Penerapan Steganografi pada *Near Field Communication* berbasis *Mobile*

Emil Fahmi Yakhya - 13509069
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia
emilfahmi@students.itb.ac.id

***Abstract*—NFC merupakan salah satu teknologi komunikasi terbaru memanfaatkan gelombang radio. Teknologi NFC ini masih memiliki berbagai isu keamanan selayaknya teknologi baru yang masih bisa dikatakan berada dalam tahap pengembangan. Berangkat dari isu keamanan pada NFC tersebut, dibuat makalah ini yang bertujuan untuk mengaplikasikan ilmu steganografi sederhana yang diajarkan pada mata kuliah IF3058-Kriptografi sebagai kontribusi untuk meminimalkan isu keamanan yang selama ini masih belum ditemukan inovasinya secara teknis oleh para pengembang NFC.**

Kata Kunci – NFC, Steganografi.

I. PENDAHULUAN

Near Field Communication (NFC) merupakan teknologi baru dalam dunia komunikasi. Teknologi ini merupakan suatu standar untuk *smartphones* atau perangkat lain yang memanfaatkan gelombang radio untuk berkomunikasi satu sama lain dalam jarak dekat atau saling menyentuhkan antara dua perangkat NFC.

Walaupun penggunaan NFC dalam aplikasi berbasis *moblie* masih belum populer, namun perlahan tapi pasti NFC ini terus mengalami peningkatan baik dalam pengembangan dalam aspek teknologinya atau pun pengembangan dalam aspek penerapannya.

Peningkatan penggunaan ini menyebabkan munculnya berbagai ancaman baru terhadap penggunaan NFC. Apalagi bila mempertimbangkan faktor keamanan tag NFC yang masih sangat rawan disadap oleh semua pengguna yang memiliki *device* NFC aktif.

Berangkat dari hal tersebut, dibuatlah makalah dengan topik penerapan steganografi pada NFC. Steganografi ini merupakan pengembangan algoritma kriptografi klasik dengan cara menambahkan kode atau mekanisme penerjemahan yang tidak diketahui selain para penggunanya.

Diharapkan, dengan adanya penerapan steganografi menggunakan tag NFC dengan kasus-kasus sederhana dapat memberikan dasar dan referensi bagi para pengembang aspek keamanan untuk teknologi NFC berbasis *mobile*.

.

II. STEGANOGRAFI

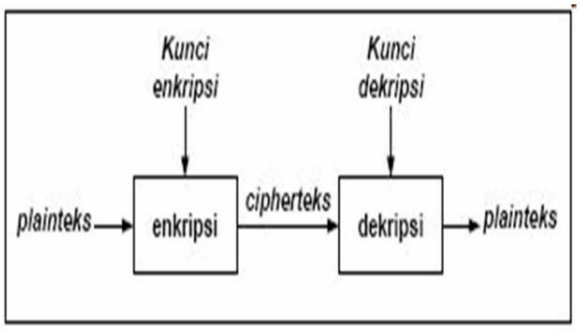
A. Prinsip Dasar

Steganografi merupakan bagian dari ilmu kriptografi yang juga memiliki empat prinsip sebagai berikut:

1. *Confidelity* (Kerahasiaan)
   Memiliki makna setiap pesan yang dikirimkan tetap rahasia dan tidak diketahui oleh pihak lain selain pengirim dan penerima.
2. *Data integrity* (Keutuhan data)
   Memiliki makna setiap data mampu dikenali/dideteksi tanpa adanya manipulasi oleh pihak lain.
3. *Authentication* (Keontetikan)
   Memiliki makna bahwa dua pihak yang berhubungan adalah pihak yang sebenarnya, biasanya dibuktikan dengan isi data, waktu pengiriman, identitas pengenal, dll.
4. *Non-repudation* (Anti penyangkalan)
   Memiliki makna informasi yang dikirimkan adalah benar berasal dari pihak yang dimaksud tanpa adanya penyangkalan.

B. Proses Enkripsi dan Dekripsi

Kemudian, steganografi juga memiliki prinsip dasar enkripsi/dekripsi sebagaimana digambarkan di bawah ini:



Gambar 1. Proses Enkripsi dan Dekripsi

Berikut adalah penjelasan untuk istilah-istilah pada gambar di atas:

- **Plainteks**
  Plainteks adalah pesan berupa data asli yang

dikirimkan. Umumnya pesan ini bisa dipahami langsung oleh manusia.

