BAB III

METODOLOGI PENELITIAN

3.1 Pendahuluan

Pada bab ini akan membahas mengenai prosedur yang dilakukan dalam melaksanakan penelitian tahap demi tahap. Secara umum, rangka kerja yang terdapat dalam penelitian ini terbagi menjadi tiga fase yaitu fase identifikasi masalah dari metode kriptografi simetrik yang digunakan saat ini dan memformulasikan solusi yang mungkin sebagai penyelesaian, fase penerapan metode yang telah ditentukan yaitu jaringan saraf *backpropagation* pada kriptografi simetrik, serta yang terakhir adalah fase evaluasi dari hasil yang didapat dengan menggunakan objektif yang telah ditentukan pada tahapan awal penelitian. Setiap fase yang ada berisi aktivitas yang berbeda serta hasil akhir yang diharapkan pun berbeda. Terakhir, bab ini menjelaskan mengenai pengukuran performa dari metode yang dipilih termasuk dengan perngkat keras (*hardware*) dan perangkat lunak (*software*) yang digunakan dalam melakukan penelitian.

3.2 Metode Pengumpulan Data

Pada bagian ini akan membahas mengenai secara rinci mengenai penggunaan data yang dipakai sebagai objek dalam penelitian. Pembahasan secara detail tersebut antara lain:

3.2.1 Jenis dan Sumber Data

Data yang dipergunakan dalam penelitian ini sebagai objek pembahasan adalah jenis data sekunder yang berupa file *.txt yang diambil dan tersedian pada situs http://www.textfiles.com/directory.html. Data yang diperoleh dari situs tersebut harus melalui proses validasi data secara manual untuk memastikan bahwa tidak ada karakter yang tidak termasuk dalam ASCII pada file teks yang digunakan.

3.2.2 Metode Pengumpulan Data

Metode pengumpulan data dilakukan secara manual dengan cara melakukan proses pengunduhan pada situs http://www.textfiles.com/directory.html. Data yang digunakan adalah kata-kata pendek atau frasa yang terdapat pada halaman *textfile.com.* Pada tahapan pengumpulan data, data akan disaring terlebih dahulu agar sesuai dengan masukan yang dapat diterima jaringan misalnya menghapus tanda baca.

3.2.3 Masukan yang Digunakan

Waktu pemrosesan jaringan yang dibentuk didasarkan oleh jumlah data yang diproses. Pada penelitian ini masukan yang digunakan memiliki panjang dengan ukuran maksimal 448-*bit.* Masukan yang digunakan dalam format ASCII yang memiliki ukuran 8-*bit* untuk setiap panjang karakter. Tabel III-1 menunjukkan data uji yang digunakan akan disimpan pada file dengan format .txt. Setiap satu kali proses pelatihan dan pengujian hanya dapat menggunakan satu file dengan ukuran maksimum tidak lebih dari 5 MB.

Tabel III-1. Daftar Data Uji

No	Nama File	Plain Text
1	Aboutems.txt	microprocessor
2	Aids.txt	detective Barry Donovan
3	Amscsi.txt	circuit description
4	Anetwork.txt	loading and setup
5	Apple.txt	text of apple microsoft agreement
6	Bitsbaud.txt	Modem transmission
7	Buildit.txt	hardware manufacturing business
8	Cascade.txt	cascade electronics
9	Cheats.txt	Statistics screen
10	Config.txt	Compatible computer

3.2.4 Penggunaan kunci

Jumlah bobot yang terdapat pada masing-masing lapisan masukan menuju lapisan tersembunyi dan lapisan tersembunyi menuju lapisan keluaran berjumlah sebanyak 25 buah sehingga jumlah bobot yang ada yaitu 50 buah. Kunci yang akan dikonversi menjadi bobot merupakan karakter dengan ukuran 8-bit pada setiap karakter sehingga ukuran maksimum kunci yaitu 400-bit. Tabel-III-2 menunjukkan contoh kunci yang digunakan pada proses pelatihan dan pengujian data.

