BAB 1
PENDAHULUAN

1.1 Latar Belakang Masalah

Dalam empat tahun terakhir, berbagai jenis piranti tanpa awak telah digunakan oleh kalangan sipil dan ilmiah. Piranti tersebut dilengkapi dengan berbagai macam peralatan untuk memberikan data dalam berbagai aplikasi[1]. Pesawat tanpa awak atau *Unmanned Aerial Vehicle* (UAV) yang berkembang pesat untuk aplikasi penginderaan penglihatan jarak jauh, UAV merupakan sistem tanpa awak (*Unmanned System*), yaitu sistem berbasis elektro-mekanik yang dapat melakukan misi-misi terprogram[2]. Pada dasarnya meskipun mempunyai kemampuan *autonomous*, UAV tetap membutuhkan *Ground Control System* (GCS). Dalam operasional UAV tugas GCS adalah sebagai stasiun monitoring dan komando dimana operator di darat dapat mengirimkan perintah misi dan mengawasi jalannya misi tersebut dan kondisi UAV selama di udara [3].

UAV dengan GCS dapat berkomunikasi 2 arah dan saling mengirimkan data melalui telemetri. Berdasarkan hasil dari penelitian memebuktikan bahwa UAV profesional sekalipun masih bisa dilakukan serangan berupa *Man-in-the-Middle* (MitM), penulis memberikan dua solusi dapat digunakan: (1) enkripsi *on-board* XBee 868LP, adalah satu-satunya solusi yang juga mengurangi risiko *Remote AT Commands*, dan (2) enkripsi lapisan aplikasi. Sehingga diperlukan enkripsi pada data yang dikrimkan dan diterima oleh GCS[4].

Sulitnya mendapatkan *hardware* yang menanamkan enkripsi yang dijual bebas dipasaran dan dengan berbagai pertimbangan maka enkripsi ditingkat lapisan aplikasi dipilih. Enkripsi lapisan aplikasi lebih mudah digunakan dan lebih hemat biaya daripada enkripsi perangkat keras dalam berbagai kasus. Secara khusus, ketika layanan enkripsi baru diperlukan untuk lingkungan komputasi yang sudah digunakan, enkripsi lapisan aplikasi lebih cocok daripada perangkat keras[5].

Penelitian sebelumnya terkait keamanan UAV dan GCS adalah pengamanan data antara UAV dan GCS pernah dilakukan dengan berbasis *One Time Pad*[6].

Otentikasi komunikasi UAV menggunakan *Caesar Cipher Cryptography* telah dirancang dan disimulasikan. Sistem telah menjalani tes awal, simulasi dan hasilnya memuaskan[7]. Kombinasi keamanan UAV dilakukan dengan pembangkit kunci ChaCha sebagai *stream chipper* dan menggunakan otentikasi algoritma Poly1305[8]. Pengamanan antara *Micro Air Vehicle* (MAV) dan GCS menerapkan skema *Advanced Encryption Standard* (AES) pada mode CTR untuk enkripsi, SHA-256 untuk *hashing* kunci dan *Diffie Hellman* untuk pertukaran kunci pengiriman data dengan menggunakan *MAVLink protocol*[9]. Dalam penelitian yang dilakukan penulis tentang penerapan kriptografi AES pada UAV dan GCS berkontribusi untuk membuat algoritma kunci yang hanya diketahui oleh pihak terkait dengan pengiriman data menggunakan radio frekuensi.

