**JURUSAN TEKNIK INFORMATIKA**

**FAKULTAS TEKNOLOGI INFORMASI**

**INSTITUT TEKNOLOGI SEPULUH NOPEMBER**

---

**USULAN TUGAS AKHIR**

## 1. IDENTITAS PENGUSUL

| | | |
|---|---|---|
| **NAMA** | **:** | **DHIKA WAHYU OCTAVIANI** |
| **NRP** | **:** | **5110100166** |
| **DOSEN WALI** | **:** | **Ir. MUHAMMAD HUSNI, M.Kom.** |
| **DOSEN PEMBIMBING** | **:** | **1.TOHARI AHMAD, S.Kom., MIT., Ph.D.** |
| | | **2. HENNING TITI C, S.Kom., M.Kom.** |

## 2. JUDUL TUGAS AKHIR

**"Pemanfaatan Teknologi *Near Field Communication* (NFC) sebagai Perantara Pertukaran Kartu Nama dan Permintaan Pertemanan di Jejaring Sosial Secara Otomatis dengan Sistem Keamanan Kriptografi Kunci Publik"**

## 3. LATAR BELAKANG

Kartu nama berkembang seiring dengan perkembangan manusia. Penggunaan kartu nama bertujuan sebagai media informatif, sosial, serta bisnis. Kartu nama biasanya berupa kertas kecil berisi informasi kontak sesorang seperti nama lengkap, alamat, nomor telepon, *e-mail*, dan lain-lain disesuaikan dengan kebutuhan serta profesi orang tersebut.

Selain kontak berupa alamat dan nomor telepon, kini setiap orang telah terhubung melalui jejaring sosial. Jejaring sosial tidak hanya dapat menjadi penghubung tiap individu, tetapi juga sebagai media profil perusahaan. Sehingga keberadaan jejaring sosial kini dianggap cukup krusial, tetapi *link* jejaring sosial pada kartu nama biasanya hanya menuju halaman profil saja.

Seiring dengan berkembangnya teknologi informasi maka kartu nama konvensional kini mulai berubah menjadi bentuk *digital*. Penggunaan perangkat bergerak yang semakin canggih membuat penggunaan kartu nama konvensional dianggap merepotkan, karena informasi kontak harus dimasukkan satu persatu. Selain itu kini sudah mulai jarang orang selalu membawa kartu nama cetak karena dianggap tidak praktis padahal peran kartu nama masih penting dalam kehidupan sehari-hari. Solusi termudah biasanya adalah menggunakan kamera untuk mengambil gambar kartu nama tersebut untuk disimpan. Akan tetapi tetap saja apabila akan menghubungi kontak pada kartu nama harus melihat gambar yang tersimpan dan memasukkan data secara manual.

NFC (*Near Field Communication*) merupakan teknologi yang telah banyak tertanam pada ponsel pintar masa kini yang memungkinkan komunikasi jarak dekat seperti pertukaran data. Dengan memanfaatkan teknologi ini, pertukaran data seperti kartu nama dapat lebih mudah dan cepat.

Seperti pada sistem komunikasi *wireless* lainnya, teknologi NFC juga rawan akan serangan. Beberapa jenis serangan yang memungkinkan terjadi seperti penyadapan data, modifikasi data, dan serangan *relay*. Serangan tersebut dimungkinkan saat perpindahan data dari dua perangkat sama-sama aktif melakukan pertukaran data. Jadi diperlukan sebuah sistem yang aman sehingga data pengirim maupun penerima aman dari serangan.

Pada Tugas Akhir ini akan dibuat sebuah aplikasi berbasis sistem operasi Android yang dapat melakukan komunikasi pertukaran data kartu nama yang berisi kontak serta alamat jejaring sosial dan dapat mengirimkan permintaan pertemanan secara otomatis dengan proses yang aman dengan menerapkan Kriptografi Kunci Publik. Aplikasi ini dapat memudahkan pengguna dalam proses pertukaran kartu nama untuk menyimpan kontak serta menjalin pertemanan jejaring sosial sehingga diharapkan mampu memenuhi ekspektasi pengguna terhadap sebuah metode pertukaran kartu nama yang lebih mutakhir, mudah, dan otomatis

## 4. RUMUSAN MASALAH

Rumusan masalah dari pembuatan Tugas Akhir ini adalah sebagai berikut:

a. Bagaimana membuat aplikasi manajemen kartu nama pada perangkat bergerak?
b. Bagaimana membuat metode permintaan pertemanan di jejaring sosial secara otomatis dengan fitur yang telah difasilitasi?
c. Bagaimana membuat kartu nama serta pertukaran kartu nama dengan media NFC?
d. Bagaimana menerapkan Kriptografi Kunci Publik untuk mencegah serangan pada saat pertukaran data?