Tabel III-2. Contoh Ukuran Kunci

No	Panjang Kunci	Kunci
1	128 *bit*	enkripsidekripsi

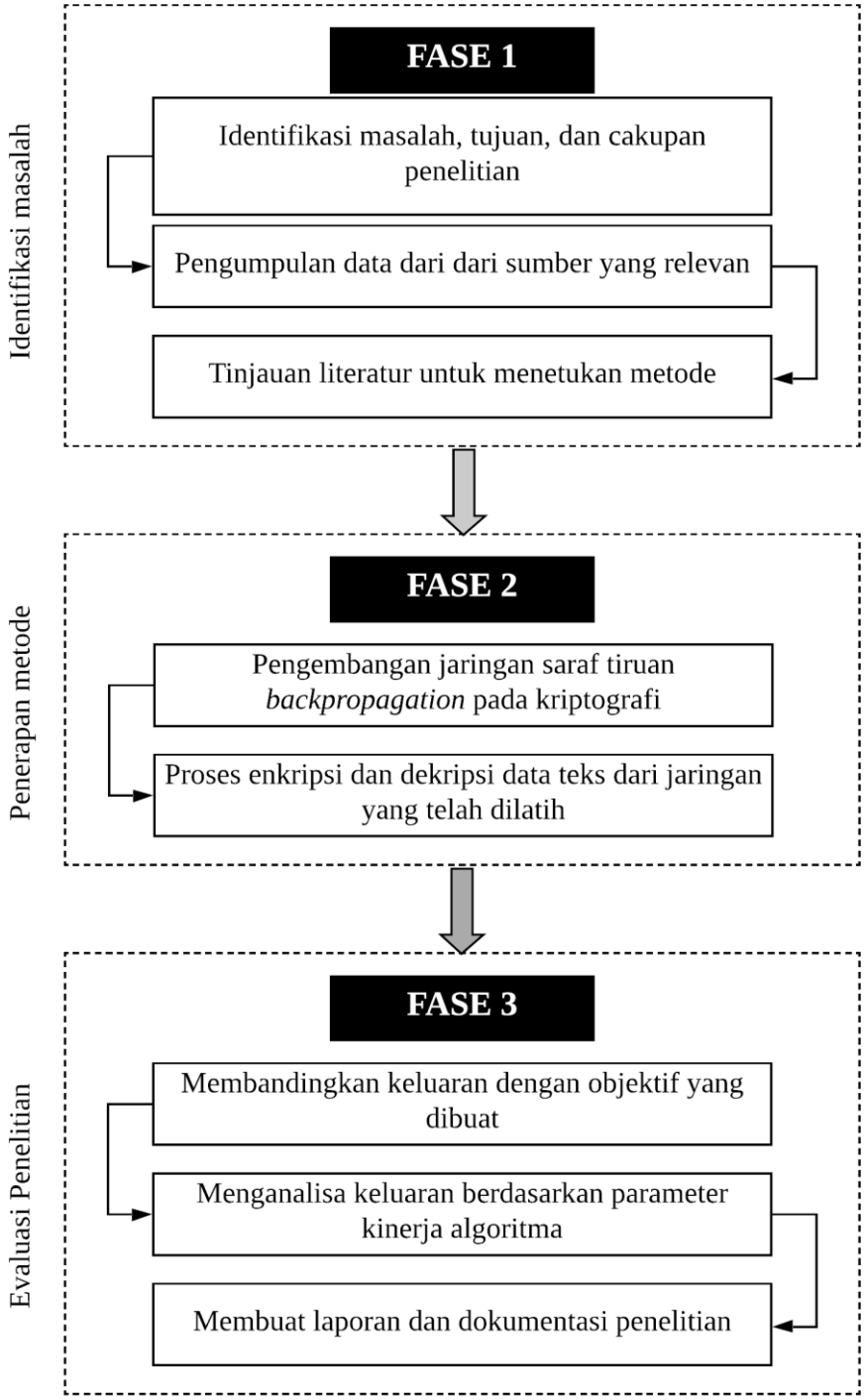
2	192 *bit*	enkripsidekripsijaringan
3	256 *bit*	enkripsidekripsijaringan
4	320 *bit*	enkripsidekripsijaringankeamanan
5	384 *bit*	enkripsidekripsijaringankeamanankomputer

3.3 Metode Penelitian / Kerangka kerja

Kerangka kerja penelitian terdiri dari beberapa fase yang akan dilakukan selama melaksanakan penelitian yang akan dibagi menjadi tiga bagian pada pembahasan ini antara lain:

1. Fase dimulai dengan melakukan identifikasi beberapa macam metode yang digunakan pada kriptografi dalam mengamankan data kemudian menganalisa masalah yang ada serta mengusulkan gagasan ide untuk menyelesaikan masalah tersebut.
2. Fase yang kedua adalah penerapan jaringan saraf *backpropagation* pada kriptografi simetris berdasarkan literatur yang telah dipelajari.
3. Fase yang terakhir adalah fase evaluasi terhadap keluaran yang dihasilkan oleh metode yang diusulkan berdasarkan objektif yang telah ditentukan.

Pada setiap fase terdapat tugas-tugas yang spesifik dengan tujuan untuk memastikan bahwa setiap fase sesuai dengan objektif yang telah dibuat. Gambar III-1 menunjukkan keseluruhan proses selama melaksanakan penelitian.