Enkripsi merupakan proses mengamankan suatu informasi dengan membuat informasi tersebut tidak dapat dibaca tanpa bantuan pengetahuan khusus. Saat ini, AES merupakan algoritma kriptografi yang cukup aman untuk melindungi data atau informasi yang bersifat rahasia. Pada tahun 2001, AES digunakan sebagai standar algoritma kriptografi terbaru yang dipublikasikan oleh *National Institute of Standard and Technology* (NIST). Algoritma AES adalah algoritma kriptografi yang dapat mengenkripsi dan mendekripsi data dengan panjang kunci yang bervariasi, yaitu 128 bit, 192 bit, dan 256 bit, mengetahui bahwa mode CBC jauh lebih baik dari mode ECB dalam hal perlindungan[10]. Hasil penelitian untuk mengenkripsi dan dekripsi semua jenis file dengan algoritma AES-256, hasil dari penelitian menunjukkan bahwa algoritma AES dengan panjang kunci 256 bit dapat menyandikan isi suatu file sehingga dapat mengamankan file tersebut[11], enkripsi AES dapat mengamankan file multimedia, gambar bitmap, maupun file lainya[12][13][14]. Penelitian selanjutnya dijelaskan bahwa penggunaan MD5 pada enkripsi SSO masih bisa dapat diretas, sedangkan jika diterapkan menggunakan AES dengan kata kunci dinamis, maka SSO tidak dapat diretas[15], penelitian berikutnya dapat mengamankan E-diploma dengan menggunakan *digital signature autentication*[16]. Dengan demikian dapat disimpulkan bawah algoritma AES dapat mengamankan semua jenis file.

AES dengan panjang kunci 128 bit (AES-128) memiliki beberapa kelebihan dibandingkan dengan variasi kunci 192 bit dan 256 bit. Salah satunya adalah memiliki waktu proses yang paling cepat yaitu 110.78 ns[17]. Untuk melakukan *cracking* dengan menggunakan *brute force attack* pada AES-128 dibutuhkan waktu $1{,}02\ x\ 10^{18}$ Tahun[18]. Enkripsi AES dengan panjang kunci 128 bit cukup baik untuk dilakukan sebagai mana belum adanya *cryptanalysis* yang berhasil meretas AES[19].

Berdasarkan pemaparan latar belakang penelitian di atas bahwa UAV profesional sekalipun jika tanpa penerapan kriptografi maka dapat dilakukan penyerangan dan dari penelitian sebelumnya mengenai penerapan algoritma kriptografi yang diterapkan pada UAV dan GCS belum pernah diterapkan kriptografi AES-128. Penulis mengambil tema tentang keamanan sistem pada *Unmanned Aerial Vehicle* (UAV) dan *Ground Control System* (GCS) dengan judul "Implementasi Kriptografi AES-128 pada *Unmanned Aerial Vehicle* dan *Ground Control System*" sebagai aplikasi yang akan melakukan enkripsi dan dekripsi pada pengiriman data antara UAV dan GCS.

1.2 Rumusan Masalah

Berdasarkan latar belakang penelitian yang telah diuraikan, maka rumusan masalahnya sebagai adalah:

Bagaimana implementasi kriptografi AES-128 pada *unmanned aerial vehicle* dan *ground control system?*

1.3 Maksud dan Tujuan

Maksud dari penulisan penelitian ini adalah membuat data yang dikirimkan *Unmanned Aerial Vehicle* ke *Ground Control System* tidak dapat terbaca oleh penyerang. Sedangkan tujuan yang ingin dicapai dari penelitian ini adalah untuk mengimplementasikan kriptografi AES-128 pada *unmanned aerial vehicle* dan *ground control system*.

