Implementasi dan Analisis Performa Algoritma Enkripsi ChaCha20 Berbasis Protokol Komunikasi ESP-NOW Pada Wireless Sensor Network

Disusun oleh:

Naufal Farras Trikusuma

NIM: 215150301111047



**PROGRAM STUDI TEKNIK KOMPUTER**

**DEPARTEMEN TEKNIK INFORMATIKA**

**FAKULTAS ILMU KOMPUTER**

**UNIVERSITAS BRAWIJAYA**

**MALANG**

**2024**

DAFTAR ISI

[DAFTAR ISI ii](#_Toc496077787)

[DAFTAR TABEL iv](#_Toc496077788)

[DAFTAR GAMBAR v](#_Toc496077789)

[DAFTAR LAMPIRAN vi](#_Toc496077790)

[BAB 1 PENDAHULUAN 1](#_Toc496077791)

[1.1 Latar Belakang 1](#_Toc496077792)

[1.2 Rumusan Masalah 1](#_Toc496077793)

[1.3 Tujuan 4](#_Toc496077794)

[1.4 Manfaat 6](#_Toc496077795)

[1.5 Batasan Masalah 6](#_Toc496077796)

[1.6 Sistematika Pembahasan 7](#_Toc496077797)

[BAB 2 LANDASAN KEPUSTAKAAN 8](#_Toc496077798)

[2.1 Isi Landasan Kepustakaan 8](#_Toc496077799)

[2.1.1 Ringkasan dan Sintesis 8](#_Toc496077800)

[2.1.2 Referensi dan Judul Bab 9](#_Toc496077801)

[2.2 Persamaan, Tabel, Gambar, dan Simbol 9](#_Toc496077802)

[2.2.1 Persamaan 9](#_Toc496077803)

[2.2.2 Tabel 9](#_Toc496077804)

[2.2.3 Gambar 11](#_Toc496077805)

[2.2.4 Lambang, Satuan, dan Singkatan 12](#_Toc496077806)

[2.2.5 Tanda Sitasi Tabel dan Gambar dari Sumber Lain 13](#_Toc496077807)

[2.2.6 Daftar Pernyataan 14](#_Toc496077808)

[2.2.7 Kode Sumber 14](#_Toc496077809)

[BAB 3 METODOLOGI 16](#_Toc496077810)

[3.1 Isi Metodologi 16](#_Toc496077811)

[3.1.1 Komponen-komponen Metodologi 16](#_Toc496077812)

[3.1.2 Penomoran Subbab 17](#_Toc496077813)

[3.2 Lain-lain 17](#_Toc496077814)

[DAFTAR REFERENSI 18](#_Toc496077815)

[LAMPIRAN A PERSYARATAN FISIK DAN TATA LETAK 21](#_Toc496077816)

[LAMPIRAN B PENGGUNAAN BAHASA 23](#_Toc496077817)

DAFTAR TABEL

[Tabel ‎2.1 Pembentukan bilangan random untuk Indeks Masa Tubuh (IMT) 2](#_Toc175521661)

[Tabel ‎2.2 Contoh tabel 2 3](#_Toc175521662)

DAFTAR GAMBAR

[Gambar ‎2.1 Pengaruh nilai K terhadap akurasi 12](#_Toc496077820)

DAFTAR LAMPIRAN

[LAMPIRAN A PERSYARATAN FISIK DAN TATA LETAK 21](#_Toc496077821)

[A.1 Kertas 21](#_Toc496077822)

[A.2 Margin 21](#_Toc496077823)

[A.3 Jenis dan ukuran huruf 21](#_Toc496077824)

[A.4 Spasi 21](#_Toc496077825)

[A.5 Kepala Bab dan Subbab 21](#_Toc496077826)

[A.6 Nomor halaman 22](#_Toc496077827)

[LAMPIRAN B PENGGUNAAN BAHASA 23](#_Toc496077828)

# PENDAHULUAN

Pada bab pendahuluan ini berisi penelitian yang berisikan uraian mengenai latar belakang penelitian, rumusan masalah yang diangkat penulis, tujuan dan manfaat penelitian, serta batasan masalah dari lingkup penelitian ini. Pada bab ini terdapat sistematika penulisan mengenai isi secara umum dari setiap bab yang terdapat dalam penelitian ini.

## Latar Belakang

Perkembangan teknologi pada bidang wireless sensor network dalam beberapa tahun terakhir memiliki fungsionalitas yang beragam untuk membantu proses automasi pekerjaan manusia seperti proses untuk pengumpulan data dari sensor, pengendalian sistem secara nirkabel, dan monitoring/pengawasan. Menurut Astuti dan Wibisono (2017), Jaringan Sensor Nirkabel (Wireless sensor network/WSN) merupakan kumpulan jaringan node sensor yang saling berkomunikasi untuk melakukan pemindaian dan pengiriman/penerimaan data secara nirkabel yang memiliki keterbatasan pada sumber daya dan kemampuan komunikasi.

Pada aplikasi WSN, keamanan data merupakan aspek penting yang perlu diperhatikan khususnya pada komunikasi yang dilakukan pada jaringan lokal ataupun internet. Data atau informasi yang ditransmisikan pada beberapa kasus merupakan data privat dan sensitif yang perlu diamankan karena dapat mengakibatkan data breach dan unauthorized access oleh orang yang tidak bertanggung jawab (Sarker et al, 2020). Oleh karena itu, diperlukan penggunaan metode kriptografi seperti menggunakan algoritma enkripsi pada data yang akan ditransmisikan untuk meningkatkan keamanan pada aspek konfidensialitas dan integritas.