Gambar III-1. Kerangka kerja penelitian

3.3.1 Fase 1 : Identifikasi Masalah

Pada proses identifikasi masalah, fase awal yaitu untuk memastikan objektif dari penelitian telah terdefinisikan berdasarkan masalah yang telah diidentifikasikan. Selain itu, pada tahap ini data yang telah dikumpulkan akan digunakan sebagai substansi atau referensi pada penerapan metode yang dipilih untuk memecahkan masalah yang telah diidentifikasi. Sumber dari koleksi data bervariasi dan diambil dari berbagai macam situs-situs literatur seperti *Research gate, Science direct, Library genesis, IEEE,* dan lain-lain.

Setelah itu, pembelajaran terkait dengan elemen penelitian seperti algoritma-algoritma, metode-metode, atau teknik-teknik yang digunakan akan dibandingkan dengan identifikasi permasalahan. Penelitian terkait yang pernah dilakukan sebelumnya telah dilakukan yang meliputi topik : (1) simetrik kriptografi, (2) jaringan saraf *backpropagation*, (3) data teks.

3.3.2 Fase 2 : Penerapan Metode

Algoritma yang akan digunakan dalam penelitian ini adalah jaringan saraf *backpropagation* dan menerapkannya pada kriptografi kunci simetris. Oleh karena itu, integrasi antara jaringan saraf dan kriptografi akan tercakupi pada pembahasan ini dan diimplementasikan dengan menggunakan bahasa pemrograman Java.

3.3.3 Fase 3 : Evaluasi Penelitian

Tahapan terakhir dari penelitian ini adalah evaluasi keluaran yang dihasilkan oleh metode yang digunakan berdasarkan objektif dan parameter yang

telah didefinisikan pada awal penelitian atau fase pertama. Pada akhir fase 3 terdapat laporan dan juga dokumentasi yang dibuat untuk menyampaikan analisa penelitian serta kesimpulan yang didapat dari metode yang ditawarkan.

3.3.3.1 Menentukan Format Pengujian Data

Hasil penelitian atau keluaran yang didapat akan digambarkan serta dideskripsikan melalui table III-2 sebagai berikut:

Tabel III-3. Rancangan Tabel Hasil Percobaan Enkripsi dan Dekripsi

Percobaan	Akurasi Enkripsi	Akurasi Dekripsi	Ukuran (*bit*)	Waktu (ms)
ER-01				
ER-02				
ER-03				
ER-04				
ER-05				
Rata-rata				

Metode kriptografi yang dipilih terutama tahapan enkripsi dapat dihitung berdasarkan kesesuaian dan kompatibilitas data dalam hal ukuran sebagai masukan dalam jaringan yang dibentuk (Ismail et. at, 2012). Menurut Al-nima et. al (2009) tingkat akurasi metode yang digunakan dapat dihitung dengan cara menghitung nilai mutlak selisih antara data sebelum enkripsi dan data setelah enkripsi dengan perhitungan sebagai berikut:

$$e = \sum_{i=0}^{n} |(x_i - y_i)| \quad \text{(III-1)}$$

Dimana

e adalah minimum nilai *error*.

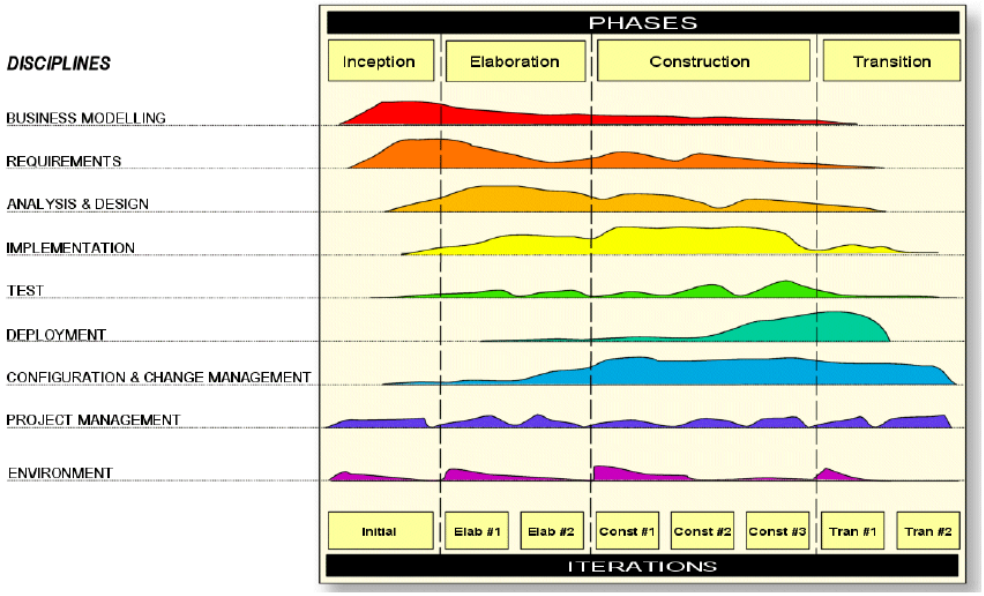
x_i adalah data masukan (*input*) pada urutan ke-i sebelum proses enkripsi.

y_i adalah data masukan (*input*) pada urutan ke-i setelah proses enkripsi.

n adalah ukuran data yang dienkripsi.