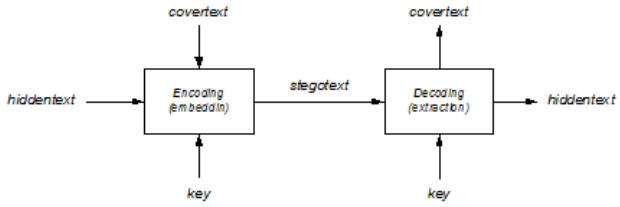
- **Cipherteks**
  Cipherteks adalah pesan hasil enkripsi. Biasanya pesan ini tidak bisa langsung dipahami oleh manusia.
- **Enkripsi**
  Enkripsi merupakan fungsi yang mengubah plainteks menjadi cipherteks.
- **Dekripsi**
  Dekripsi merupakan fungsi yang mengubah cipherteks menjadi plainteks. Fungsi ini merupakan kebalikan dari enkripsi.
- **Kunci**
  Kunci adalah suatu sandi yagn dirahasiakan yang digunakan dalam proses enkripsi dan dekripsi.

C. Definisi Steganografi

Steganografi secara bahasa memiliki arti tulisan tersembunyi. Sedangkan secara istilah adalah ilmu dan seni menyembunyikan *(embedded)* informasi dengan cara menyisipkan pesan rahasia di dalam pesan lain.

Pada konteks penerapannya di teknologi digital, steganografi merupakan penyembunyian pesan menggunakan media pada komputer digital seperti gambar, suara, teks, dsb.

Kemudian, berikut adalah properti-properti yang terdapat pada steganografi:



Gambar 2 – Properti pada Steganografi

Dengan penjelasan sebagai berikut:

- ***Embedded Message***
  Merupakan pesan yang disembunyikan.
- ***Cover-object***
  Merupakan pesan yang digunakan untuk menyembunyikan *embedded message*.
- ***Stego-object***
  Merupakan pesan yang sudah berisi *embedded message*.
- ***Stego-key***
  Merupakan kunci yang digunakan untuk menyisipkan pesan dan mengekstraksi pesan dari stegoteks

D. Rancangan Algoritma

Algoritma sederhana yang dirancang untuk diimplementasikan pada NFC ini merupakan kombinasi antara cipher transposisi dengan pembangkitan kunci steganografi.

Pembangkitan Kunci

Pembangkitan kunci steganografi dilakukan berdasarkan nama id pengguna aplikasi. Setiap karakter dari nama pengguna aplikasi ini akan dideteksi nilai ASCII-nya, kemudian dijumlahkan keseluruhannya dan dibagi dengan nilai modulo 26 sebagai representasi alfabet.

Sebagai contoh, bila nama pengguna adalah “Emil” maka total nilai ASCII-nya (69 + 109 + 105 + 108) dibagi dengan nilai modulo 26 adalah ‘1’. Nilai ‘1’ ini akan menjadi kunci pergeseran untuk kata yang dienkripsi pada tag NFC.

Penggunaan Prinsip Transposisi

Penggunaan prinsip transposisi pada makalah ini adalah dengan mengadopsi metode *Caesar’s Cipher* dimana kunci yang digunakan dibangkitkan secara unik dari karakter id pengguna.

Sebagai contoh bila plainteks yang ditanamkan pada Tag NFC adalah “Buka”, maka cipherteks untuk nama pengguna “Emil” adalah “Cvlb”.

III. Permasalahan Keamanan pada NFC

Dalam suatu penggunaan teknologi NFC, terdapat potensi-potensi masalah keamanan sebagai berikut:

1. Penyadapan
   Sinyal radio yang digunakan untuk melakukan transfer data antara *device* NFC sangat memungkinkan adanya penyadapan dalam jarak tertentu. NFC aktif dalam jarak beberapa meter dan sangat memungkinkan adanya penyadapan ketika dua peralatan berbasis NFC saling berkomunikasi satu sama lain.
2. Modifikasi Data
   Masalah berikutnya adalah terkait modifikasi data. Sangat mudah untuk menghancurkan data dengan *jammer*. Hingga saat ini belum ada penanganan untuk mengatasi serangan semacam ini. Selain itu, bila peralatan NFC aktif pada frekuensi radio, khususnya ketika sedang melakukan pengiriman maka akan sangat mudah dideteksi oleh pengguna lain yang berniat melakukan penyerangan.
3. Serangan Relay
   Dikarenakan NFC termasuk ke dalam protokol ISO/IEC 14443, serangan relay sangat *feasible* untuk dilakukan pada NFC. Serangan ini menggunakan prinsip dengan cara mendahului permintaan transfer data antara pengirim dan itpenerima, kemudian penyerang memberikan data kepada pengirim dan penerima seakan-akan data tersebut adalah data yang valid.
4. Kehilangan Properti
   Ketika suatu *device* NFC atau kartu NFC hilang,