Perangkat pada sistem tertanam dan/atau WSN memiliki kapasitas komputasi dan sumber daya yang rendah seperti terbatasnya random access memory (RAM), penyimpanan internal, daya komputasi pada prosesor, dan energi/sumber daya seperti baterai. Perangkat seperti ini tidak dapat mengalokasikan secara besar penggunaan sumber daya komputasi hanya untuk aspek keamanan. Oleh karena itu, diperlukan lightweight cryptography (LWC) yang diharapkan dapat mengeksekusi algoritma kriptografi yang lebih ringan atau dengan penggunaan sumber daya komputasi yang lebih rendah dibandingkan teknik kriptografi konvensional dan masih dapat menyediakan fungsi keamanan yang kuat untuk menanggulangi security attacks (Gunathilake et al, 2019).

Algoritma enkripsi ChaCha20 adalah stream cipher berkecepatan tinggi yang dirancang oleh D. J. Bernstein pada tahun 2008 sebagai penyempurnaan dari stream cipher Salsa20. ChaCha20 merupakan alternatif algoritma pada Transport Layer Security (TLS) protokol yang bertujuan untuk meningkatkan batas keamanan tanpa mengorbankan kinerja pada platform perangkat lunak namun menghasilkan performa high-throughput stream cipher. (Santis et al, 2017).

Penelitian ini mengangkat masalah keamanan data dan keterbatasan sumber daya pada perangkat dalam aplikasi Wireless Sensor Network (WSN). Solusi yang ditawarkan adalah menganalisis performa algoritma enkripsi ChaCha20 dengan algoritma lainnya pada protokol komunikasi ESP-NOW berbasis ESP32. Pengujian meliputi kecepatan enkripsi, dekripsi, key setup, serta uji penetrasi seperti sniffing dan known-plaintext attack (KPA). Selain itu, penelitian ini juga menilai penggunaan sumber daya pada mikrokontroler, untuk menentukan apakah algoritma ChaCha20 efektif dalam memberikan keamanan pada WSN yang memiliki keterbatasan sumber daya.

## Rumusan Masalah

Berdasarkan latar belakang yang telah dipaparkan diatas, rumusan masalah dalam penelitian ini adalah sebagai berikut:

1. Bagaimana performa algoritma ChaCha20 dalam hal waktu komputasi pada perangkat ESP32?

2. Bagaimana pengaruh penggunaan algoritma enkripsi ChaCha20 terhadap penggunaan sumber daya komputasi pada ESP32?

3. Bagaimana implementasi algoritma enkripsi ChaCha20 pada protokol komunikasi ESP-NOW dan hasil pengujian algoritma dalam aspek keamanan?

## Tujuan

Adapun beberapa tujuan yang ingin dicapai oleh penulis dari penelitian ini adalah sebagai berikut:

1. Menganalisis dan evaluasi performa algoritma ChaCha20 dalam hal waktu waktu komputasi pada perangkat ESP32.
2. Menganalisis pengaruh penggunaan algoritma enkripsi ChaCha20 terhadap penggunaan sumber daya komputasi pada ESP32.
3. Mengetahui implementasi dan evaluasi aspek keamanan algoritma enkripsi ChaCha20 pada protokol komunikasi ESP-NOW.

## Manfaat

Penelitian ini diharapkan dapat bermanfaat bagi para peneliti atau masyarakat terkhusus dalam mengimplementasikan dan menggunakan algoritma keamanan pada sistem WSN. Sehingga pembaca dapat memilih lebih tepat algoritma enkripsi yang lebih hemat sumber daya, cepat, dan aman pada sistem atau penelitian selanjutnya. Selain itu, penulis berharap agar masyarakat yang membaca skripsi ini dapat meningkatkan pemahaman mengenai aspek keamanan yang efisien pada *wireless sensor network*.

## Batasan Masalah

Agar lingkup penelitian ini lebih spesifik dan keterbatasan pengujian maka perlu adanya beberapa batasan masalah, yaitu:

1. Implementasi sistem berupa prototipe menggunakan 3 perangkat ESP32.
2. Subjek pengujian dalam perbandingan performa algoritma sebanyak 2.

## Sistematika Pembahasan

Pada sistematika pembahasan terdapat penjelasan umum tiap bagian bab yang terdapat dalam penelitian ini. Penelitian ini dibagi pada beberapa bagian bab yang sesuai dengan alur penelitian. Sistematika penulisan skripsi dibagi menjadi beberapa bab, yaitu:

**BAB I PENDAHULUAN**

Bab ini memiliki beberapa subbab berisikan latar belakang dari penelitian, rumusan masalah dari latar belakang penelitian, tujuan, manfaat, batasan masalah, dan sistematika pembahasan skripsi.

**BAB II LANDASAN KEPUSTAKAAN**

Bab ini memuat kajian atau tinjauan kepustakaan dan landasan teori dari penelitian sebelumnya. Tinjauan dan landasan teori yang digunakan akan memiliki keterkaitan dengan teori dan implementasi dari penelitian ini sebagai landasan metode dan referensi.

