Therefore, this research was made to complement the security aspects for implementing electronic key with Advanced Encryption Standard (AES) with a key of 128 bits, 192 bits, and 256 bits. After testing in terms of time, the maximum total execution time at a distance of 20 m is 385 ms. It is still lower than the limit of user convenience without being distracted that below 1000 ms (Nielsen, 1993).

Keywords: *AES, electronic key, bluetooth security, Arduino microcontroller*

1. PENDAHULUAN

Bluetooth pada telepon selular merupakan teknologi yang telah lama muncul. Salah satu aplikasi yang dapat diterapkan pada *handphone* berfasilitas bluetooth adalah menggunakannya sebagai perangkat pengakses kunci elektronik secara nirkabel. Kunci elektronik yang dimaksud adalah suatu perangkat dari kunci elektronik kendaraan yang untuk membuka atau menguncinya tidak memerlukan anak kunci tetapi dengan menggunakan pesan yang disampaikan secara digital (Wardana, A.S.). Pada penggunaannya satu *handphone* dapat menjadi kunci untuk banyak kendaraan, tidak seperti kunci konvensioal atau kunci remote biasa yang hanya bisa digunakan untuk satu kendaraan saja. Kunci elektronik biasanya digunakan untuk mengunci sesuatu yang penggunaannya dibatasi, jadi hanya orang-orang tertentu yang mempunyai hak akses. Kunci elektronik yang baik harus memiliki sistem kendali akses yang terjamin keamanannya.

Jika dilihat dari kebutuhan fungsionalitas kunci elektronik kendaraan maka pesan yang dikirimkan melalui *Bluetooth* berisi data yang relatif pendek tetapi mengandung informasi yang sangat rahasia. Oleh karena itu, kunci elektronik kendaraan harus mendapatkan perhatian lebih khususnya pada aspek keamanan. *Bluetooth* merupakan media komunikasi yang saat ini masih rentan terhadap ancaman keamanan, dimana celah keamanan bluetooth dilaporkan sudah bisa dibongkar (Syahfitra, 2007) (Vainio, 2000). Salah satu cara untuk meningkatkan keamanan adalah dengan menerapkan enkripsi pesan yang akan dikirimkan melalui *bluetooth*. Selain sisi keamanan, sisi kenyamanan juga harus diperhatian. Response time dari sistem akan mempengaruhi layak atau tidak suatu sistem untuk diterapkan.

Algoritma AES pada penelitian ini difungsikan sebagai pengaman komunikasi data antara handphone dengan kendaraan yang terpasang modul *bluetooth* yang terintegrasi dengan mikrokontroler Arduino sehingga tingkat keamanannya meningkat. Parameter yang dianalisis adalah performansi sistem dilihat dari segi waktu yang digunakan dan keamanan data, sehingga dapat diketahui kelayakan sistem untuk diterapkan.
Sistem ini diimplementasikan pada *handphone* dengan sistem operasi Android dan mikrokontroler Arduino. Sistem operasi Android dipilih sebagai platform aplikasi karena Android merupakan sistem operasi *mobile* yang *open source* (Wikipedia, 2013). Selain itu, Android merupakan *platform* yang telah populer dan hampir semua *handphone* Android telah memiliki built-in *bluetooth*. Sedangkan Arduino sendiri dipilih karena kemudahan konfigurasi dengan kendaraan, didukung dengan dokumentasi yang cukup, dan dilengkapi IDE tersendiri untuk membuat aplikasinya.

