

BAB I

PENDAHULUAN

1.1 Latar Belakang

Kriptografi adalah sebuah ilmu atau seni yang berguna sebagai penjaga kerahasiaan pesan dengan cara mengubah pesan ke dalam bentuk yang tidak dapat dimengerti lagi maknanya (Simargolang, 2017). Ilmu ini biasanya dipelajari di dalam ilmu komputer maupun jurusan-jurusan yang berkaitan dengan ilmu komputer lainya seperti teknik informatika maupun sistem informasi. Apabila diadaptasi ke dalam sebuah mata kuliah di dalam sebuah jurusan, biasanya mata kuliah ini bersifat wajib karena mengingat pentingnya ilmu ini untuk mengubah pesan maupun file menjadi tidak dapat terbaca oleh orang lain.

Materi-materi di dalam mata kuliah kriptografi dapat dikatakan banyak karena biasanya di dalam sebuah pertemuan kuliah akan membahas mengenai tata cara melakukan suatu metode kriptografi. Metode kriptografi ada banyak dan beragam karena ada banyak algoritma yang terkait dengan metode kriptografi. Contoh-contohnya adalah operasi XOR, *Vigenere Cipher*, *Caesar Cipher*, RSA, dan masih banyak lagi. Metode ini perlu dipelajari dalam jangka waktu yang lama karena masing-masing metode kriptografi ini mempunyai algoritma yang berbeda-beda.

Banyaknya metode-metode kriptografi yang beragam membuat mahasiswa kesulitan memahami materi-materi di dalam mata kuliah kriptografi. Terkadang, tenaga pengajar seperti dosen juga kesulitan memahami materi-materi di dalam mata kuliah kriptografi karena banyaknya metode-metode kriptografi yang beragam. Hal ini sangat berdampak kepada mahasiswa dan membuat mahasiswa menjadi sulit mempelajari mata kuliah kriptografi karena dosen tidak dapat menjelaskan suatu metode kriptografi dengan lancar dan lengkap. Mahasiswa sering mendapatkan penjelasan-penjelasan yang tidak lengkap sehubungan dengan tata cara untuk melakukan sebuah metode kriptografi tertentu.

Teknologi yang sangat pesat memungkinkan orang-orang mencari solusi akan suatu permasalahan di dalam telepon genggamnya. Telepon genggam yang

sering digunakan adalah telepon genggam yang memiliki sistem operasi android. Android adalah sistem operasi untuk telepon seluler yang berbasis linux. Android menyediakan platform terbuka bagi para pengembang untuk membuat aplikasi mereka sendiri (Kuswanto & Radiansah, 2018). Di dalam android, terdapat perangkat lunak untuk berselancar di *internet* sehingga memungkinkan mahasiswa untuk mencari penjelasan seputar metode kriptografi tertentu. Mahasiswa jarang menggunakan perangkat lainya seperti laptop maupun komputer karena perangkat tersebut sulit diakses ketika dalam situasi tertentu.

Mahasiswa sering mencari-cari penjelasan sehubungan dengan metode kriptografi di dalam telepon genggam android sehingga mereka dapat memperoleh penjelasan yang baik dan lengkap sehubungan dengan tata cara untuk melakukan metode kriptografi tertentu. Akan tetapi, permasalahan yang ditemukan di dalam pencarian seringkali tidak memuaskan karena masalah yang ditemukan tidak beragam. Pencarian yang ditemukan memiliki permasalahan yang sama sehingga mahasiswa tidak dapat melihat perbedaan sehubungan dengan tata cara melakukan suatu metode kriptografi tertentu.

Di dalam sebuah mata kuliah, kemungkinan besar terdapat tugas di dalamnya. Tugas-tugas yang diberikan oleh dosen pengampu sehubungan dengan mata kuliah kriptografi pasti menyangkut metode-metode kriptografi yang telah dijelaskan kepada mahasiswa. Tugas-tugas ini biasanya berbentuk pertanyaan yang meminta penjelasan tentang bagaimana sebuah hasil dari metode kriptografi tertentu dapat diperoleh. Permasalahan yang terdapat di dalam tugas-tugas ini pasti bersifat konstan karena di dalam sebuah metode kriptografi terdapat algoritma yang serupa.

Permasalahan ini sulit ditemukan solusinya karena tidak ada sebuah perangkat lunak yang mampu memberikan penjelasan sehubungan dengan melakukan metode-metode kriptografi tertentu (contoh aplikasi: “*Crypto – Tools for Encryption & Cryptography*”, “Belajar Kriptografi RC4 & RSA”). Sebagian besar perangkat lunak kriptografi hanya menampilkan hasil karena fungsinya bukan sebagai media pembelajaran melainkan sebagai perangkat lunak yang menyandikan pesan agar tidak dapat dimengerti oleh orang lain. Perangkat lunak berjenis ini tidak

dapat dijadikan sebagai solusi untuk menangani permasalahan yang dihadapi oleh para mahasiswa terkait dengan tugas dalam mata kuliah kriptografi.

Mahasiswa lebih berorientasi kepada perangkat lunak yang dapat diakses secara luring (luar jaringan / *offline*) karena perangkat lunak ini dapat berjalan tanpa bantuan koneksi *internet*. Perangkat lunak yang bersifat luring ini diharapkan dapat membantu mahasiswa untuk mempelajari tata cara untuk melakukan metode kriptografi tertentu. Perangkat lunak ini akan lebih baik apabila dapat diimplementasikan di dalam telepon seluler berbasis android karena telepon seluler dapat digunakan oleh orang-orang dalam waktu dan tempat yang bebas. Perangkat lunak ini harus mudah diakses oleh pengguna android sehingga pengguna tidak segan-segan ketika ingin memasang perangkat lunak ini pada telepon seluler pengguna tersebut.