**BAB III METODOLOGI PENELITIAN**

Bab ini berisikan alur proses dan metode yang akan digunakan dalam penelitian ini. Pada bab III secara lebih spesifik akan dimuat mengenai metode yang akan digunakan oleh penulis seperti diagram alir dan penjelasan prosesnya.

**BAB IV REKAYASA KEBUTUHAN**

Bab ini memuat pengkajian masalah secara umum, kebutuhan fungsional yang dimiliki sistem meliputi perangkat lunak, perangkat keras, dan alat yang digunakan dalam pengujian.

**BAB V PERANCANGAN DAN IMPLEMENTASI**

Bab ini berisikan proses perancangan dan implementasi sistem, yaitu bagaimana merancang sistem dari perangkat lunak dan perangkat keras berdasarkan rekayasa kebutuhan seperti membuat blok diagram, skematik, konfigurasi sistem, dan diagram alir hingga proses implementasi sistem.

**BAB VI PENGUJIAN DAN ANALISIS**

Bab ini berisikan hasil pengujian untuk menganalisis dan mengevaluasi kinerja sistem secara keseluruhan. Pada bab ini juga akan terdapat jawaban daripada rumusan masalah yang ada.

**BAB VII PENUTUP**

Bab ini memuat kesimpulan dan saran yang didapat setelah penelitian dilakukan berdasarkan hasil pengujian dan analisis. Saran dan kesimpulan penelitian diharapkan dapat meningkatkan penelitian selanjutnya dari hasil penelitian penulis.

# LANDASAN KEPUSTAKAAN

Landasan kepustakaan berisi uraian dan pembahasan tentang teori, konsep, model, metode, atau sistem dari pustaka ilmiah, yang berkaitan dengan tema, masalah, atau pertanyaan penelitian. Dalam landasan kepustakaan terdapat landasan teori dari berbagai sumber pustaka yang terkait dengan teori dan metode yang digunakan dalam penelitian. Jika dibutuhkan sesuai dengan karakteristik penelitiannya dan syarat kecukupan khusus keminatan tertentu, bisa juga terdapat kajian pustaka yang menjelaskan secara umum penelitian-penelitian terdahulu yang berhubungan dengan topik skripsi dan menunjukkan persamaan dan perbedaan skripsi tersebut terhadap penelitian terdahulu yang dituliskan.

## Tinjauan Kepustakaan

Pada saat dimulai penelitian, penulis meninjau beberapa literatur dan jurnal yang berhubungan/berkaitan dengan penelitian untuk mendapatkan informasi dan referensi dalam penelitian ini. Berikut adalah isi dari kajian pustaka yang berisikan penelitian-penelitian sebelumnya, dapat dilihat pada Tabel.2.1.

Tabel 2.1 Daftar Tinjauan Pustaka

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| No. | Nama Penulis (Tahun),  Judul Penelitian | Persamaan Penelitian | Perbedaan | |
| Penelitian Sebelumnya | Penelitian Sekarang |
| 1 | Hyeopgeon et al (2010) *"Implementation and Performance Analysis of AES-128 CBC algorithm in WSNs."* | Menggunakan algoritma enkripsi pada WSN dan pengujian performa sebagai subjek penelitian. | MenggunakanATmega644p 8-bit, pengujian performa algoritma AES CBC pada kecepatan komputasi. | Menggunakan  ESP32, pengujian performa algoritma chacha20 pada penggunaan sumber daya komputasi. |
| 2 | Imran et al (2022) “*Implementasi Algoritme Clefia 128-Bit untuk Pengamanan Modul Komunikasi Lora.* ” | Menggunakan algoritma enkripsi pada WSN dan pengujian keamanan algoritma sebagai subjek penelitian. | Menggunakan  arduino uno, modul LoRa, pengujian algoritma clefia 128-bit. | Menggunakan  ESP32 dan protokol ESP-NOW, pengujian performa algoritma chacha20. |
| 3 | *Pratama et al (2021),*  *“Implementasi Algoritma Enkripsi Snow-V pada Wireless Sensor Network (WSN)”* | Menggunakan algoritma enkripsi pada WSN, pengujian performa dan keamanan algoritma sebagai subjek penelitian. | Menggunakan  arduino uno, modul nRF24L01, pengujian performa algoritma snow-v. | Menggunakan  ESP32 dan protokol ESP-NOW, pengujian performa algoritma chacha20 |

### Ringkasan dan Sintesis

Dalam membuat ringkasan, informasi teoritik yang dipilih dari sumber pustaka haruslah yang benar-benar relevan dengan masalah penelitian. Oleh karena itu, peneliti harus kritis dalam menyeleksi informasi. Kemudian, untuk menjaga agar informasi yang dipilih memang berasal dari studi atau kajian ilmiah, disarankan menggunakan sumber-sumber pustaka ilmiah, seperti jurnal, prosiding konferensi atau seminar, tesis, disertasi, skripsi, atau buku teks, dan dihindari sumber-sumber yang tidak jelas penulisnya atau kapasitas penulisnya. Jika informasi yang diambil dimaksudkan untuk pembahasan teori, konsep, atau metode terkini, maka sebaiknya sumber yang digunakan adalah yang semutakhir mungkin. Akan tetapi, jika informasi yang dimaksud adalah informasi yang memang sudah ada sejak lama, misalkan tentang teori yang sangat mendasar, sumber untuk informasi tersebut bisa saja merupakan sumber yang telah lama dipublikasikan.