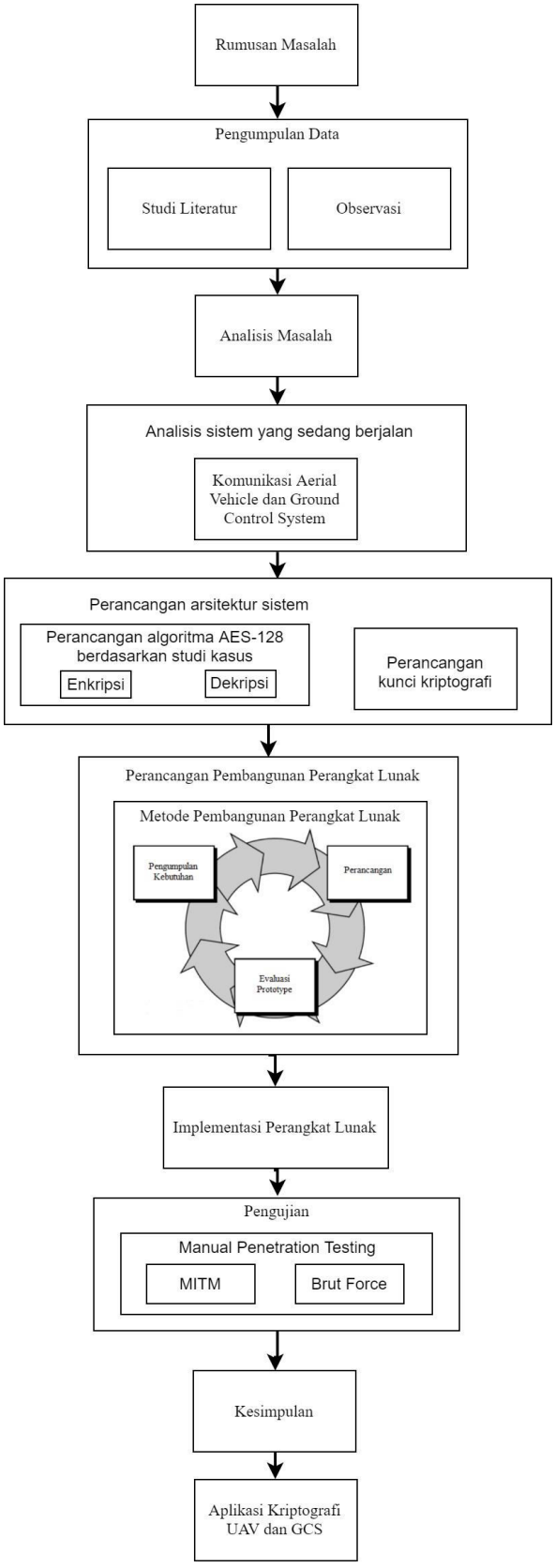
1.4 Batasan Masalah

Adapun batasan masalah dari implementasi enkripsi dan dekripsi AES pada *Unmanned Aerial Vehicle* (UAV) dan *Ground Control System* (GCS) ini agar penelitian lebih terarah dan mencapai tujuan yang telah ditentukan:

1. Aplikasi ini dibangun pada sisi *software* berbasis *desktop*, dan di terapkan pada sisi *software mikrokontroler* berbasis *command line interface* (CLI).
2. Panjang kunci enkripsi dapat menggunakan 128 bit (16 Byte).
3. Mode kriptografi yang digunakan adalah *Advanced Encryption Standard* (AES) dengan mode *Cipher Block Chaining* (CBC).
4. Proses pembangkitan kunci awal menggunakan tanggal dan digabungkan dengan *invers* dari tanggal, sebagai contoh: 1706201991026071.
5. Panjang data (*input*) yang di enkripsi adalah *fixed condition.*
6. Percobaan dilakukan pada sebuah *protorype* UAV dan sebuah *prototype* GCS.
7. Data dikirimkan dengan frekuensi radio 2,4Ghz dan radio frekuensi yang digunakan adalah NRF24l01.
8. Konsep *Man-in-the-Middle* (MitM) digunakan untuk mengetahui data yang dikirimkan melalui radio frekuensi.

1.5 Metodologi Penelitian

Metodologi penelitian merupakan suatu proses yang akan digunakan untuk memecahkan suatu masalah yang logis, dimana memerlukan data untuk mendukung terlaksananya suatu penelitian. Metodologi penelitian yang digunakan adalah metode analisis deskriptif, yaitu suatu metode untuk mendapatkan gambaran yang jelas tentang hal-hal yang diperlukan. Metodologi penelitian yang digunakan dalam penilitian ini terbagi menjadi beberapa tahapan. Seperti yang ditampilkan pada Gambar 1.1, yaitu sebagai berikut.