## 5. BATASAN MASALAH

Dari permasalahan yang sudah disebutkan pada poin Rumusan Masalah, terdapat beberapa batasan masalah pada Tugas Akhir ini antara lain:

a. Aplikasi yang dibuat merupakan aplikasi untuk perangkat bergerak dengan sistem operasi Android.
b. Perangkat bergerak yang digunakan harus sudah tertanam *chip* NFC.
c. Bahasa pemrograman yang digunakan adalah Java.
d. Jejaring sosial yang menjadi target permintaan pertemanan otomatis adalah Facebook dan Twitter.

## 6. TUJUAN PEMBUATAN TUGAS AKHIR

Tujuan dari pembuatan Tugas Akhir ini adalah sebagai berikut:

a. Membuat aplikasi manajemen kartu nama pada perangkat bergerak.
b. Membuat metode permintaan pertemanan di jejaring sosial secara otomatis.
c. Membuat kartu nama serta pertukaran kartu nama dengan media NFC.
d. Menerapkan Kriptografi Kunci Publik untuk mencegah serangan pada saat pertukaran data.

## 7. MANFAAT TUGAS AKHIR

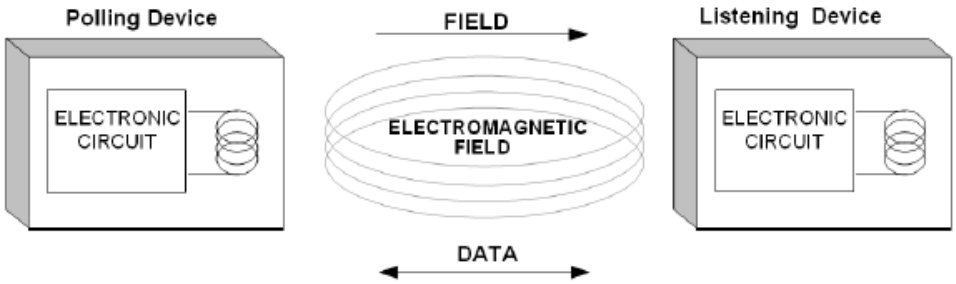
Manfaat yang diharapkan dengan adanya perancangan dan pembangunan aplikasi Tugas Akhir ini adalah mampu membantu orang lain dalam melakukan pertukaran kartu nama dengan memanfaatkan teknologi NFC yang aman dengan menerapkan Kriptografi Kunci Publik, penyimpanan data serta manajemen kartu nama yang telah diterima agar lebih mudah digunakan, dan melakukan permintaan pertemanan otomatis berdasarkan kartu nama yang diterima.

## 8. TINJAUAN PUSTAKA

### a. NFC

NFC (*Near Field Communication*) adalah teknologi *wireless* yang memiliki frekuensi tinggi (13.56 MHz) yang memiliki kecepatan pertukaran data 424 Kb/s dengan jarak jangkauan yang pendek atau dekat [1]. Alat ini dapat dipergunakan dalam pertukaran data dengan jarak sekitar 10 cm. Teknologi NFC merupakan gabungan antara *smartcard* dan *smartcard reader* yang ditanam di dalam satu perangkat, umumnya perangkat tersebut merupakan perangkat bergerak seperti telepon genggam.

Transmisi data pada NFC dilakukan dengan cara mendekatkan area kumparan konduktor yang berfungsi untuk menghubungkan dua perangkat yaitu *polling device* (inisiator) dan *listening device* (target) seperti pada Gambar 1. Frekuensi yang bekerja sebesar 13.56 MHz, dengan *bitrate* 106 Kb/s, sehingga transmisi data dapat dilakukan dengan lebih cepat dan menggunakan lebih sedikit daya.




**Gambar 1.** Konfigurasi pada Polling *Device* dan Listening *Device*

Beberapa fungsi dan kemampuan utama yang dimiliki oleh NFC antara lain:

1. Pembayaran menggunakan perangkat bergerak.
2. Media otentifikasi, dan verifikasi pada kunci elektronik.
3. Pertukaran data antar perangkat NFC secara *peer to peer.*
4. Membuka servis lainnya, seperti akses komunikasi data.
5. Membaca melalui media digital.