2. TINJAUAN PUSTAKA

2.1 Teknologi *Bluetooth*

Bluetooth terdiri dari *microchip* radio penerima/pemancar yang sangat kecil/pipih dan beroperasi pada pita frekuensi standar global 2,4 GHz (Haartsen, 2008). Teknologi *bluetooth*dirancang dan dioptimalkan untuk perangkat yang bersifat *mobile (mobile device)* seperti laptop, *network access point*, printer, PDA, *keyboard*, *joystick*, dan lain sebagainya. *Bluetooth* juga didesain untuk mendukung komunikasi secara bersamaan antara suara dan data dengan kemampuan transfer data sampai 721 kbps. *Bluetooth* juga mendukung layanan *synchronous* dan *asynchronous* dan mudah diintegrasikan dengan jaringan TCP/IP.
Bluetooth merupakan teknologi jaringan telekomunikasi nirkabel yang menyedikan standar dan protokol dalam pertukaran data pada jarak 1-100 meter. Untuk menjaga keamanan data diperlukan enkripsi yang baik namun karena sifatnya *mobile*, enkripsi tersebut harus efisien dan mengkonsumsi sedikit tenaga. E0 (E nol) merupakan metode yang dipilih untuk mengenkripsi pertukaran data dalam protokol *bluetooth*. E0 termasuk salah satu jenis *stream cipher* seperti layaknya A5 atau RC4 (Latchmanan). Sebelum menuju ke algoritma E0 perlu diketahui tentang proses enkripsi pada *bluetooth* sendiri (Gehrmann, 2004). Algoritma E0 memiliki 3 masukan yaitu:

1. Kunci enkripsi atau pada dunia nyata sering dikenal dengan nama PIN (*Personal Identification Number)* yang terdiri dari 1-16 karakter (8-128 bit). Kunci enkripsi kemudian akan di kombinasikan dengan EN_RAND untuk membentuk kunci tengah (K'c).
2. *Master Address* (BD_ADDR) yang nilainya sudah tertentu terdiri dari 48 bit yang dimiliki secara unik untuk setiap perangkat *bluetooth* dan disebut dengan *bluetooth Device Address*
3. *Master Clock*, waktu pengiriman paket yang terdiri dari 26 bit.

Sejumlah serangan telah ditemukan pada algoritma E0, beberapa diantaranya sebagai berikut: (Sapronov, 2006)

1. *Pin Cracking Attack* yang ditemukan oleh Yaniv Shaked dan Avishai Wool
2. *Attack Against Full E0* yang ditemukan oleh Scott R. Fluhrer dan Stefan Lucks
3. *Conditional Corelation* Attack oleh Yi Lu

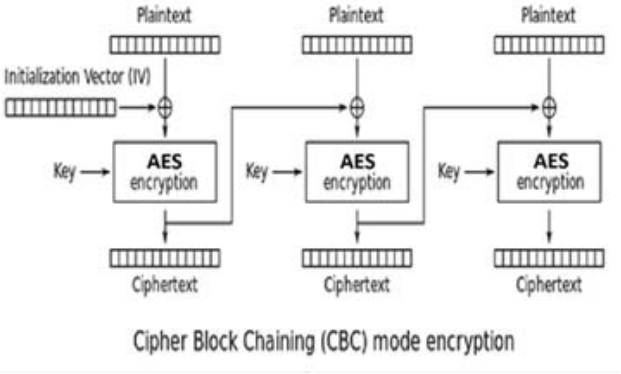
Beberapa tipe serangan *bluetooth* diantaranya *BlueBug*, *Blueprinting*, *BlueSmack*, *BlueSnarf*, *BlueSnarf++*, *HelloMoto*, *BlueBump*, *BlueDump attack*, *BlueChop*. Dewasa ini penyadapan *bluetooth* dapat dilakukan bahkan tanpa harus *paired* dengan *bluetooth* yang akan disadap. *Frontline* (http://www.fte.com) adalah salah satu perusahaan penyedia alat untuk melakukan penyadapan jaringan komunikasi *bluetooth* (Munir, 2006). Bahkan ada komunitas yang membuat tutorial untuk menciptakan *bluetooth sniffer* sendiri dengan cara mengkostumisasi *Firmware* dari *bluetooth dongle* biasa sehingga dapat melakukan *sniffing* (Bluetooth pentest, 2013).

