Sistem *Secure e-book* Berbasis Desktop Dengan Algoritma AES

Tugas Akhir

Disusun oleh:

LIDYA AGNES PUSPITASARI

22084393

PROGRAM STUDI TEKNIK INFORMATIKA

FAKULTAS TEKNOLOGI INFORMASI

UNIVERSITAS KRISTEN DUTA WACANA

YOGYAKARTA

2016

Sistem *Secure e-book* Berbasis Desktop Dengan Algoritma AES

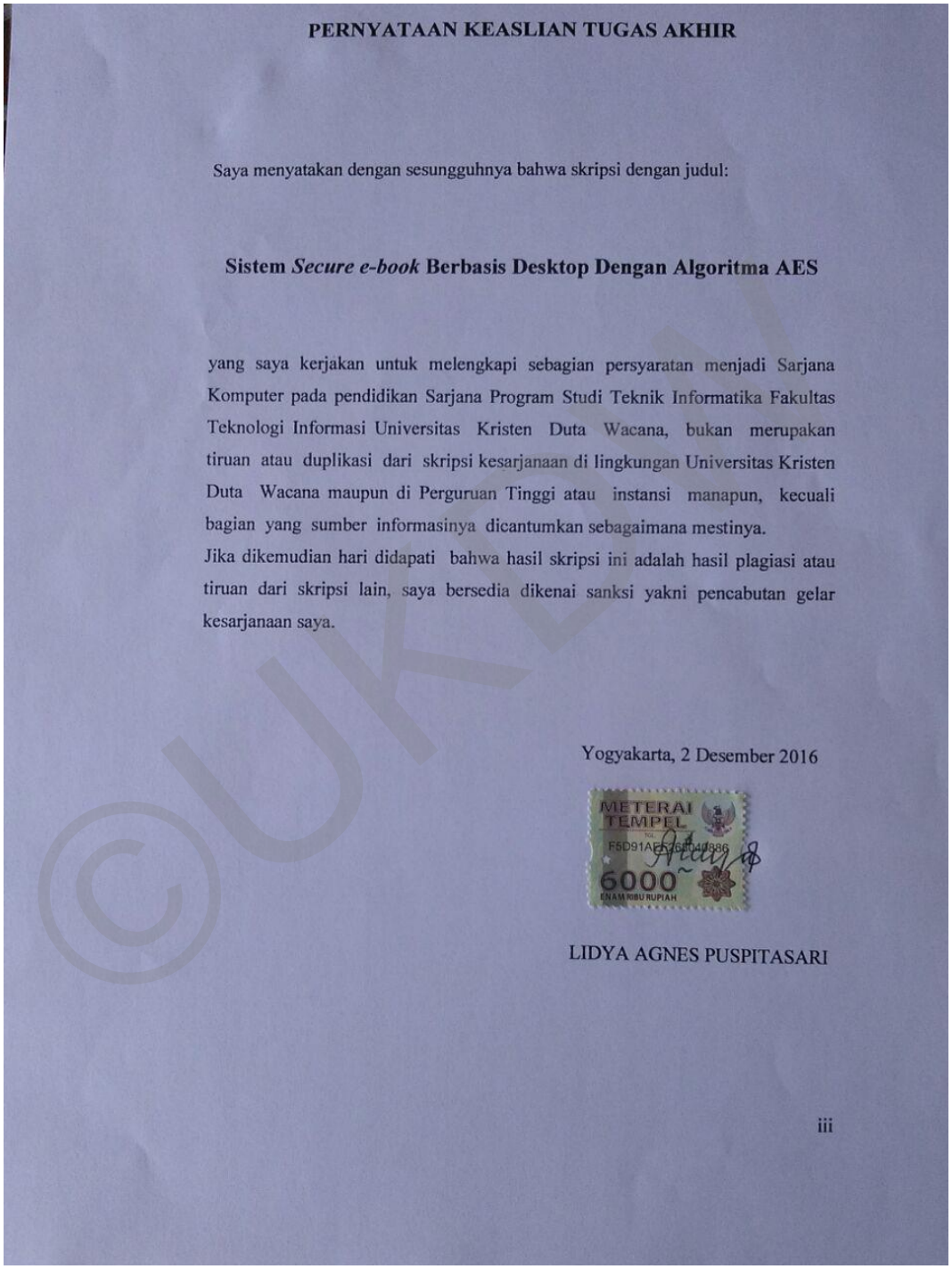
Tugas Akhir

Diajukan kepada Program Studi Teknik Informatika Fakultas Teknologi Informasi
Universitas Kristen Duta Wacana
Sebagai Salah Satu Syarat dalam Memperoleh Gelar
Sarjana Komputer

Disusun oleh:
LIDYA AGNES PUSPITASARI
22084393

PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS TEKNOLOGI INFORMASI
UNIVERSITAS KRISTEN DUTA WACANA
YOGYAKARTA
2016

PERNYATAAN KEASLIAN TUGAS AKHIR



PERNYATAAN KEASLIAN TUGAS AKHIR

Saya menyatakan dengan sesungguhnya bahwa skripsi dengan judul:

Sistem *Secure e-book* Berbasis Desktop Dengan Algoritma AES

yang saya kerjakan untuk melengkapi sebagian persyaratan menjadi Sarjana Komputer pada pendidikan Sarjana Program Studi Teknik Informatika Fakultas Teknologi Informasi Universitas Kristen Duta Wacana, bukan merupakan tiruan atau duplikasi dari skripsi kesarjanaan di lingkungan Universitas Kristen Duta Wacana maupun di Perguruan Tinggi atau instansi manapun, kecuali bagian yang sumber informasinya dicantumkan sebagaimana mestinya.
Jika dikemudian hari didapati bahwa hasil skripsi ini adalah hasil plagiasi atau tiruan dari skripsi lain, saya bersedia dikenai sanksi yakni pencabutan gelar kesarjanaan saya.