Komunikasi data melalui NFC juga memiliki kelemahan dari sisi keamanan [2] antara lain:

1. Penyadapan

   Sinyal radio yang digunakan untuk melakukan pertukaran data antara perangkat 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*

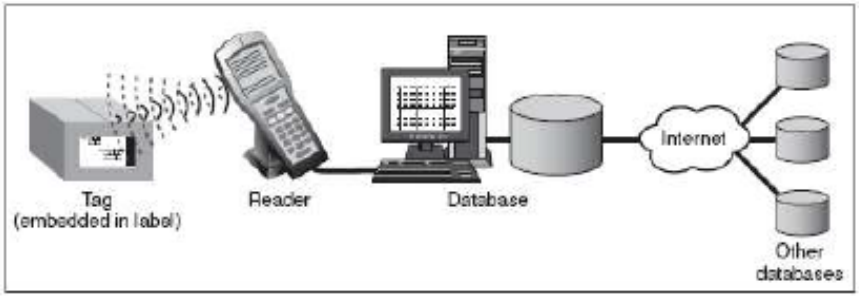
   Dikarenakan NFC termasuk ke dalam protokol ISO/IEC 14443, serangan *relay* sangat *feasible* untuk dilakukan pada NFC. Serangan ini menggunakan prinsip dengan cara mendahului permintaan pertukaran data antara pengirim dan penerima, kemudian penyerang memberikan data kepada pengirim dan penerima seakan-akan data tersebut adalah data yang valid.

**b. RFID**

RFID (*Radio-Frequency IDentification*) adalah proses identifikasi seseorang atau objek dengan menggunakan frekuensi transmisi radio [3]. RFID menggunakan frekuensi radio untuk membaca informasi dari sebuah perangkat kecil yang disebut *tag* atau *transponder* (*Transmitter + Responder*). *Tag* RFID akan mengenali diri sendiri ketika mendeteksi sinyal dari perangkat yang kompatibel, yaitu pembaca RFID (*Micro-Reader*).

Gambar 2 menjelaskan sistem RFID, yang terdiri dari empat komponen:

1. *Tag*
   Perangkat yang menyimpan informasi untuk identifikasi objek. *Tag* RFID sering juga disebut sebagai *transponder*.
2. Antena
   Berfungsi mentransmisikan sinyal frekuensi radio antara pembaca RFID dengan *tag* RFID.
3. Pembaca RFID (Micro-Reader)
   Alat yang kompatibel dengan *tag* RFID yang akan berkomunikasi secara *wireless* dengan *tag*.
4. *Software* Aplikasi
   Aplikasi pada sebuah *workstation* atau PC yang dapat membaca data dari *tag* melalui pembaca RFID. Baik *tag* dan pembaca RFID dilengkapi dengan antena sehingga dapat menerima dan memancarkan gelombang elektromagnetik.




**Gambar 2.** Komponen Utama Sistem RFID

**c. Jejaring Sosial**

Situs jejaring sosial yang dalam bahasa Inggris disebut *social network sites* merupakan sebuah *web* berbasis pelayanan yang memungkinkan penggunanya untuk membuat profil, melihat daftar pengguna yang tersedia, serta mengundang atau menerima teman untuk bergabung dalam situs tersebut. Tampilan dasar situs jejaring sosial ini menampilkan halaman profil pengguna, yang di dalamnya terdiri dari identitas diri dan foto pengguna [4].

Keberadaan situs jejaring sosial ini memudahkan kita untuk berinteraksi secara mudah dengan orang-orang dari seluruh belahan dunia dengan biaya yang lebih murah dibandingkan menggunakan telepon [4].

Jejaring social merupakan sebuah fenomena baru yang memberikan pengaruh terhadap seluruh aspek kehidupan manusia. Hampir semua orang kini melakukan

interaksi lebih banyak melalui jejaring sosial daripada media lainnya. Perkembangan teknologi juga turut menyumbang pengaruh perkembangan jejaring sosial karena setiap orang kini dapat mengakses akun jejaring sosial masing-masing untuk mengetahui berita terbaru melalui perangkat bergerak [5].

**d. Kriptografi Kunci Publik**

Teknik yang digunakan dalam kriptografi kunci publik adalah penggunaan algoritma *Asymmetric Key* dimana kunci yang digunakan untuk enkripsi adalah kunci yang berbeda dengan kunci yang digunakan untuk dekripsi. Tiap pengguna memiliki sepasang kunci kriptografi, Kunci Publik untuk enkripsi dan Kunci Privat untuk dekripsi. Kunci Publik untuk mengenkripsi disebarkan secara luas, sedangkan kunci privat hanya akan diketahui oleh penerima pesan. Pesan akan dienkripsi oleh Kunci Publik pengirim dan hanya akan bisa didekripsi oleh Kunci Privat yang benar. Kedua kunci berhubungan secara matematis, dan algoritma yang dapat menghasilkan pasangan kedua kunci tersebut mulai berkembang pada pertengahan tahun 1970 [6].