2.2 *Advanced Encryption System (AES)*

Dalam kriptografi, *Advanced Encryption Standard* (AES) merupakan standar enkripsi dengan kunci-simetris yang diadopsi oleh pemerintah Amerika Serikat. Standar ini terdiri atas 3 blok *cipher*, yaitu AES-128, AES-192 and AES-256, yang diadopsi dari koleksi yang lebih besar yang awalnya diterbitkan sebagai Rijndael. Masing-masing *cipher* memiliki ukuran 128-bit, dengan ukuran kunci masing-masing 128, 192, dan 256 bit. AES telah dianalisis secara luas dan sekarang digunakan di seluruh dunia, seperti halnya dengan pendahulunya, *Data Encryption Standard (DES).* Jika dibandingkan dengan pendahulunya yaitu DES yang memiliki panjang key 56 bit, AES mendukung panjang key 128, 192, dan 256 bit. Secara teori 56 bit DES dapat dipecahkan dalam 1 detik dengan cara mencoba setiap key. Dengan cara yang sama, 128 bit AES hanya dapat dipecahkan selama $1,3x10^{44}$ tahun, 192 bit AES hanya dapat dipecahkan selama $2,8x10^{63}$ tahun, 256 bit AES hanya dapat dipecahkan selama $5,1x10^{82}$ tahun. Dapat disimpulkan bahwa AES memiliki keamanan yang cukup tangguh hingga saat ini (Jennifer, 2003). Pengujian keamanan dilakukan menggunakan metode pengujian keamanan *exhaustive search* atau yang lebih dikenal dengan istilah *brute force*. Percobaan metode ini dilakukan untuk mencari nilai *private key* dengan cara mencoba kemungkinan kunci satu per satu.
AES sendiri memiliki panjang kunci tertinggi yaitu 256 bit, untuk meng-*crack* 256 *bit key* dengan melakukan *brute force* akan membutuhkan 2^{128} kali lipat kemampuan komputasi dibandingkan dengan 128 *bit key*. AES menawarkan keamanan yang luar biasa dan juga performansi yang mumpuni, itulah mengapa hingga saat ini banyak produk perangkat lunak yang menggunakan AES dalam implementasi keamanannya. Beberapa produk

yang mengimplementasikan AES hingga kini yaitu 7z, WinZip, UltraISO, EFS di Windows 2000 ke atas, DiskCryptor, GBDE, LUKS, dan masih banyak lagi.

2.3 Enkripsi Mode CBC



Gambar 1. CBC enkripsi mode

Pada *cipher* blok, rangkaian bit-bit plainteks dibagi menjadi blok-blok bit dengan panjang sama, yaitu 128 bit. Algoritma AES menghasilkan blok cipherteks yang berukuran sama dengan blok plainteks. Mode pemrosesan *cipher* paling sederhana adalah *Electronic Code Book (ECB)*. Pada mode ini, setiap blok plainteks dienkripsi secara individual dan independen, kelemahan mode ECB adalah deterministik dikarenakan blok data yang sama selalu menghasilkan *cipher* yang sama juga.
Penggunaan *Cipher Block Chaining (CBC)* pada sistem yang dikembangkan dapat menghasilkan sistem yang lebih baik. Dengan mode CBC, setiap blok cipherteks bergantung tidak hanya pada blok plainteksnya tetapi juga pada seluruh blok plainteks sebelumnya. Dekripsi dilakukan dengan memasukkan blok cipherteks yang *current* ke fungsi dekripsi, kemudian meng-XOR-kan hasilnya dengan blok cipherteks sebelumnya. Blok cipherteks sebelumnya berfungsi sebagai umpan-maju (*feedforward*) pada akhir proses dekripsi. blok plainteks pertama menggunakan *Initialization Vector (IV)* sebagai vektor awal. IV tidak perlu rahasia. Algoritma AES dengan CBC membutuhkan input yang memiliki ukuran tepat multiplikasi dari ukuran blok. Penggunaan *padding* dengan standarisasi tertentu tidak diperlukan. Blok dapat dipenuhi agar sesuai dengan spesifikasinya cukup dengan karakter kosong (spasi), selain itu Arduino sendiri tidak menerapkan standarisasi tertentu untuk *padding*.

2.4 Mikrokontroler Arduino

Arduino adalah pengendali mikro *single-board* yang bersifat *open-source*, diturunkan dari *wiring platform*, dan dirancang untuk memudahkan penggunaan elektronik dalam berbagai bidang. Perangkat kerasnya memiliki prosesor Atmel AVR dan perangkat lunaknya memiliki bahasa pemrograman sendiri (Arduino, 2013).