Gambar 1.1 Metodologi Penelitian

1.5.1 Rumusan Masalah

Rumusan masalah adalah kalimat singkat berupa pertanyaan terhadap keberadaan variabel mandiri baik hanya satu variabel maupun lebih, rumusan masalah digunakan untuk menjelaskan masalah atau isu yang sedang diteliti.

1.5.2 Pengumpulan Data

Metode pengumpulan data yang dilakukan pada penelitian ini dilakukan dengan studi literatur dan observasi. Studi Literatur adalah pengumpulan data dengan cara mengumpulkan jurnal, paper dan bacaan-bacaan yang berkaitan dengan judul penelitian yang diambil dan mengumpulkan segala informasi untuk pembangunan sistem.

1.5.3 Analisis Masalah

Hasil dari rumusan masalah dan pengumpulan data menghasilkan analisis masalah, masalah dapat tervalidasi untuk dilakukan penelitian.

1.5.4 Analisis Sistem yang Sedang Berjalan

Pada tahapan ini, sistem yang berjalan perlu di analisis untuk evaluasi dari sistem baru yang akan dibuat. Dari tahapan ini didapatkan proses bisnis mana saja yang mungknin akan berubah untuk menyesuaikan dengan sistem yang baru.

1.5.5 Perancangan Arsitektur Sistem

Pada tahapan ini sudah terlihat arsitektur sistem yang baru, yang akan diterapkan pada UAV dan GCS. Arsitektur sistem akan membahas proses bisnis yang baru. Arsitektur sistem juga sudah bisa memberikan gambaran di mana kriptografi akan diterapkan dan entitas yang akan ada di sistem.

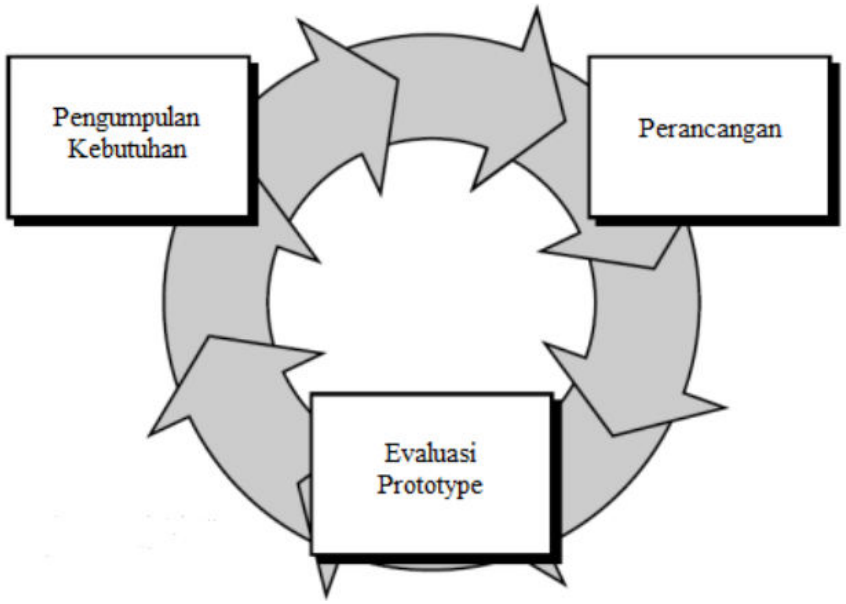
1.5.6 Perancangan Perangkat Lunak

Perancangan perangkat lunak adalah suatu proses bertahap dimana semua kebutuhan atau persyaratan yang ada pada dokumen diterjemahkan menjadi suatu

cetak blue (*blue print*) yang akan digunakan untuk membangun perangkat lunak dan memenuhi kebutuhan yang sesuai.