Keuntungan dari Kriptografi Kunci Publik antara lain adalah:

1. Tidak diperlukan pengiriman kunci rahasia.
2. Jumlah kunci dapat ditekan.

Sistem Kriptografi Kunci Publik yang aman didasarkan pada fakta [6]:

1. Komputasi untuk enkripsi/dekripsi pesan mudah dilakukan.
2. Secara komputasi hampir tidak mungkin menurunkan Kunci Privat, bila diketahui Kunci Publik pasangannya.

**e. Android SDK**

Android SDK adalah *software development kit*, yang bisa dikembangkan untuk membuat sebuah aplikasi ataupun *game* untuk digunakan dalam *platform* Android. Dalam Android *software development kit* terdapat *sample project*, SDK, *development tools*, emulator, dan *libraries* untuk membangun sebuah aplikasi Android. Aplikasi Android ini dapat ditulis dengan menggunakan bahasa pemrograman Java [7].

## 9. RINGKASAN ISI TUGAS AKHIR

Pada Tugas Akhir ini, akan dibuat sebuah aplikasi yang memudahkan pengguna dalam melakukan pertukaran kartu nama melalui teknologi NFC dan dapat melakukan permintaan pertemanan otomatis pada jejaring sosial yang tersimpan pada kartu nama dan aman karena juga menerapkan kriptografi Kunci Publik.

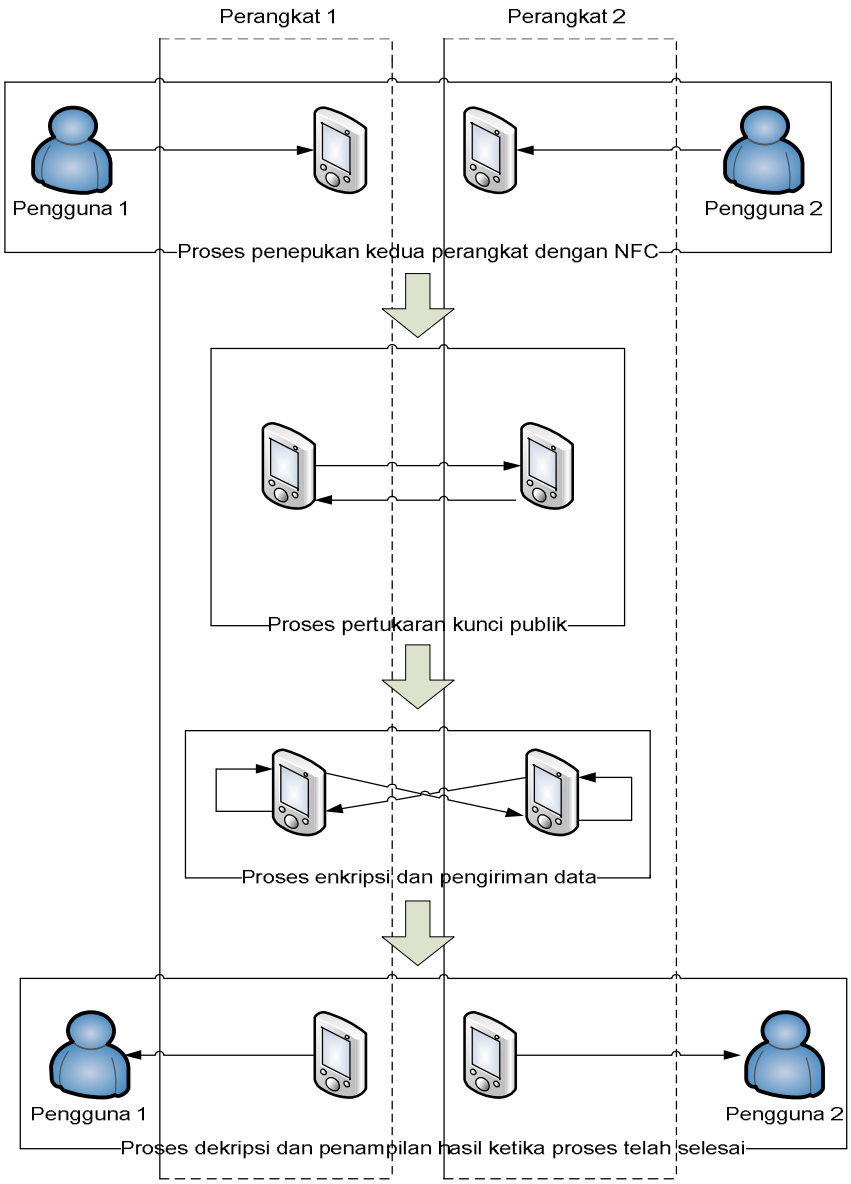
Aplikasi yang akan dibuat dapat melakukan penulisan dan penyimpanan data kartu nama pada perangkat bergerak pemilik. Kartu nama ini berisi data pemilik seperti nama, nomor telepon, alamat, email, serta alamat jejaring sosial pemilik. Dengan melakukan pertukaran kartu nama melalui aplikasi ini maka salah satu pihak akan menjadi inisiator, dan pihal lainnya akan menjadi target.