Gambar 2.Mikrokontroler Arduino

Spesifikasi mikrokontroler Arduino Uno adalah sbb:

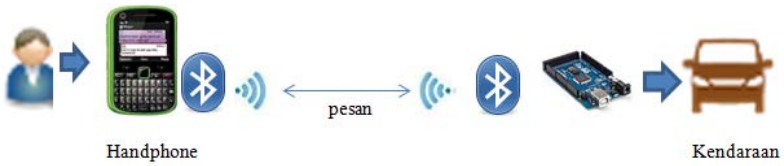
Microcontroller	ATmega328
Operating Voltage	5V
Input Voltage (recommended)	7-12V
Input Voltage (limits)	6-20V

Digital I/O Pins	14 (of which 6 provide PWM output)
Analog Input Pins	6
DC Current per I/O Pin	40 mA
DC Current for 3.3V Pin	50 mA
Flash Memory	32 kB (ATmega328) of which 0.5 KB used by bootloader
SRAM	2 kB (ATmega328)
EEPROM	1 kB (ATmega328)
Clock Speed	16 MHz

Dengan keterbatasan spesifikasi perangkat keras Arduino Uno, sangat diperlukan enkripsi yang tidak hanya aman, melainkan memiliki kompatibilitas untuk banyak perangkat keras. Setelah dilakukan studi literatur, AES dapat diimplementasikan pada Arduino Uno.

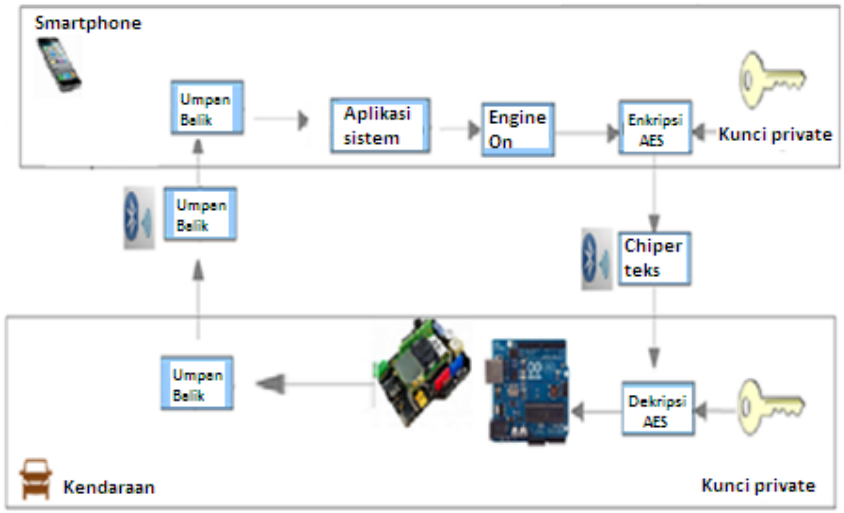
3. METODE PENELITIAN

Sistem kunci elektronik kendaraan merupakan suatu sistem pengontrol kendaraan secara digital yang terintegrasi dengan mikrokontroler pada kendaraan yang memungkinkan untuk mengontrol kendaraan tanpa anak kunci, cukup menggunakan sebuah handphone sebagai kuncinya (Wardana, A.S.). Terintegrasinya *bluetooth* pada modul mikrokontroler dapat memungkinkan untuk menghidupkan atau mematikan mesin kendaraan secara digital melalui *handphone*. Pemanfaatan teknologi *bluetooth* menjadi populer karena tanpa biaya, nyaman dan mudah menerima pesan dengan kehandalan yang cukup tinggi.



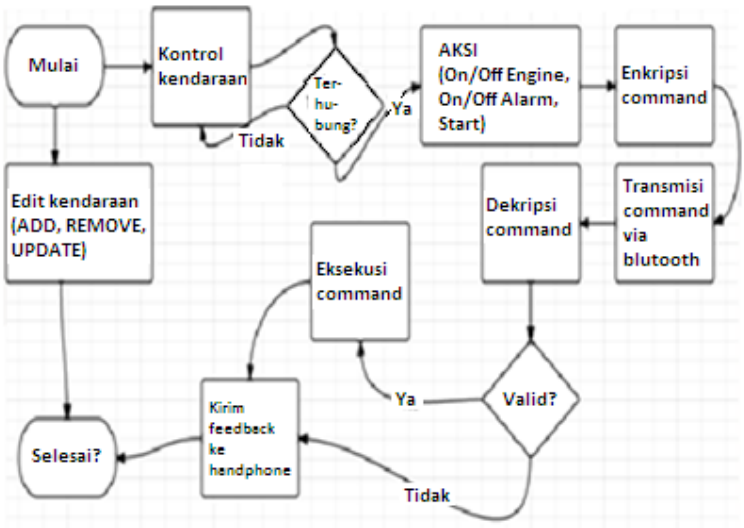
Gambar 3. Diagram blok sistem kunci elektronik kendaraan