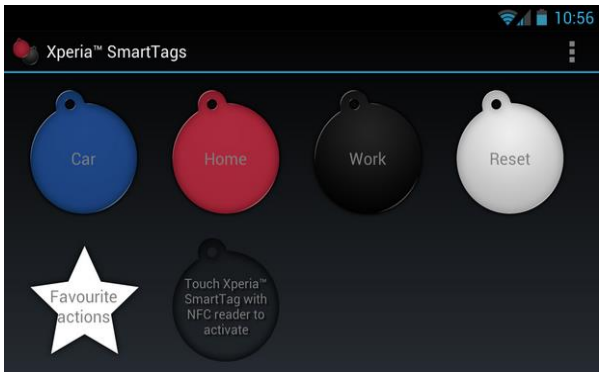
maka peralatan yang hilang tersebut akan memberikan akses kepada pengguna NFC lain yang berlaku sebagai pengguna tunggal.

5. Terputusnya Koneksi
   Terkahir, NFC menggunakan frekuensi radio jarak dekat yang memiliki resiko koneksi terputus ketika akan

Kelima masalah tersebut merupakan masalah klasik yang disebabkan teknologi NFC yang masih terus dikembangkan. Aspek permasalahan teknis tersebut masi belum bisa diatasi dengan riset sederhana. Satu-satunya cara untuk mengurangi permasalahan keamanan tersebut dalam skala aplikasi sehari-hari adalah dengan cara memberikan penerapan kriptografi pada *device* aktif (mis: ponsel, tablet, dsb) dan meletakkan cipherteks pada Tag NFC.

IV. PENERAPAN STEGANOGRAFI

A. Contoh Penerapan Tag NFC yang Populer



Gambar 3 – Tag NFC Sony Xperia

Gambar di atas dalah tag NFC yang dimiliki oleh Sony Xperia. Dalam tag di atas pengguna bisa menyimpan empat buah status yang disesuaikan dengan kondisi pengguna sedang berada dimana. Kelemahan dari penggunaan tag ini adalah setiap pengguna Xperia yang memiliki fitur NFC dapat mengakses tag yang dimiliki oleh pengguna lain. Selain itu, ketika ada dua ponsel yang memiliki fitur NFC dapat menyebabkan adanya masalah komunikasi antara Tag NFC sebagai peralatan NFC pasif dan ponsel sebagai peralatan NFC aktif.

B. *Tools* yang Digunakan untuk Implementasi

Peralatan yang digunakan untuk menerapkan steganografi dalam NFC ini dibagi menjadi dua yakni peralatan NFC aktif dan peralatan NFC pasif.

Peralatan NFC Aktif

Peralatan NFC Aktif yang digunakan dalam implementasi steganografi ini adalah Blakcbery Dev Alpha. Blackberry ini memiliki fitur NFC dan *library* dimana bisa mengaktifkan suatu peralatan NFC pasif baik itu untuk melakukan pembacaan data maupun melakukan penulisan data kepada NFC pasif.

Berikut adalah gambar dari Blackberry Dev Alpha untuk implementasi:

Gambar 4 – Blackberry Dev Alpha

Peralatan NFC Pasif

Peralatan yang kedua dalam implementasi ini adalah peralatan NFC Pasif dimana peralatan ini hanya ‘aktif’ ketika menerima respon dari peralatan yang aktif. Dalam hal ini, peralatan NFC pasif yang digunakan tidak lain adalah tag NFC yang *rewriteable*.

Dalam implementasi terkait steganografi, tag NFC ini ditanamkan cipherteks yang telah dienkripsi menggunakan nama pengguna aplikasi.