Selain bertukar kartu nama, proses lain yang akan terjadi adalah inisiator akan melakukan permintaan pertemanan pada media sosial milik target. Hal ini akan menjadi

nilai lebih dari aplikasi yang akan dibuat mengingat banyak yang mengharapkan semua proses dapat berlangsung secara otomatis, tidak hanya menyimpan data pertukaran kartu nama.

Gambar 3 akan menjelaskan arsitektur aplikasi secara keseluruhan. Terdapat empat proses utama yaitu:

1. Proses Penepukan Perangkat
   Proses awal untuk memulai pertukaran perangkat dengan cara mendekatkan perrangkat dan menyambungkan melalui NFC.
2. Proses Pertukaran Kunci Publik
   Proses untuk saling mengirimkan Kunci Publik dari masing-masing perangkat sehingga memastikan kedua perangkat memilki Kunci Publik. Kunci Publik yang diterima ini akan menjadi kunci untuk proses enkripsi data masing–masing pengguna.
3. Proses Enkripsi dan Pengiriman Data
   Proses enkripsi menggunakan Kunci Publik lawan yang sudah diterima oleh masing–masing pengguna dilakukan di masing-masing perangkat. Lalu perangkat yang telah melakukan enkripsi seling bertukar data.
4. Proses Penampilan Data Akhir
   Proses menampilkan data diawali dengan dekripsi data yang diterima dengan Kunci Privat yang dimiliki. Lalu dilanjutkan dengan proses penyimpanan kartu nama. Setelah kartu nama tersimpan maka dilakukan proses permintaan pertemanan di jejaring sosial.




**Gambar 3.** Arsitektur Keseluruhan Aplikasi

## 10. METODOLOGI

### a. Penyusunan proposal Tugas Akhir

Penyusunan proposal Tugas Akhir merupakan tahap awal dalam proses pengerjaan Tugas Akhir. Dalam proposal ini diajukan gagasan "Pemanfaatan Teknologi *Near Field Communication* (NFC) sebagai Perantara Pertukaran Kartu Nama dan Permintaan Pertemanan di Jejaring Sosial Secara Otomatis dengan Sistem Keamanan Kriptografi Kunci Publik".

**b. Studi literatur**

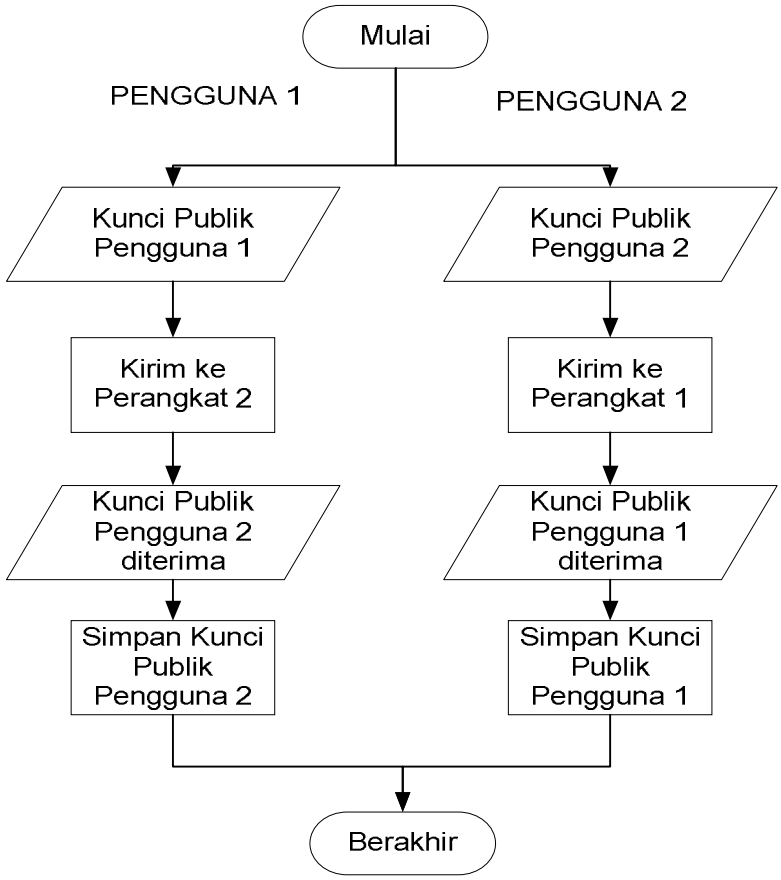
Literatur yang akan dipelajari antara lain teknologi NFC, teknologi RFID, API jejaring sosial, Android SDK, dan bahasa pemrograman Java.