1.5.6.1 Metode Pembangunan Perangkat Lunak

Metode pembangunan perangkat lunak menggunakan paradigma perangkat lunak secara *prototype*. Alur dari metode *prototype* bisa di lihat pada Gambar 1.2 untuk penjelasan dari setiap alur metode *prototype* adalah sebagai berikut[20]:



Gambar 1.2 Model Prototype

1. Pengumpulan Kebutuhan

   Pengumpulan data dengan cara mengumpulkan literatur, jurnal, paper dan bacaan-bacaan yang ada kaitannya dengan judul penelitian.
2. Perancangan

   Perancangan dilakukan cepat dan rancangan mewakili semua aspek software yang diketahui. Rancangan ini akan menjadi dasar pembuatan protoype.
3. Evaluasi Prototype

   Pengujian terhadap software yang dibuat dan digunakan untuk memperjelas kebutuhan software.

1.5.7 Implementasi Perangkat Lunak

Suatu proses pengubahan spesifikasi sistem menjadi sistem yang dapat dijalankan untuk dapat dilakukan pengujian.

1.5.8 Pengujian

Pengujian merupakan tahap untuk menguji dari hasil program yang sudah dibangun agar sesuai dengan yang di inginkan. Pengujian yang digunakan adalah *Manual penetration testing* yaitu pengujian penetrasi yang dilakukan oleh manusia. Dalam jenis pengujian ini, kerentanan dan resiko suatu mesin diuji oleh seorang ahli di bidangnya[21].

Secara umum, teknisi pengujian melakukan metode berikut :

Data Collection − *Data collection* memiliki peran penting untuk pengujian. Seseorang dapat mengumpulkan data secara manual atau dapat menggunakan layanan alat / *software* (seperti teknik analisis kode sumber halaman web, *man-in-the-middle attack,* dll.).

Vulnerability Assessment −Setelah data dikumpulkan,selanjutnya penguji untuk mengidentifikasi kelemahan keamanan dan mengambil langkah-langkah pencegahan yang sesuai.

Actual Exploit − adalah metode khas yang digunakan oleh penguji ahli untuk melakukan serangan pada sistem target dan juga, mengurangi risiko serangan. Dalam penelitian ini menggunakan *brute force attack*.

Report Preparation − Setelah penetrasi dilakukan, tenaga ahli menyiapkan laporan akhir yang menjelaskan segala sesuatu tentang sistem. Akhirnya laporan dianalisis untuk mengambil langkah korektif untuk melindungi sistem target.

1.5.9 Kesimpulan

Kesimpulan adalah pernyataan singkat tentang hasil analisis deskripsi dan pembahasan tentang isi dari penelitian, kesimpulan berisikan fakta-fakta jawaban dari pertanyaan yang ada di rumusan masalah penelitian.

1.6 Sistematika Penulisan

Penyusunan penelitian ini dibagi kedalam beberapa bab secara sistematis sesuai dengan pokok-pokok permasalahan yang dibahas. Adapun sistematika penulisan secara secara umum adalah sebagai berikut :

BAB 1 PENDAHULUAN

Bab ini menjelaskan mengenai latar belakang masalah, identifikasi masalah, maksud dan tujuan, batasan masalah, metodelogi penelitian, dan sistematika penulisan.

BAB 2 TINJAUAN PUSTAKA

Bab ini menjelaskan mengenai landasan teori dan konsep dasar yang menyangkut kasus yang diangkat.

BAB 3 ANALISIS DAN PERANCANGAN SISTEM

Bab ini akan menganalisis masalah dari perangkat lunak yang akan dibangun dan merupakan tahapan yang dilakukan dalam pembangunan secara garis besar, mulai dari tahap persiapan sampai penarikan kesimpulan.

BAB 4 IMPLEMENTASI DAN PENGUJIAN SISTEM

Bab ini membahas implementasi dalam bahasa pemograman yaitu implementasi kebutuhan perangkat keras dan perangkat lunak, implementasi antarmuka dan tahap-tahap dalam melakukan pengujian perangkat lunak.

BAB 5 KESIMPULAN DAN SARAN

Pembahasan mengenai kesimpulan dari keseluruhan masalah yang telah dibahas pada bab sebelumnya dan dilengkapi dengan saran–saran yang dapat dijadikan masukan dalam melakukan pengembangan dari hasil penulisan tugas akhir.