Menurut Berndtsson et al. (2008), dalam melakukan sintesis, informasi teoritik sebaiknya dijelaskan mulai dari informasi yang lebih umum dan secara bertahap menuju ke yang lebih khusus. Penulis juga seharusnya menjelaskan aspek-aspek mana dari informasi teoritik tersebut yang langsung berhubungan atau menjadi dasar dari masalah penelitian, serta bagaimana aspek tersebut berhubungan dengan masalah penelitian (Rumbaugh et al., 2005; Brodjonegoro, 2009a; Sommerville, 2011).

### Referensi dan Judul Bab

Ketika harus mengacu informasi dari sumber pustaka, penulis wajib memberikan apresiasi kepada penulis pustaka tersebut dengan cara menuliskan identitas pustaka tersebut beserta penulisnya dalam daftar referensi dan mereferensi informasi tersebut dari badan tulisan dengan cara yang tepat.

## Dasar Teori

Pada dasar teori akan dijelaskan teori-teori yang digunakan dalam mengimplementasikan penelitian ini. Dengan adanya pengertian, persamaan, dan cara kerja yang diharapkan dapat sebagai penunjang pemahaman dalam penelitian.

### Wireless Sensor Network

Jaringan Sensor Nirkabel(Wireless sensor network)  merupakan kumpulan jaringan *node* sensor yang saling berkomunikasi untuk melakukan pemindaian dan pengiriman/penerimaan data secara nirkabel yang memiliki keterbatasan pada sumber daya dan kemampuan komunikasi (Astuti dan Wibisono, 2017).

### Kriptografi

Kriptografi adalah konsep penyandian yang digunakan untuk menjaga kerahasiaan data, sehingga hanya pihak yang berwenang yang dapat mengetahui informasi dari data tersebut. Dalam kriptografi, data asli (plaintext) akan dienkripsi menjadi ciphertext dan kemudian didekripsi kembali menjadi plaintext ketika diterima oleh pihak yang berhak. Saat ini, algoritma modern banyak digunakan untuk mengamankan data, yang secara umum dibagi menjadi dua jenis, yaitu stream ciphers dan block ciphers. Stream ciphers bekerja dengan melakukan operasi XOR antara keystream dan plaintext untuk menghasilkan ciphertext. (Qadir dan Varol, 2019).

### Algoritma ChaCha20

ChaCha20 adalah stream cipher berkecepatan tinggi yang dirancang oleh D. J. Bernstein pada tahun 2008 sebagai penyempurnaan dari stream cipher Salsa20. ChaCha20 merupakan alternatif algoritma pada *Transport Layer Security* (TLS) protokol yang bertujuan untuk meningkatkan batas keamanan tanpa mengorbankan kinerja pada platform perangkat lunak namun menghasilkan performa *high-throughput stream cipher*. (Santis et al, 2017).

Setiap persamaan yang digunakan harus diberi nomor berurutan berdasar bab dan urutan munculnya persamaan. Huruf pertama suatu persamaan dimulai setelah 10 ketikan spasi dari batas kiri. Nomor persamaan ditulis di kanan persamaan dan ditempatkan pada batas kanan halaman dalam tanda kurung. Bilangan pertama menunjukkkan bab letak persamaan tersebut dan bilangan kedua yang dipisahkan tanda hubung merupakan nomor urutan persamaan dalam bab tersebut. Contoh persamaan ke-10 dalam bab kedua adalah:

 (2.10)

Ketika persamaan ini diacu dari dalam teks maka dapat dituliskan sebagai Persamaan 2.10.

Sebuah gambar tidak berdiri sendiri tanpa teks yang merujuknya. Gambar dapat mengilustrasikan apa yang disebutkan dalam teks atau sebaliknya teks dapat menjelaskan apa yang berada dalam gambar. Gambar yang berada pada lampiran juga tetap harus dirujuk dari teks dalam bagian utama.

### Lambang, Satuan, dan Singkatan

Penulisan lambang atau simbol sebaiknya menggunakan fasilitas simbol atau jenis huruf Symbol yang ada pada program komputer pengolah kata untuk membedakannya dengan huruf biasa. Sebagai contoh untuk tanda perkalian tidak menggunakan huruf x tetapi “×” dari symbol. Untuk rumus matematika diusahakan ditulis dalam satu baris. Bila hal ini tidak memungkinkan maka harus diatur sedemikian rupa agar mudah dimengerti.

Satuan dan singkatan yang digunakan adalah yang lazim dipakai dalam disiplin ilmu terkait, misalnya 25°C; 10 ppm; H2O; dan sebagainya. *Superscript* dan *subscript* sebaiknya digunakan ketika diperlukan.

### Tanda Sitasi Tabel dan Gambar dari Sumber Lain

Tabel atau gambar yang direproduksi dari sumber lain, baik itu disalin langsung secara keseluruhan, atau diadaptasi (misalnya, disesuaikan bentuk dan formatnya, atau ditambahkan keterngan legenda dengan tidak mengubah arti), harus dibuatkan referensinya dalam daftar referensi dan sitasinya di bawah tabel atau gambar tersebut.