**c. Analisis dan desain perangkat lunak**

Dalam aplikasi ini, akan dimulai dengan proses penepukan kedua perangkat lunak sebagai proses pemasangan kedua perangkat. Proses berikutnya adalah proses pertukaran kunci publik antar kedua perangkat sehingga nantinya perangkat bisa mendekripsi data yang diterima. Selanjutnya adalah proses enkripsi dan pengiriman data serta proses yang terakhir adalah penampilan data. Pada Gambar 4, Gambar 5, dan Gambar 6 akan diilustrasikan proses-proses yang terjadi pada aplikasi.

1. Flowchart Proses Pertukaran Kunci Privat

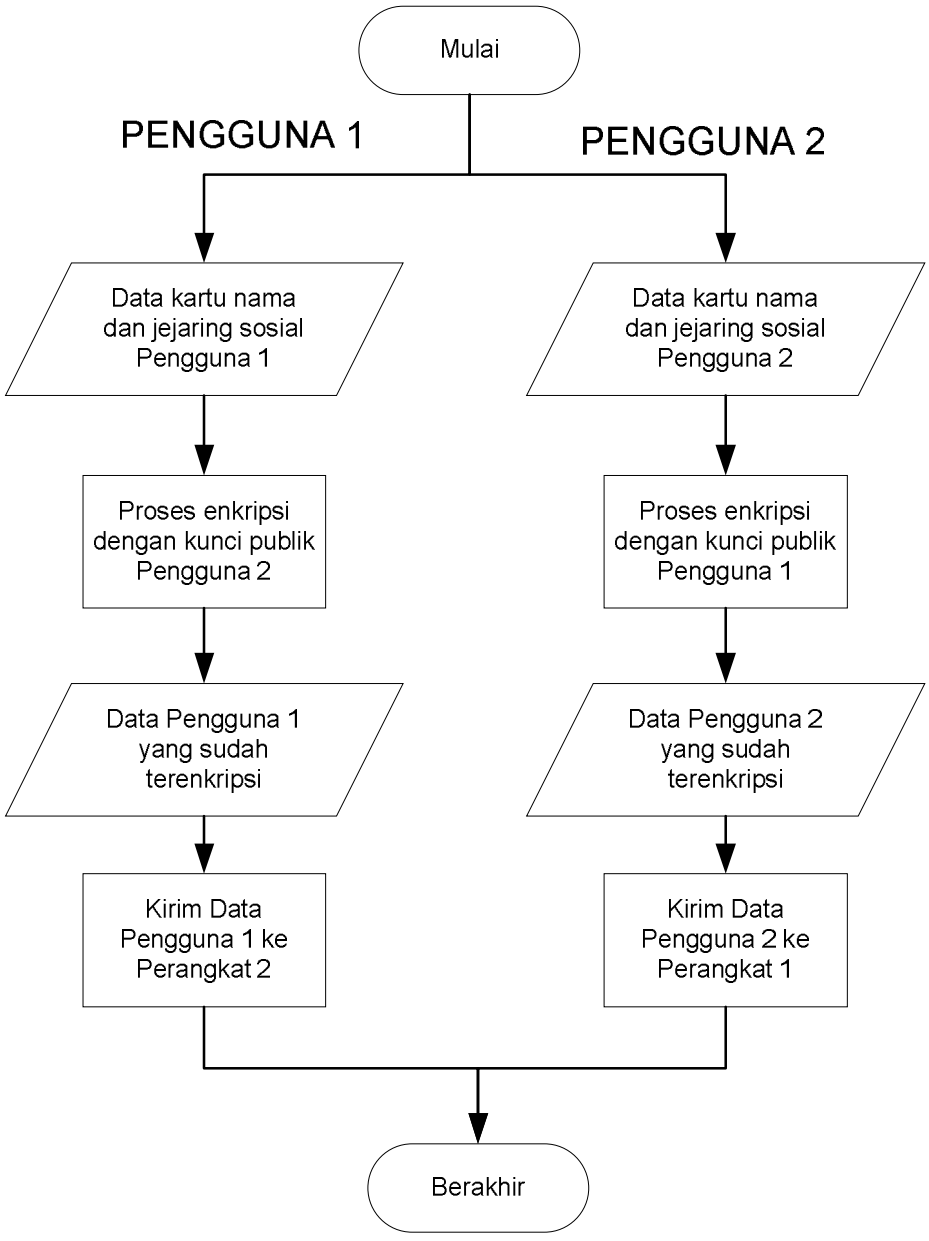
Pada Gambar 4 diilustrasikan alur proses untuk saling mengirimkan Kunci Publik dari masing-masing perangkat. Fungsinya adalah untuk memastikan kedua perangkat memilki Kunci Publik. Kunci Publik yang diterima ini akan menjadi kunci untuk proses dekripsi data yang diterima.