Berikut adalah contoh gambar dari tag yang digunakan untuk mengembangkan aplikasi ini:

Gambar 5 – Tag NFC sebagai perangkat pasif

Lingkungan Pengembangan

Dalam implementasinya, lingkungan pengembangan yang digunakan adalah Java dengan IDE Eclipse yang telah diintegrasikan dengan *plugin* dan simulator Blackberry.

C. Deskripsi Aplikasi yang Dikembangkan

Kemudian, implementasi dari aplikasi ini dibagi menjadi empat bagian utama berupa program utama, fungsi pembaca tag NFC, fungsi menulis ke tag NFC dan fungsi steganografi untuk membangkitkan bilangan acak serta melakukan transposisi terhadap cipherteks.

Program Utama

```
package nfcstegano;

import net.rim.device.api.ui.UiApplication;

public class NFCStegano extends UiApplication {
    public NFCStegano() {
        pushScreen(new NFCStegano_WriteTag());
    }

    /**
     * Entry point for application
     * @param args Command line arguments (not used)
     */
    public static void main(String[] args){
        new NFCStegano().enterEventDispatcher();
    }
}
```

Gambar 6 – Dokumentasi Program Utama

Pada program utama ini, dilakukan *import* terhadap *library* NFC yang dimiliki Blackberry dan juga melakukan inisiasi terhadap aplikasi untuk dapat menulis dan membaca Tag NFC.

Fungsi Pembaca Tag NFC

```
package Nfcvigenere;

import java.io.IOException;

import net.rim.device.api.io.nfc.ndef.NDEFMessage;
import net.rim.device.api.io.nfc.ndef.NDEFMessageListener;
import net.rim.device.api.io.nfc.ndef.NDEFRecord;
import net.rim.device.api.io.nfc.readerwriter.ReaderWriterManager;
import net.rim.device.api.ui.component.EditField;
import net.rim.device.api.ui.component.LabelField;
import net.rim.device.api.ui.container.MainScreen;

public class NFCVigenere_ReadTag extends MainScreen {

    ReaderWriterManager rwman;

    LabelField instruction;
    EditField ciphertext;
    EditField plaintext;

    public NFCVigenere_ReadTag() {
        // Instantiate NFC
        try {
            // Get instance
            rwman = ReaderWriterManager.getInstance();

            // Set listener
            rwman.addNDEFMessageListener(new MessageListener(), NDEFRecord.TNF_UNKNOWN, "text/cipher");
        } catch (IOException e) {
        }

        // Constructs UI
        instruction = new LabelField();
        instruction.setText("Tap phone to a NFC Tag");
        add(instruction);

        ciphertext = new EditField("Ciphertext: ", "");
        ciphertext.setEditable(false);
        add(ciphertext);

        plaintext = new EditField();
        plaintext.setEditable(false);
        add(plaintext);
    }

    private class MessageListener implements NDEFMessageListener {

        public void onNDEFMessageDetected(NDEFMessage msg) {
            // TODO Auto-generated method stub
            String cipher = new String(msg.getRecords()[0].getPayload());
            ciphertext.setText(cipher);
            plaintext.setText(Vigenere.decrypt(cipher));
        }

    }

}
```

Gambar 7 – Dokumentasi Fungsi Pembaca Tag NFC

Secara teknis, fungsi pembaca Tag NFC ini melakukan pembacaan terhadap cipherteks dari tag NFC dan memanggil fungsi dekripsi dari fungsi steganografi.

Ketika cipherteks yang dibaca sesuai dengan kunci acak yang dibangkitkan dari nama pengguna, maka aplikasi akan memberikan pernyataan bahwa Tag yang dibaca adalah valid dan secara otomatis membuat ponsel mengaktifkan fitur yang telah ditetapkan sebelumnya.

Ketika cipherteks yang dibaca tidak sesuai dengan kunci acak yang dibangkitkan dari nama pengguna, maka aplikasi akan menolak akses terhadap Tag NFC dan membatalkan pengguna untuk mengaktifkan fitur di dalam ponsel.