3.4 Metode Pengembangan Perangkat Lunak

Metode pengembangan perangkat lunak yang digunakan dalam penelitian ini yaitu *Rational Unified Process* (RUP). RUP merupakan proses rekayasa perangkat lunak yang bertujuan untuk memastikan perangkat lunak yang dihasilkan memenuhi kebutuhan pengguna (*user*) dengan menyediakan pendekatan untuk mendefinisikan tugas dalam sistem pengembangan yang terorganisir (Eduardo & Hirata, 2007). Pada metode ini terdapat empat fase antara lain fase insepsi, fase elaborasi, fase konstruksi, dan fase transisi seperti yang terlihat pada gambar III-2. Setiap fase memiliki peranan dan tahapan pengembangan yang berbeda-beda.



Gambar III-2. Arsitektur RUP (Anwar, 2014)

3.4.1 Fase Insepsi

Pada fase insepsi, pengembangan sistem perangkat lunak akan lebih berfokus kepada tahapan *business modeling* dan *requirements* yaitu memetakan atau melakukan pemodelan terhadap kebutuhan pengguna yang mencakup kebutuhan yang diperlukan dalam membangun sistem seperti mendefinisikan kebutuhan fungsional dan nonfungsional. Tahapan ini sangat krusial karena menurut (Kruchten, 2000) bahwa pada tahapan insepsi hingga elaborasi, jumlah kesalahan (*flaws*) lebih banyak muncul dan terdeteksi. Pada tahapan ini juga, analisa serta desain awal terhadap sistem mulai ditentukan pada bagian *analysis and design* yang pada penelitian ini meliputin rancangan *use-case diagram* sistem yang dibangun.

3.4.2 Fase Elaborasi

Pada tahapan ini, selain menambahkan *requirements* serta *design* pada perangkat lunak seperti *mock-up user interface* dan *sequence diagram*, penerapan metode yang digunakan atau pembangunan awal perangkat lunak mulai dilakukan dengan menggunakan bahasa pemrograman serta *software* bantuan yang telah ditetapkan pada tahapan sebelumnya. Eduardo dan Hirata (2007) menyatakan bahwa pada fase elaborasi, *use case* yang sudah dipilih telah sepenuhnya dianalisa dan didesain pada *workflow analysis and design.*

3.4.3 Fase Konstruksi

Fase konstruksi berfokus pada pengembangan komponen dan fitur serta pembuatan sistem operasional dengan menggunakan arsitektur yang dapat dieksekusi yang telah ditetapkan pada fase sebelumnya (Anwar, 2014). Pada tahap *business modeling* meliputi pembangunan basis data sedangkan tahapan *requirements* meliputi pembangunan kelas-kelas yang akan digunakan dalam pembanguna perangkat lunak. Pada fase kontruksi, hampir keseluruhan program telah selesai dibangun karena pada *workflow implementation* kelas-kelas yang telah ditentukan digabungkan dengan bahasa pemrograman yang telah ditentukan.

3.4.4 Fase Transisi

Fase transisi merupakan langkah terakhir atau disebut sebagai kegiatan pelepasan produk dan berfokus pada transisi sistem dari tahap pengembangan menuju tahapan produksi perangkat lunak yang telah dibentuk (Anwar, 2004).

Tahapan transisi banyak melakukan pengujian terhadap sistem yang telah dibangun untuk mengurangi kemungkinan timbulnya cacat (*defect*) pada sistem.

3.5 Kesimpulan

Pada pembahasan ini menjelaskan tentang metode yang akan diterapkan pada proses pengembangan perangkat lunak serta rancangan yang akan digunakan dalam mengukur hasil dari pengimplementasian algoritma yang dilakukan pada pembahasan pada bab berikutnya. Aktivitas yang dilakukan dalam melaksanakan penelitian berdasarkan rangka kerja yang dibangun. Proses pengukuran terhadap performa algoritma diperlukan untuk menganalisa hasil yang didapatkan dengan keluaran yang diharapkan dan membandingkan keluaran tersebut dengan penelitian yang berkaitan. Pada bab ini juga membahas mengenai perangkat lunak (*software*) dan perangkat keras (*hardware*) yang digunakan untuk menunjang proses penelitian.