Contoh:

Referensi dalam daftar referensi:

Angriawan, B., 2014. Sistem pakar untuk penentuan kondisi tubuh ideal atlet sepakbola usia remaja. S1. Universitas Malang Raya.

Sitasi untuk tabel yang disalin langsung:

**Tabel 3.1 Pembentukan bilangan random untuk Indeks Masa Tubuh (IMT)**

|  |  |  |
| --- | --- | --- |
| No | Keanggotaan IMT | Rentang Nilai |
| 1 | Sangat Kurus | 0.0 - 19.0 |
| 2 | Kurus | 15.0 - 20.0 |
| 3 | Normal | 17.0 - 27.0 |
| 4 | Gemuk | 23.0 - 29.0 |
| 5 | Obesitas | 25.0 - 50.0 |
| Sumber: Anggariawan (2014) | | |

Cara menyitasi untuk tabel yang diadaptasi:

**Tabel 3.1 Pembentukan bilangan random untuk Indeks Masa Tubuh (IMT)**

| **No** | **Keanggotaan IMT** | **Rentang Nilai** |
| --- | --- | --- |
| 1 | Sangat Kurus | 0.0 - 19.0 |
| 2 | Kurus | 15.0 - 20.0 |
| 3 | Normal | 17.0 - 27.0 |
| 4 | Gemuk | 23.0 - 29.0 |
| 5 | Obesitas | 25.0 - 50.0 |
| Sumber: Diadaptasi dari Anggariawan (2014) | | |

Cara menyitasi untuk gambar/diagram:

Gambar 2.3 Pengaruh nilai K terhadap akurasi

Sumber: Anggariawan (2014)

Jika tabel atau gambar adalah hasil perujukan sekunder, maka penulisan tanda sitasi mengikuti aturan perujukan sekunder. Contohnya:

Sumber: Angriawan (2014) disitasi dalam Alfian (2015, p.45)

Penulisan istilah “Sumber” hanya digunakan jika tabel atau gambar berasal dari sumber lainnya sehingga perlu dilakukan sitasi. Jika tabel atau gambar adalah hasil karya penulis sendiri, tentu tidak diperlukan penulisan sumber dan kode sitasi.

### Daftar Pernyataan

Berikut ini adalah contoh penggunaan daftar beberapa pernyataan yang tersusun bernomor dan yang berindeks alfabetik:

1. Aspek satu berkaitan dengan:
2. Aspek satu a
3. Aspek satu b
4. Aspek dua berkaitan dengan:
5. Aspek dua a
6. Aspek dua b
7. Aspek dua c

Aspek-aspek tersebut bisa dijelaskan lebih lanjut sesuai tujuan dan kebutuhan. Penulisan di atas adalah sebuah contoh.

### Kode Sumber

Kode sumber (*source code*) dapat dituliskan dalam bagian utama atau lampiran skripsi hanya jika benar-benar dibutuhkan untuk memperjelas solusi yang diusulkan. Penulisannya dibatasi hanya pada bagian-bagian yang terpenting, misalkan metode atau algoritme utama yang digunakan. Akan tetapi lebih disarankan untuk menggantinya dengan *pseudocode* atau notasi lainnya. Hal ini karena penulisan kode sumber yang berlebihan hanya mempertebal skripsi tanpa memberikan nilai tambah. Selain itu, kode sumber tersebut sebenarnya termasuk properti intelektual penulis yang seharusnya dilindungi.

Jika terpaksa harus dituliskan, kode sumber menggunakan tipe huruf Courier New berukuran 9 dan berspasi *single*. Kemudian, kode sumber dimasukkan ke dalam kolom ke-2 sebuah tabel yang dilengkapi dengan nomor baris di kolom ke-1. Contoh penulisan kode sumber adalah sebagai berikut:

|  |  |
| --- | --- |
| Algoritme 1: Fungsi Iteratif | |
| 1  2  3 | tipedatakembalian namaFungsi(tipeparameter parameter){  *// kode*  } |

# METODOLOGI

Makna dari metodologi penelitian dapat dilihat dari dua sudut pandang. Pertama, dari pandangan umum ia bisa berarti sebuah cara sistematik untuk menyelesaikan masalah penelitian. Dalam hal ini ia juga dapat merupakan kumpulan cara (metode) yang lebih spesifik dalam penyelesaian masalah. Kedua, metodologi penelitian dapat dipahami sebagai sebuah ilmu untuk mempelajari bagaimana sebuah penelitian dilakukan secara sistematik. Dalam ilmu ini kita mempelajari berbagai langkah yang umumnya digunakan oleh peneliti ketika mempelajari masalah penelitian beserta alasan-alasan logis di belakangnya. Oleh karena itu di dalam pembahasan metodologi penelitian, yang dibicarakan tidak hanya metode, teknik, atau langkah-langkah yang digunakan dalam sebuah penelitian tetapi juga logika di balik metode, teknik, atau langkah-langkah tersebut sesuai dengan konteks penelitiannya masing-masing. Dalam hal ini perlu dijelaskan mengapa sebuah metode atau teknik dipilih.