Sistem yang telah dibuat adalah sistem enkripsi pesan menggunakan AES yang digunakan untuk melakukan pengiriman pesan antara *handphone* dan kendaraan. *Private key* yang digunakan telah ditentukan oleh kedua perangkat. Cara ini dilakukan agar pengguna dengan *handphone*-nya dapat melakukan enkripsi pesan, sedangkan dekripsi pesan dilakukan oleh mikrokontroler yang terpasang pada kendaraan. Sesuai dengan tujuan awal bahwa enkripsi pesan menggunakan algoritma simetrik AES disesuaikan dengan data yang berukuran relatif kecil yang sesuai dengan ukuran data konten pada pesan yang ditransmisikan melalui *bluetooth*. Rancangan sistem kunci elektronik kendaraan yang dibuat dapat dilihat pada gambar 4.



Gambar 4. Rancangan sistem kunci elektronik kendaraan

Sistem yang dibangun membutuhkan beberapa tahap dan *timeline* yang akan dilewati. *Flowchart* implementasi sistem dapat dilihat pada gambar 5.

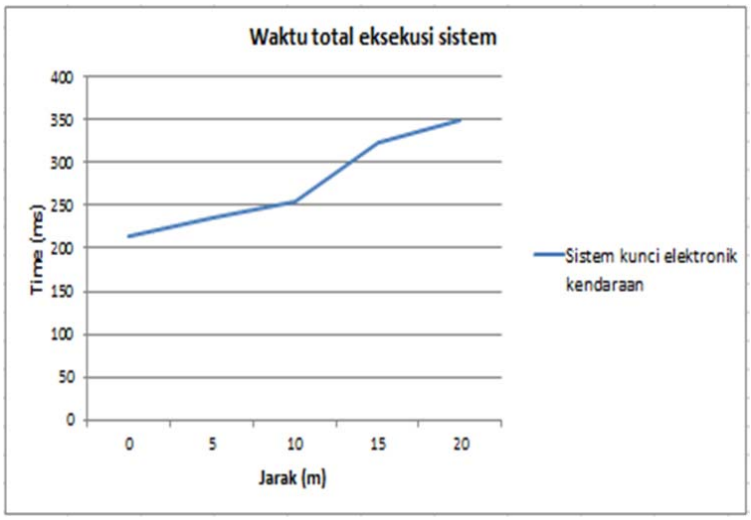


Gambar 5. Diagram alir sistem

4. HASIL DAN PEMBAHASAN

4.1 Pengujian Waktu Eksekusi Sistem Secara Keseluruhan

Pengujian ini bertujuan untuk mengetahui total waktu yang diperlukan oleh sistem secara keseluruhan, sehingga dapat diketahui apakah sistem layak diterapkan atau tidak. Waktu diukur sejak sistem mengirimkan pesan ke kendaraan hingga menerima umpan balik dari kendaraan pada jarak ukur tertentu.