1.2 Perumusan Masalah

1.2.1 Batasan Masalah

Berikut ini merupakan batasan-batasan dari masalah yang telah diidentifikasi pada bagian sebelumnya:

1. Penjelasan yang dibutuhkan oleh mahasiswa maupun pihak lainya berbentuk teks.
2. Permasalahan yang dialami oleh mahasiswa maupun pihak lainya adalah berupa teks, bukan file.
3. Masalah yang dipaparkan dikhususkan hanya untuk pihak mahasiswa sebagai pelajar yang kesulitan mempelajari ilmu kriptografi.

1.2.2 Rumusan Masalah

Berikut ini merupakan hasil rumusan masalah berdasarkan masalah yang telah dipaparkan dan diidentifikasi pada bagian latar belakang:

1. Apakah perangkat lunak media pembelajaran teknologi informasi berbasis android mempengaruhi mahasiswa dalam mempelajari materi-materi di dalam mata kuliah kriptografi?

2. Apa solusi yang mampu mengatasi kesulitan mahasiswa jurusan Teknik Informatika sehubungan dengan mempelajari materi-materi di dalam mata kuliah kriptografi?
3. Apa tanggapan dari para ahli mengenai media pembelajaran yang telah dikembangkan?

1.3 Tujuan dan Manfaat

1.3.1 Tujuan Penelitian

Bedasarkan masalah yang telah dirumuskan, tujuan dari diadakanya penelitian ini adalah sebagai berikut:

1. Menilai seberapa baik pemanfaatan media pembelajaran teknologi informasi aplikasi Belajar Kriptografi berbasis android.
2. Mengembangkan sebuah perangkat lunak berbasis android untuk belajar materi kriptografi secara interaktif dan menilai kelayakan aplikasi.
3. Menilai tanggapan para ahli terkait dengan aplikasi media pembelajaran Belajar Kriptografi.

1.3.2 Manfaat Penelitian

Berikut ini merupakan manfaat-manfaat diadakanya penelitian:

1. Memberikan kontribusi bagi dunia pendidikan seputar pengembangan perangkat lunak.
2. Memberikan bahan referensi bagi peneliti-peneliti yang ingin membuat penelitian dengan jenis yang sama.
3. Memberikan bahan referensi bagi pengembang-pengembang yang ingin mengembangkan perangkat lunak di telepon genggam yang memiliki sistem operasi android.
4. Menambah pengetahuan serta wawasan peneliti seputar pengembangan perangkat lunak berbasis android.
5. Menambah pengetahuan seputar cara mengembangkan algoritma kriptografi menjadi dapat dijelaskan.

6. Memberikan sebuah aplikasi berbasis android yang dapat menangani permasalahan mahasiswa atau orang-orang yang sedang mempelajari ilmu kriptografi.
7. Membuat orang-orang mengetahui cara mengimplementasikan metode pengembangan perangkat lunak ke dalam proses pengembangan perangkat lunak berbasis android.

1.4 Ruang Lingkup Studi

Penelitian ini harus dilakukan secara terstruktur serta terorganisir dengan baik. Agar dapat melakukan penelitian yang baik, diperlukan sebuah ruang lingkup studi yang dapat menjelaskan struktur dari penelitian. Struktur dari penelitian meliputi bab dan isi dari masing-masing bab yang terdapat di dalam penelitian tersebut. Berikut ini merupakan ruang lingkup studi dari penelitian (struktur penulisan):

1. BAB I PENDAHULUAN

Memuat latar belakang serta masalah yang ditemukan seputar penelitian ini. Pendahuluan juga memuat tujuan dan manfaat diadakannya penelitian ini serta ruang lingkup studi (skema penulisan).

2. BAB II LANDASAN TEORI

Memuat teori-teori yang berhubungan dengan penelitian yang dilakukan. Teori-teori ini hendaknya mengutip dari jurnal atau bacaan resmi lainnya dan tidak menyalin. Landasan teori juga memuat hipotesis maupun tinjauan pustaka yang digunakan untuk mengembangkan penelitian ini.

3. BAB III METODE PENELITIAN

Memuat tempat dan waktu penelitian, tahapan penelitian, kerangka berpikir, serta metode pengumpulan data. Di dalam metode penelitian juga perlu dilampirkan metode untuk menganalisis data yang telah dikumpulkan untuk dapat digunakan di dalam bab empat. Metode-metode yang terdapat di dalam bab ini harus bersumber dari literatur yang terpercaya atau direkomendasikan oleh para ahli.

4. BAB IV HASIL DAN PEMBAHASAN

Bagian laporan yang membahas hasil dari penelitian yang telah dirancang. Hasil ini berupa data kuantitatif yang dihadirkan beserta dengan analisisnya. Selain itu, dihadirkan juga hasil pengembangan aplikasi media pembelajaran berupa rancangan aplikasi dalam bentuk diagram-diagram serta antarmuka tampilan aplikasi. Hasil konstruksi aplikasi juga akan dibahas serta dipaparkan di dalam bagian ini.

5. BAB V KESIMPULAN

Kesimpulan dari seluruh penelitian yang diadakan akan dibahas di dalam bagian ini. Hasil pengembangan dan penelitian juga akan dibuat konklusinya dalam bentuk paragraf singkat di bagian ini.