## Isi Metodologi

Dari penjelasan di atas dapat dikatakan bahwa metodologi penelitian memiliki cakupan lebih luas daripada metode. Metode sendiri dapat diartikan sebagai cara, prosedur, atau teknik untuk menjalankan sebuah proses secara logis, terurut, dan sistematik. Metode/teknik dapat berupa metode/teknik untuk pengumpulan data, untuk analisis data, atau algoritme untuk pemecahan masalah penelitian. Terkadang metode dibedakan dari teknik dengan pemahaman bahwa teknik itu lebih khusus dan operasional daripada metode. Dalam panduan penulisan ini pemilihan istilah tersebut diserahkan kepada penulis dan pembimbingnya. Yang terpenting, apapun metode/teknik yang dipilih harus sesuai dengan sifat penelitian, masalah yang hendak diselesaikan, dan pertanyaan yang hendak dijawab.

### Komponen-komponen Metodologi

Hal-hal yang perlu dijelaskan dalam metodologi penelitian adalah:

1. Tipe penelitian. Misalkan, nonimplementatif (deskriptif atau analitik) atau implementatif (pengembangan, perancangan, atau lainnya)
2. Strategi dan rancangan penelitian

* Strategi/metode secara umum. Misalnya, pembuatan artefak TI, studi kasus, survey, eksperimen, dan sebagainya.
* Subjek atau partisipan penelitian. Siapa saja yang terlibat secara langsung dalam penelitian sebagai pelaku atau orang yang diambil datanya, serta bagaimana karakteristiknya yang dibutuhkan.
* Lokasi penelitian. Misalkan, di laboratorium atau studi lapangan di mana.
* Metode/teknik pengumpulan data. Misalnya, wawancara, observasi, kuisioner, studi dokumen.
* Metode/teknik analisis data dan pembahasan hasilnya. Misalnya, analisis kuantitatif secara statistik menggunakan uji t, analisis kualitatif terhadap teori A, B, dan sebagainya.
* Peralatan pendukung yang digunakan. Misalnya, spesifikasi piranti keras dan piranti lunak untuk menyusun kode sumber atau menguji sistem yang dibangun.
* Metode/teknik lainnya. Misalkan, jika strategi yang dipilih adalah pembangunan perangkat lunak, umumnya perlu dijelaskan model proses perangkat lunak yang digunakan. Sebagai catatan, Bab Metodologi Penelitian terfokus pada menjelaskan cara meneliti, sementara hasilnya dituliskan dalam bab-bab berikutnya. Oleh karena itu, dalam menjelaskan aktivitas dalam proses perangkat lunak, perlu dihindari dalam bab ini penjelasan daftar persyaratan/kebutuhan yang telah diidentifikasi, hasil perancangan, dan sebagainya. Contoh lainnya, untuk implementasi algoritma, perlu disebutkan dan dapat dideksripsikan secara singkat fungsi algoritme tersebut. Penjelasan yang lebih detil tentang algoritme tersebut dapat dimasukkan dalam bab lainnya, misalkan Bab Perancangan.

Dalam mendeskripsikan hal-hal di atas, penulis dapat menyusun subbab-subbab beserta alur logikanya dengan pertimbangan sendiri di bawah supervisi pembimbing, berdasarkan relevansi dengan sifat penelitian dan aspek keterbacaan.

### Penomoran Subbab

Penomoran subbab disarankan tidak lebih dari 4 level (maksimal subbab X.X.X.X), tetapi sebaiknya hanya sampai 3 level. Kepala bab dan subbab tidak boleh mengandung *widow* atau *orphan* sehingga nampak menggantung atau terputus di bagian awal atau akhir sebuah halaman. *Widow* adalah sebuah paragraf dengan hanya satu baris pertama pada akhir halaman sedangkan sisanya berada pada halaman berikutnya. Sedangkan *orphan* adalah baris terakhir dari satu paragraf yang tertulis pada awal suatu halaman sedangkan baris lainnya dari paragraf tersebut berada pada halaman sebelumnya.

## Lain-lain

Deskripsi dari subbab Lain-lain, dan seterusnya.

DAFTAR REFERENSI

Adobe Systems Incorporated, 2013. Adobe Air (3.5 beta). [program komputer] Adobe Labs. Tersedia di: <http://labs.adobe.com/technologies/  
flashruntimes/air/> [Diakses 1 Mei 2013]

Alif, A., 2013. *Komputasi cerdas untuk pemula*. Malang: ABC Press.

Angriawan, B., 2014. *Sistem pakar untuk penentuan kondisi tubuh ideal atlet sepakbola usia remaja*. S1. Universitas Malang Raya.

Berndtsson, M., Hansson, J., Olsson, B. & Lundell, B., 2008. *Thesis projects: a guide for students in Computer Science and Information Systems*. 2nd ed. London: Springer-Verlag London Limited.

Boots Group Plc., 2003. *Corporate social responsibility*. [online] Boots Group Plc. Tersedia di: <http://www.boots-plc.com/information/info.asp?id1=1a> [Diakses 1 April 2004]

Brata, K.C., 2012. *Rancang bangun aplikasi jejaring sosial kampus berbasis GPS pada ponsel cerdas Android*. S1. Universitas Brawijaya. Tersedia di <http://ptiik.ub.ac.id/skripsi> [Diakses 1 Agustus 2014]

British Standards Institution, 2011*. BS EN 594:2011 Timber structures. Test methods. Racking strength and stiffness of timbre frame wall panels*. British Standards Online [online] Tersedia melalui: Anglia Ruskin University Library <http://libweb.anglia.ac.uk> [Diakses 31 Augustus 2011]

Brodjonegoro, A., 2009a. *Dunia teknologi informasi bagi komunitas* *open source.* Bandung: Bandung Indah Press.