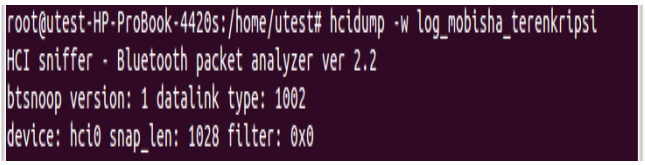


Gambar 6. Waktu total eksekusi sistem terhadap jarak

Jarak yang diambil dalam pengujian ini adalah jarak antara kendaraan dan *handphone* pada kondisi *outdoor*, dapat diketahui bahwa jarak maksimum untuk penggunaan sistem adalah 20 m, karena koneksi sistem akan tidak stabil atau terputus setelah melebihi jarak 20 m. Setelah dilakukan percobaan sebanyak 20 kali untuk setiap jarak ukur, dapat diketahui bahwa rata-rata total waktu yang dibutuhkan untuk eksekusi sistem adalah 275.76 ms. Dapat diketahui bahwa waktu untuk mengeksekusi algoritma AES tidak menjadi proses yang dominan karena waktu untuk enkripsi pada *handphone* hanya membutuhkan kurang dari 0,45 ms atau hanya 0,2% dari total waktu yang dibutuhkan, sedangkan dekripsi pada Arduino hanya membutuhkan waktu kurang dari 4,5 ms atau hanya 2% dari total waktu yang dibutuhkan. Waktu yang paling dominan yaitu proses kerja sistem kunci elektronik kendaraan itu sendiri, sejak transmisi pesan dari *handphone* ke kendaraan, pesan tersebut dieksekusi, hingga ada umpan balik dari kendaraan. Diketahui waktu total eksekusi sistem maksimum sebesar 385 ms, masih lebih rendah dibanding batas kenyamanan pengguna tanpa merasa terganggu yaitu di bawah 1000 ms (Nielsen, 1993). Dengan data tersebut dapat disimpulkan bahwa sistem layak diterapkan karena response time sistem masih di bawah ambang batas kenyamanan pengguna.

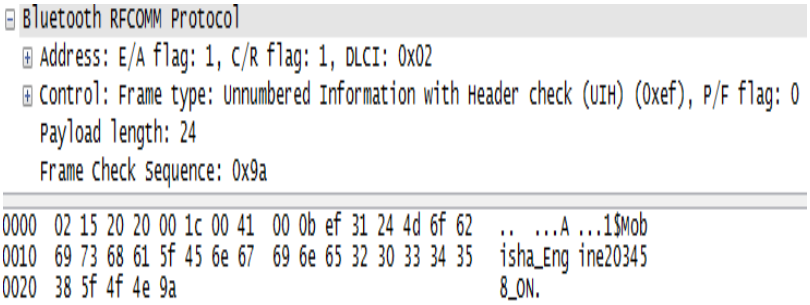
4.2 Pengujian keamanan sistem

Pengujian keamanan bertujuan untuk mengetahui apakah algoritma AES berhasil diimplementasikan ke dalam sistem yang dibuat sehingga mempunyai keamanan yang tinggi. Pengujian keamanan dilakukan dengan cara *sniffing* secara aktif terhadap transmisi *bluetooth* dari *handphone* yang menggunakan sistem kunci elektronik kendaraan yang terimplementasi AES dan transmisi *bluetooth* tanpa AES. Sistem operasi Linux (Ubuntu 12.04) yang digunakan dalam pengujian ini harus dilengkapi dengan libpcap (sistem *interface* untuk melakukan *packet capture*) terlebih dahulu. Tahap selanjutnya adalah mengaktifkan modul pada PyBluez untuk aktivasi soket rfcomm.



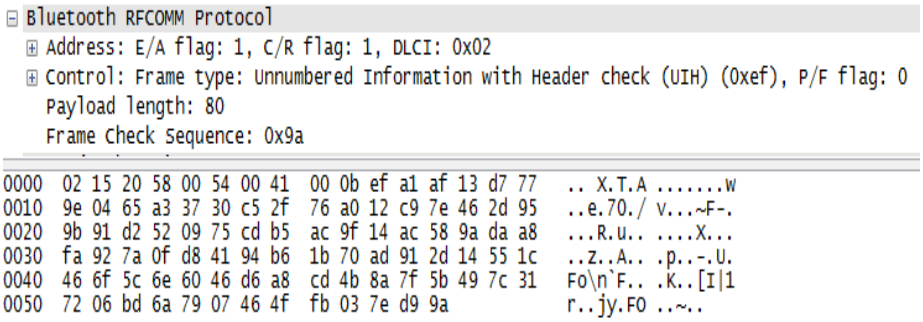
Gambar 7. Proses *packet capture*

Pada gambar di atas terlihat proses *sniffing* paket data telah diaktifkan pada *bluetooth adapter* hci0 dengan menggunakan *tool* HCIDump (HCI *sniffer – bluetooth packet analyzer* v2.2).



Gambar 8. Hasil pengujian sistem tanpa implementasi AES

Dari hasil *packet capture* dari proses *sniffing handphone* pada sistem tanpa implementasi AES seperti pada gambar 8, dapat dilihat *command* dari *handphone* ditampilkan secara *plain* yaitu *command* "$Mobisha_Engine203458_ON" yang berfungsi untuk menyalakan kendaraan. Dari pengujian ini dapat dibuktikan bahwa *command* dapat di-*capture* secara baik, sehingga *replay attack* dapat dilakukan untuk membobol sistem dengan cara melakukan transmisi ulang *command* yang telah di-*capture* dari *handphone* ke kendaraan. Dengan demikian transmisi *bluetooth* tanpa AES sangat mudah untuk dibobol.