Fungsi Menulis ke Tag NFC

```
package nfcstegano;

import net.rim.device.api.ui.Field;
import net.rim.device.api.ui.FieldChangeListener;
import net.rim.device.api.ui.component.ButtonField;
import net.rim.device.api.ui.component.EditField;
import net.rim.device.api.ui.container.MainScreen;

public class NFCStegano_WriteTag extends MainScreen {

    EditField plaintext;
    EditField ciphertext;
    EditField newplaintext;
    ButtonField write;

    public NFCStegano_WriteTag() {
        // Constructs UI
        plaintext = new EditField("Plaintext: ", "");
        add(plaintext);

        ciphertext = new EditField("Ciphertext: ", "");
        ciphertext.setEditable(false);
        add(ciphertext);

        newplaintext = new EditField("Plaintext: ", "");
        add(newplaintext);

        write = new ButtonField("Write to NFC Tag");
        write.setChangeListener(new FieldChangeListener() {

            public void fieldChanged(Field field, int context) {
                // TODO Auto-generated method stub
                if (!plaintext.getText().equals("")) {
                    ciphertext.setText(Stegano.encrypt(plaintext.getText()));
                    newplaintext.setText(Stegano.decrypt("cieppdzwkqlmfd"));
                }
            }

        });
        add(write);
    }

}
```

Gambar 8 – Dokumentasi Fungsi Penulis Tag NFC

Dari kode di atas, dapat dilihat bahwa tugas utama dari fungsi ini adalah untuk membaca plainteks yang diinginkan user, kemudian membangkitkan fungsi dekripsi dari steganografi dan menuliskan cipherteksnya pada Tag NFC.

Fungsi Steganografi

```
package nfcstegano;

public class Stegano {

    private static String key = "buka";

    public static String encrypt(String plaintext) {
        int ascii = 0;
        String ciphertext = "";
        for (int i = 0; i < plaintext.length(); i++) {
            char c = plaintext.charAt(i);
            if (((int) c > 96) && ((int) c < 123)) {
                ascii = ((int) c + (int) key.charAt(i % key.length()) + 1) - 97;
            }
            if (ascii > 122) {
                ascii -= 26;
            }
            ciphertext += (char) ascii;
        }
        return ciphertext;
    }

    public static String decrypt(String ciphertext) {
        int ascii = 0;
        String plaintext = "";
        for (int i = 0; i < ciphertext.length(); i++) {
            char c = ciphertext.charAt(i);
            if (((int) c > 96) && ((int) c < 123)) {
                ascii = ((int) c - (int) key.charAt(i % key.length()) + 1) + 97;
            }
            if ((ascii > 70) && (ascii < 96)) {
                ascii += 26;
            }
            plaintext += (char) ascii;
        }
        return plaintext;
    }

}
```

Gambar 9 – Dokumentasi Fungsi Steganografi

Fungsi steganografi ini terbagi menjadi tiga bagian utama, yakni bagian pembangkitan kunci, bagian enkripsi dan bagian dekripsi.

Seperti yang telah dijelaskan pada rancangan algoritma di bab sebelumnya, fungsi ini akan membangkitkan bilangan acak sebagai bentuk steganografi dari nama pengguna dan mengkombinasikannya dengan cipher transposisi.

Sedangkan untuk dekripsinya, ketika program utama membaca Tag NFC maka secara otomatis fungsi pembangkitan bilangan acak akan dipanggil untuk melakukan dekripsi berdasarkan nama penggunanya.

V. HASIL DAN ANALISIS

A. Hasil Pengujian

Skenario pengujian ini dibagi menjadi 12 nama pengguna untuk membaca plainteks yang sama. Namun, setiap pengujian Tag NFC ditulis dengan cipherteks yang dibangkitkan melalui bilangan acak berdasarkan nama pengguna tersebut.

Berikut adalah nama-nama pengguna yang dijadikan studi kasus untuk implementasi steganografi pada NFC berbasis *mobile*:

"Emil", "emil", "Meli", "meli", "Lime", "lime", "Meil", "meil", "Elim", "elim", "Mile", "mile".

Dan berikut adalah matriks hasil pengujian terhadap 12 nama pengguna dengan beberapa kali terjadi kombinasi karakter yang persis:

	Emil	emil	Meli	meli	Lime	lime	Meil	meil	Elim	elim	Mile	mile	
Emil		1	1	1	1	1	1	1		1	1		9
emil	1		1		1		1		1		1		6
Meli	1	1		1	1	1		1	1	1		1	9
meli	1		1		1		1		1		1		6
Lime	1	1	1	1		1	1	1	1	1	1	1	11
lime	1		1		1		1		1		1		6
Meil	1	1		1	1	1		1	1	1		1	9
meil	1		1		1		1		1		1		6
Elim		1	1	1	1	1	1	1		1	1	1	10
elim	1		1		1		1		1		1		6
Mile	1	1		1	1	1		1	1	1		1	9
mile	1		1		1		1		1		1		6
	10	6	9	6	11	6	9	6	10	6	9	5	93
												%Berhasil:	64,58

Gambar 10 – Hasil Pengujian dari 12 contoh kasus

B. Analisis Hasil Pengujian

Hasil pengujian di atas mendapatkan persentasi keberhasilan tidak terjadi penyadapan, bentrokan atau pun resiko keamanan antara dua buah *device* NFC yang aktif sebesar 64,58%.