Brodjonegoro, A., 2009b. *Peran media sosial dalam pemasaran produk perangkat lunak.* Bandung: Bandung Indah Press.

Broughton, J.M., 2002a. The Brettow Woods proposal: a brief look. *Political Science Quarterly*, 42(6), p.564.

Broughton, J.M., 2002b. The Brettow Woods proposal: a brief look. *Political Science Quarterly*, [e-journal] 42(6). Tersedia melalui: Perpustakaan Universitas BX <http://perpustakaan.ubx.ac.id> [Diakses 1 Juli 2013]

Brown, J. 2005. Evaluating surveys of transparent governance. In: UNDESA (United Nations Department of Economic and Social Affairs), 2005. *6th Global forum for reinventing government: towards participatory dan transparent governance*. Seoul, Republic of Korea, 24-27 May 2005. New York: United Nations.

Cakraningrat, R., 2011. *Sistem pendukung keputusan untuk UMKM*. [e-book]. UBX Press. Tersedia melalui: Perpustakaan Universitas BX <http://perpustakaan.ubx.ac.id> [Diakses 1 Juli 2013]

Cookson, J. dan Church, S. eds., 2007. *Leisure and the tourist*. [e-book] Wallingford: ABS Publishers. Tersedia di: Google Books <http://booksgoogle.com> [Diakses 1 Juli 2009]

Cox, C., Brown, J.T. dan Tumpington, W.T., 2002. What health care assistants know about clean hands. *Nursing Today*, Spring Issue, pp.64-68.

Diponegoro, A., 2008. *The beauty of Indonesian oceans*. [electronic print] Tersedia di: <http://adiponegoro.com/store/product\_info.php?cPath=3&  
productss\_id=99> [Diakses 1 Januari 2011]

Esemka, 2012. *Esemka bisa*. [image online] Tersedia di: <http://www.esemka.co.id/esemkabisa.aspx> [Diakses 31 Januari 2011]

Goalie, D. 2008. Remote sensing technology for modern soccer. *Popular science and Technology*, [online] Tersedia di: <http://www.popsci.com/b012378/  
soccer.html> [Diakses 1 Juli 2009]

Haryanto, A. 2002. *Dua dunia*. [foto] (Koleksi pribadi Alan Haryanto)

Higher Education Act 2004. (c.8). London: HMSO

International Standards Office, 1998. *ISO 690 – 2 Information and documentation: Bibliographical references: Electronic documents*. Geneva: ISO.

Kartolo, R., 2010. *Wawancara pada Kabar Pagi*. Diwawancara oleh Sam Basman [televisi] TVRI Saluran 1, 17 Agustus 2010, 08:30.

Keene, E., ed., 1988. *Natural language*. Cambridge: University of Cambridge Press.

Kementerian Komunikasi dan Informatika, 2013. *Laporan Tahunan Layanan Informasi Publik Tahun 2012*. [pdf] Kementerian Komunikasi dan Informatika. Tersedia di: <http://publikasi.kominfo.go.id/bitstream/handle/  
54323613/976/laporan-dan-evaluasi-ppid-tahun-2012-ditambahkan-cover-untuk-online-ppid.pdf> [Diakses 1 Agustus 2014]

NHS Evidence, 2003. *National Library of Guidelines*. [online] Tersedia di: <http://www.library.nhs.uk/guidelinesfinder> [Diakses 1 Juli 2007]

Rahardjo, S. 2001. *Presiden Habibie*. [foto] (Jakarta, Koleksi Museum Presiden)

Richmod, J., 2005. *Customer expectations in the world of elctronic banking: a case study of the Bank of Britain*. PhD. Anglia Ruskin University.

Rumbaugh, J., Jacobson, I. & Booch, G., 2005. *The Unified Modeling Language reference manual*. 2nd ed. Boston: Addison-Wesley.

Samson, C., 1970. Problems of information studies in history. Dalam: S. Stone, ed. 1980. *Humanities information research*. Sheffield: CRUS. pp. 44-68.

Scottish Intercollegiate Guidelines, 2001. *Hypertension in the elderly*. (SIGN publication 20) [online] Edinburgh: SIGN (Diterbitkan 2001) Tersedia di:<http://www.sign.ac.uk/sign49.pdf> [Diakses 22 November 2004]

Silverman, D.F. dan Propp, K.K. eds., 1990. *The active interview*. BeverlyHills, CA: Sage.

Smith, J., 1975. A source of information. Dalam: W. Jones, ed. 2000. *One hundred and one ways to find information about health*. Oxford: Oxford University Press. Ch.2.

Sommerville, I., 2011. *Software engineering*. 9th ed. London: Addison-Wesley.

Sudirman, Z., 2011. *Pembahasan tentang sitasi dan perujukan*. [surat] (Komunikasi personal, 11 Juni 2011).

Tanenbaum, A.S., 1998. *Organisasi komputer terstruktur, jilid 1*. Diterjemahkan dari Bahasa Inggris oleh T.A.H Al-Hamdany. 2001. Jakarta: Salemba Teknika.

Thompson, A. dan Thomson, B., (in press) Innocent or guilty: a studi to ascertain the status of convicts in highly uncertain situations. *Journal of Crime Scene Investigation*. (Diterima untuk publikasi Januari 2002).