Gambar 8. Hasil pengujian sistem dengan implementasi AES

Dari hasil *packet capture* dari proses *sniffing handphone* yang menggunakan sistem dengan implementasi AES, dapat dilihat *command* dari handphone tidak dapat dibaca secara jelas, karena pesan yang dikirim dari *handphone* merupakan *cipher* dari proses enkripsi AES. Pada setiap eksekusinya *payload* yang berisi *command* dari *handphone* selalu memiliki hasil yang berbeda sehingga sistem aman dari *replay attack*. Berdasarkan data pengujian tersebut dapat disimpulkan bahwa transmisi antara handphone dengan Arduino melalui *bluetooth* menjadi lebih aman sehingga pesan yang terkirim tidak dapat diketahui oleh pihak lain.

5. KESIMPULAN

Berdasarkan pembahasan dalam penelitian ini dapat disimpulkan bahwa algoritma AES berhasil diimplementasikan untuk mengenkripsi atau mendekripsi pesan dari sistem operasi *mobile* Android dengan mikrokontroler Arduino yang ada pada kendaraan. Algoritma AES cocok diterapkan pada sistem yang telah dibuat terlihat dari waktu total eksekusi sistem maksimum pada jarak 20 m hanya sebesar 385 ms, masih lebih rendah dibanding batas kenyamanan pengguna tanpa merasa terganggu yaitu 1000 ms. Berdasarkan hasil pengujian keamanan sistem dengan cara *sniffing* pada transmisi *bluetooth*, implementasi AES terbukti dapat membuat sistem lebih aman terhadap serangan *replay attack*.

Untuk mendapatkan tingkat keamanan yang lebih baik disarankan untuk mengkombinasikan *One Time* Pad (OTP) dengan AES serta integrasikan sistem dengan dukungan jaringan internet sehingga sistem dapat melakukan perubahan key bagi seluruh pengguna sistem dalam kurun waktu tertentu, misalnya setiap satu bulan atau setiap tahun.

DAFTAR PUSTAKA

Arduino, November 2013, *Arduino Hardware, Products, and Support homepage*. http://Arduino.cc/

Bluetooth pentest, September 2013, *Bluetooth sniffing for less*, http://bluetooth-pentest.narod.ru/doc /bluetooth_sniffing_for_less.txt

Gehrmann, C. J. Persson, and B. Smeets, 2004, *BluetoothSecurity*, Artech House; Boston

Haartsen, Japp., Februari 2008, *Bluetooth Baseband*, http://www.palowireless.com/infotooth/tutorial /baseband.asp

Jennifer Maurer, 2003, *Hardware Implementation of the Advanced Encryption standard*, Massachussets Institute of Technology

Latchmanan, Sivalingham and Sharmin Parveen, --, *Applicability Of Rc4 Algorithm In Bluetooth Data Encryption Method For Achieving Better Energy Efficiency Of Mobile Devices*, University of Malaya, Kuala Lumpur

Munir, R., Agustus 2006, *Kriptografi*, Bandung

Nielsen, Jakob, Januari 1993, *Response Times: The 3 Important Limits*, http://www.nngroup.com/articles /response-times-3-important-limits

Sapronov, K., Maret 2006, *Bluetooth, Bluetooth security and New Year War-nibbling*, http://www.securelist.com/en/analysis/181198286/bluetooth_bluetooth_Security_and_New_Year_War _nibbling

Syahfitra, D., 2007, *Studi dan Analisis Serangan Terhadap E0 Cipher pada Protokol Komunikasi Bluetooth*, Makalah Fakultas Informatika Institut Teknologi Bandung

Vainio, J.T., 2000, *Bluetooth Security*, Jurnal Helsinski University of Technology

Wardana, A.S., --, *Simulasi Kunci Elektronik Ter-Enkripsi Untuk Aplikasi Bluetooth Pada Telepon Selular*, Makalah Seminar Universitas Dipenogoro

Wikipedia, November 2013, *Android (Operating System)*, http://en.wikipedia.org/wiki /Android_operating_system