Hasil ini cukup membantu dimana ketika mengambil studi kasus penggunaan tag NFC populer yang diusung oleh Xperia memungkinkan adanya bentrokan ketika ada dua perangkat NFC aktif yang mengaktifkan sinyal radionya dalam waktu bersamaan.

Galat kegagalan pada hasil ini cukup besar secara persentasi, namun secara umum percobaan dengan tujuan meningkatkan keamanan informasi dari perangkat NFC berbasis *mobile* dapat dikatakan tercapai bila dibandingkan dengan studi kasus penerapan NFC populer tanpa menggunakan enkripsi.

Berangkat dari hasil percobaan ini, seccara kasar dapat disimpulkan bahwa pengembangan NFC berbasis *mobile* memanfaatkan ilmu kriptografi adalah *feasible.*

VI. KESIMPULAN

Berikut adalah beberapa kesimpulan yang dapat diberikan dari implementasi steganografi sederhana pada NFC berbasis *mobile*:

1. Dari hasil percobaan, dapat disimpulkan bahwa penerapan ilmu kriptografi pada NFC bisa dilakukan.
2. Dari hasil percobaan, dapat disimpulkan bahwa penerapan steganografi pada NFC berbasis *mobile* dapat meningkatkan keamanan pertukaran data.
3. Dari hasil percobaan, dapat disimpulkan bahwa resiko isu keamanan pada NFC dapat diminimalkan dengan memanfaatkan ilmu kriptografi sederhana.
4. Terakhir, algoritma steganografi yang dirancang masih belum efektif dalam menangai kombinasi nama dengan karakter yang persis sama. Perlu dilakukan pengembangan algoritma untuk meningkatkan keamanan dalam pertukaran data antara perangkat NFC aktif dan perangkat NFC pasif.

VII. UCAPAN TERIMA KASIH

Penulis mengucapkan terima kasih kepada Allah yang Maha Kuasa dengan segala anugerah-Nya yang diberikan penulis dapat mengaplikasikan ilmu yang didapatkan selama di kelas pada dunia nyata. Tak lupa penulis juga mengucapkan terima kasih kepada Bapak Rinaldi Munir sebagai dosen pengajar kuliah IF3058 atas segala ilmunya yang telah diberikan hingga makalah ini dapat disempurnakan. Tak lupa pula, terima kasih diucapkan kepada teman saya dari Fakultas Ilmu Komputer Universitas Gajah Mada yang telah meminjamkan perangkat untuk pengembangan steganografi pada NFC berbasis *mobile* ini.

REFERENSI

[1] Slide Kuliah IF3058-Kriptografi, Bab Kriptografi dan Bab Steganografi.

[2] "What is NFC?". NFC Forum. Retrieved 14 June 2011.H. Poor, *An Introduction to Signal Detection and Estimation*. New York: Springer-Verlag, 1985, ch. 4.

[3] "NFC Forum Announces Two New Specifications to Foster Device Interoperability and Peer-to-Peer Device Communication". 19 May 2009. Retrieved 14 June 2011.E. H. Miller, "A note on reflector arrays (Periodical style—Accepted for publication)," *IEEE Trans. Antennas Propagat.*, to be published.

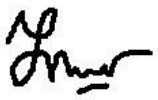
[4] Hancke, Gerhard P (July 2008). "4th Workshop on RFID Security (RFIDsec'08)". pp. 100–13..C. J. Kaufman, Rocky Mountain Research Lab., Boulder, CO, private communication, May 1995.

[5] http://developer.blackberry.com

PERNYATAAN

Dengan ini saya menyatakan bahwa makalah yang saya tulis ini adalah tulisan saya sendiri, bukan saduran, atau terjemahan dari makalah orang lain, dan bukan plagiasi.

Bandung, 26 Maret 2013



Emil Fahmi Yakhya - 13509069