Undang-undang Republik Indonesia nomor 12 tahun 2012 tentang Pendidikan Tinggi. Jakarta: Kementerian Sekretariat Negara Republik Indonesia.

UNDESA (United Nations Department of Economic and Social Affairs), 2005. *6th Global forum for reinventing government: towards participatory dan transparent governance*. Seoul, Republic of Korea, 24-27 May 2005. New York: United Nations.

1. PERSYARATAN FISIK DAN TATA LETAK
   1. Kertas

Kertas yang digunakan adalah HVS 70 mg berukuran A4. Apabila terdapat gambar-gambar yang menggunakan kertas berukuran lebih besar dari A4, hendaknya dilipat sesuai dengan aturan yang berlaku. Pengetikan hanya dilakukan pada satu muka kertas, tidak bolak balik.

* 1. Margin

Batas pengetikan naskah adalah sebagai berikut :

* Margin kiri: 4 cm
* Margin atas: 3 cm
* Margin kanan: 3 cm
* Margin bawah: 3 cm
  1. Jenis dan Ukuran Huruf

Jenis huruf yang dipakai dalam skripsi adalah Calibri dengan ketentuan sebagai berikut:

* Judul bab pada level 1 berukuran 16 pt
* Judul subbab pada level 2 berukuran 14 pt
* Judul subbab pada level 3 berukuran 14 pt
* Judul subbab pada level 4 berukuran 12 pt
* Badan teks berukuran 12 pt

Penggunaan jenis dan ukuran ini harus konsisten. Untuk memudahkan memelihara konsistensi sekaligus penyusunan struktur skripsi, fasilitas seperti *styles* dan *multilevel list* dalam program pengolah kata dapat digunakan. Sebuah *template* untuk skripsi ini telah disediakan untuk membantu mahasiswa. *Styles* dan *multilevel list* dalam template tersebut sudah dirancang untuk jenis dan ukuran huruf yang disyaratkan.

* 1. Spasi

Jarak standar antar baris dalam badan teks adalah satu spasi. Jarak antar paragraf, antara judul bab dan judul subbab, antara judul subbab dan badan teks, dan seterusnya, dapat dilihat pada masing-masing *style* yang digunakan dan tersedia dalam *template* untuk skripsi ini.

* 1. Kepala Bab dan Subbab

Kepala bab terdiri dari kata “BAB” yang diikuti dengan nomor bab dan judul dari bab tersebut, misalnya “BAB 1 PENDAHULUAN” . Kepala subbab diawali dengan nomor sesuai tingkat hirarkinya dan diikuti dengan judul subbab, misalnya “1.2 Rumusan masalah”. Penomoran subbab disarankan tidak lebih dari 4 level (maksimal subbab X.X.X.X). Kepala bab dan subbab tidak boleh mengandung *widow* atau *orphan* sehingga nampak menggantung atau terputus di bagian awal atau akhir sebuah halaman. *Widow* adalah sebuah paragraf dengan hanya satu baris pertama pada akhir halaman sedangkan sisanya berada pada halaman berikutnya. *Orphan* adalah baris terakhir dari satu paragraf yang tertulis pada awal suatu halaman sedangkan baris lainnya dari paragraf tersebut berada pada halaman sebelumnya.

* 1. Nomor Halaman

Bagian awal skripsi menggunakan nomor halaman berupa angka Romawi kecil (i, ii, iii, iv, dan seterusnya) yang dimulai dari sampul dalam. Sedangkan bagian utama dan bagian akhir skripsi menggunakan nomor halaman berupa angka Arab (1, 2, 3, dan seterusnya) yang dimulai dari bab 1. Semua nomor halaman diletakkan di tengah bawah.

1. PENGGUNAAN BAHASA

Bahasa yang dipakai dalam skripsi adalah bahasa Bahasa Indonesia yang baku. Setiap kalimat harus memiliki subjek dan predikat, dan umumnya dilengkapi juga dengan objek, pelengkap, atau keterangan. Setiap paragraf biasanya terdiri dari beberapa kalimat. Penuturan isi dalam kalimat, paragraf, maupun antar paragraf harus menggunakan bahasa yang tepat dan menggambarkan alur logika yang runtut.

Penulisan bahasa asing yang sudah diserap dalam Bahasa Indonesia disesuaikan dengan kaidah Bahasa Indonesia. Sedapat mungkin dihindari penggunaan bahasa asing jika istilah dalam bahasa Indonesia sudah ada. Jika terpaksa menggunakan istilah dalam bahasa asing, maka penulisannya harus sesuai ejaan aslinya dan dicetak miring (*italic*), kecuali jika istilah tersebut adalah nama.

Sebagai referensi untuk penulisan Bahasa Indonesia yang baku, dokumen berikut dapat digunakan:

* Kamus Bahasa Indonesia, Tim Penyusun, Pusat Bahasa Departemen Pendidikan Nasional, Jakarta 2008
* Peraturan Menteri Pendidikan Nasional Republik Indonesia nomor 46 tahun 2009 tentang Pedoman Umum Ejaan Bahasa Indonesia yang Disempurnakan
* Kamus Besar Bahasa Indonesia dalam jaringan (KBBI daring): http://bahasa.kemdiknas.go.id/kbbi/index.php