**Gambar 4.** Flowchart Pertukaran Kunci Publik

2. Flowchart Proses Enkripsi Data dan Pengiriman Data

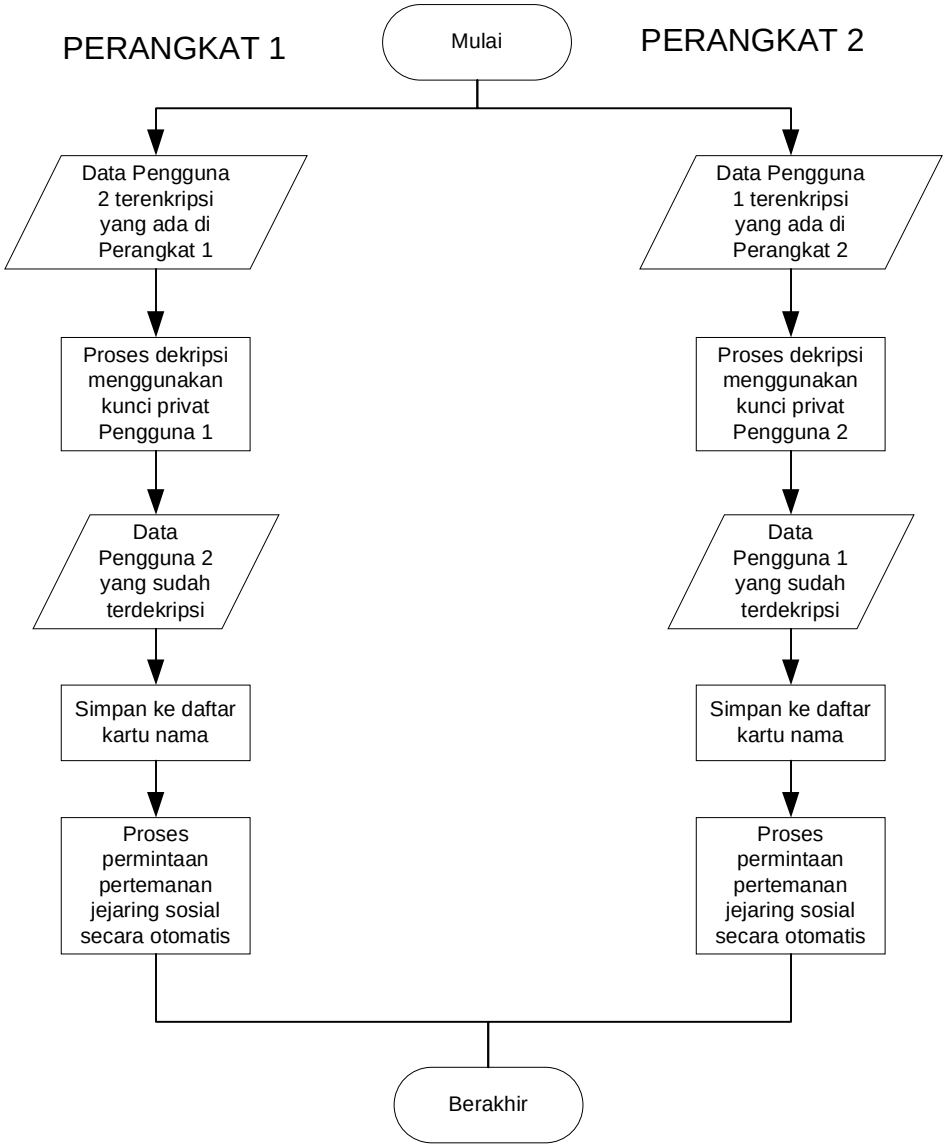
Pada Gambar 5 alur proses diawali enkripsi yang dilakukan di masing-masing perangkat. Lalu data kartu nama perangkat yang telah dienkripsi saling mengirimkan data.




**Gambar 5.** Flowchart Enkripsi Data dan Pengiriman Data

3. Flowchart Proses Penampilan Data Akhir

Pada Gambar 6 proses yang diilustrasikan dimulai dengan dekripsi data yang telah diterima dengan Kunci Privat yang dimiliki oleh masing–masing pengguna. Selanjutnya kartu nama yang telah didekripsi disimpan di masing-masing perangkat penerima. Lalu berdasarkan data yang telah diterima dilakukan proses permintaan pertemanan di jejaring sosial.




**Gambar 6.** Flowchart Penampilan Data Akhir

### d. Implementasi perangkat lunak

Rencana pembuatan perangkat lunak ini akan diimplementasikan sebagai berikut:

1. IDE yang digunakan adalah Eclipse.
2. Menggunakan android SDK.

### e. Penyusunan Buku Tugas Akhir

Pada tahap ini dilakukan penyusunan laporan yang menjelaskan dasar teori dan metode yang digunakan dalam Tugas Akhir ini serta hasil dari implementasi

aplikasi perangkat lunak yang telah dibuat. Sistematika penulisan buku Tugas Akhir secara garis besar antara lain:

1. Pendahuluan
   a. Latar Belakang
   b. Rumusan Masalah
   c. Batasan Tugas Akhir
   d. Tujuan
   e. Metodologi
   f. Sistematika Penulisan
2. Tinjauan Pustaka
3. Desain dan Implementasi
4. Pengujian dan Evaluasi
5. Kesimpulan dan Saran
6. Daftar Pustaka

## 11. JADWAL KEGIATAN

Pengerjaan Tugas Akhir ini akan dilakukan sesuai jadwal yang tertera pada Tabel 1.

**Tabel 1.** Tabel jadwal kegiatan pengerjaan Tugas Akhir

| Tahapan | 2014 | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Maret | | | | April | | | | Mei | | | | Juni | | | |
| Penyusunan Proposal | | | ■ | ■ | | | | | | | | | | | | |
| Studi Literatur | | | ■ | ■ | ■ | ■ | ■ | ■ | | | | | | | | |
| Perancangan sistem | | | | | | | ■ | ■ | ■ | ■ | ■ | ■ | | | | |
| Implementasi | | | | | | | | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ |
| Pengujian dan evaluasi | | | | | | | | | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ |
| Penyusunan buku | | | | | | | | | | | ■ | ■ | ■ | ■ | ■ | ■ |

## 12. DAFTAR PUSTAKA

[1] R. Minihold, "Near Field Communication (NFC) Technology and Measurements," 2011. [Online]. Available: http://www.rohde-schwarz.com/en/applications/near-field-communication-nfc-technology-and-measurements-application-note_56280-15836.html.

[2] K. B. Ernst Haselsteiner, "Security in Near Field Communication (NFC)," Philips, [Online]. Available: http://ece.wpi.edu/~dchasaki/papers/Security%20in%20NFC.pdf. [Accessed 21 Maret 2014].

[3] D. Supriatna, "Studi Mengenai Aspek Privasi pada Sistem RFID," Sekolah Teknik Elektro dan Informatika, Institut Teknologi Bandung, Bandung, 2007.

[4] S. Dirgayuza, Panduan Praktis Mengoptimalkan Facebook, Jakarta: Media Kita, 2011.

[5] A. Kaplan, "Users of the world, unite! The challenges and opportunities of Social Media," *Business Horizons,* vol. 53, no. 1, pp. 59-68, 2010.

[6] T. Hidayat, "Public Key Cryptography," Sekolah Teknik Elektro dan Informatika, Institut Teknologi Bandung, Bandung, 2011.

[7] A. SDK, "Android," [Online]. Available: http://www.android.pk/android-sdk.html. [Accessed 20 Maret 2014].