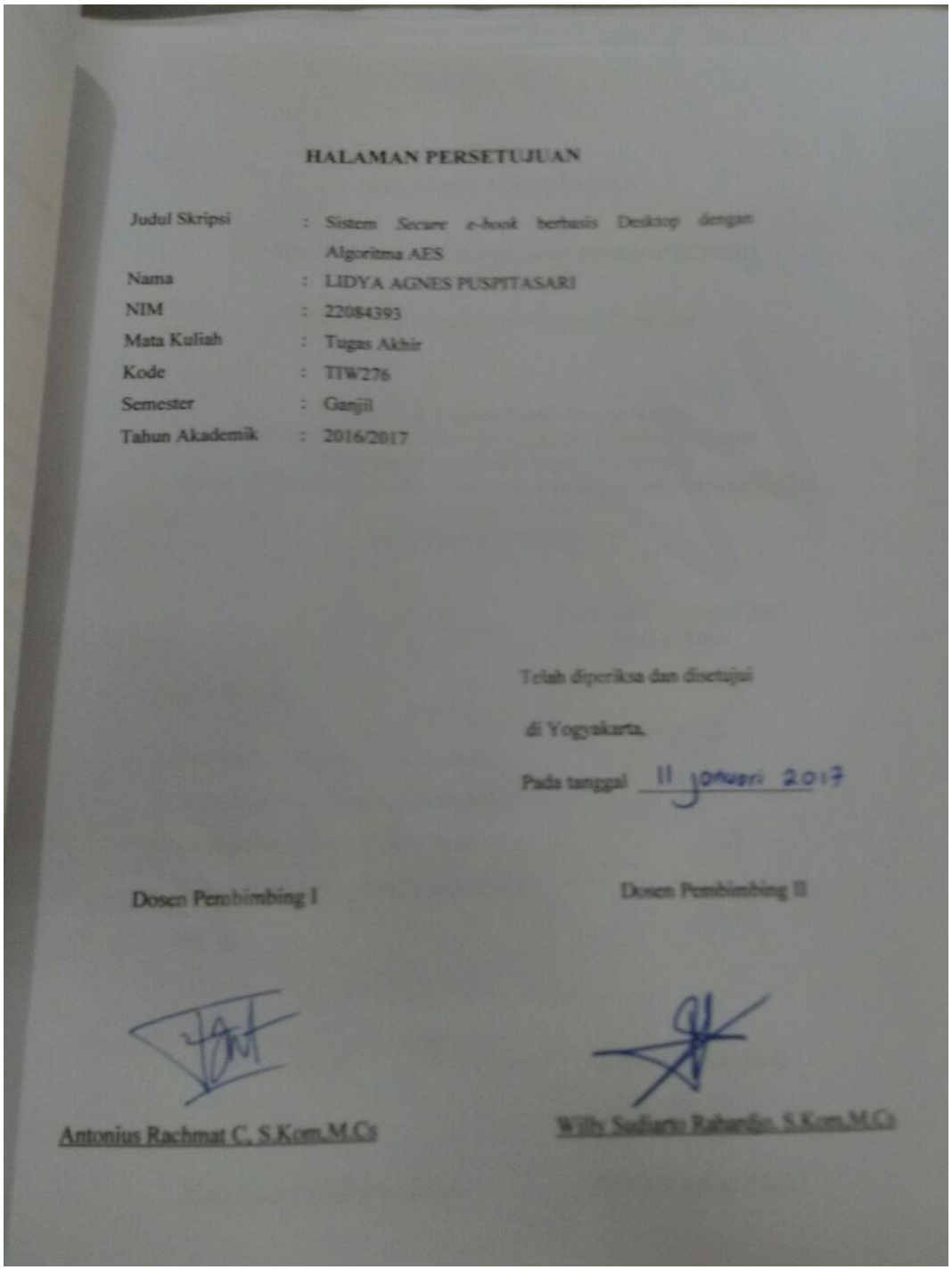
Yogyakarta, 2 Desember 2016

METERAI TEMPEL 6000 ENAM RIBU RUPIAH

LIDYA AGNES PUSPITASARI

iii

HALAMAN PERSETUJUAN



HALAMAN PERSETUJUAN

Judul Skripsi	:	Sistem *Secure e-book* berbasis Desktop dengan Algoritma AES
Nama	:	LIDYA AGNES PUSPITASARI
NIM	:	22084393
Mata Kuliah	:	Tugas Akhir
Kode	:	TIW276
Semester	:	Ganjil
Tahun Akademik	:	2016/2017

Telah diperiksa dan disetujui

di Yogyakarta,

Pada tanggal 11 januari 2017

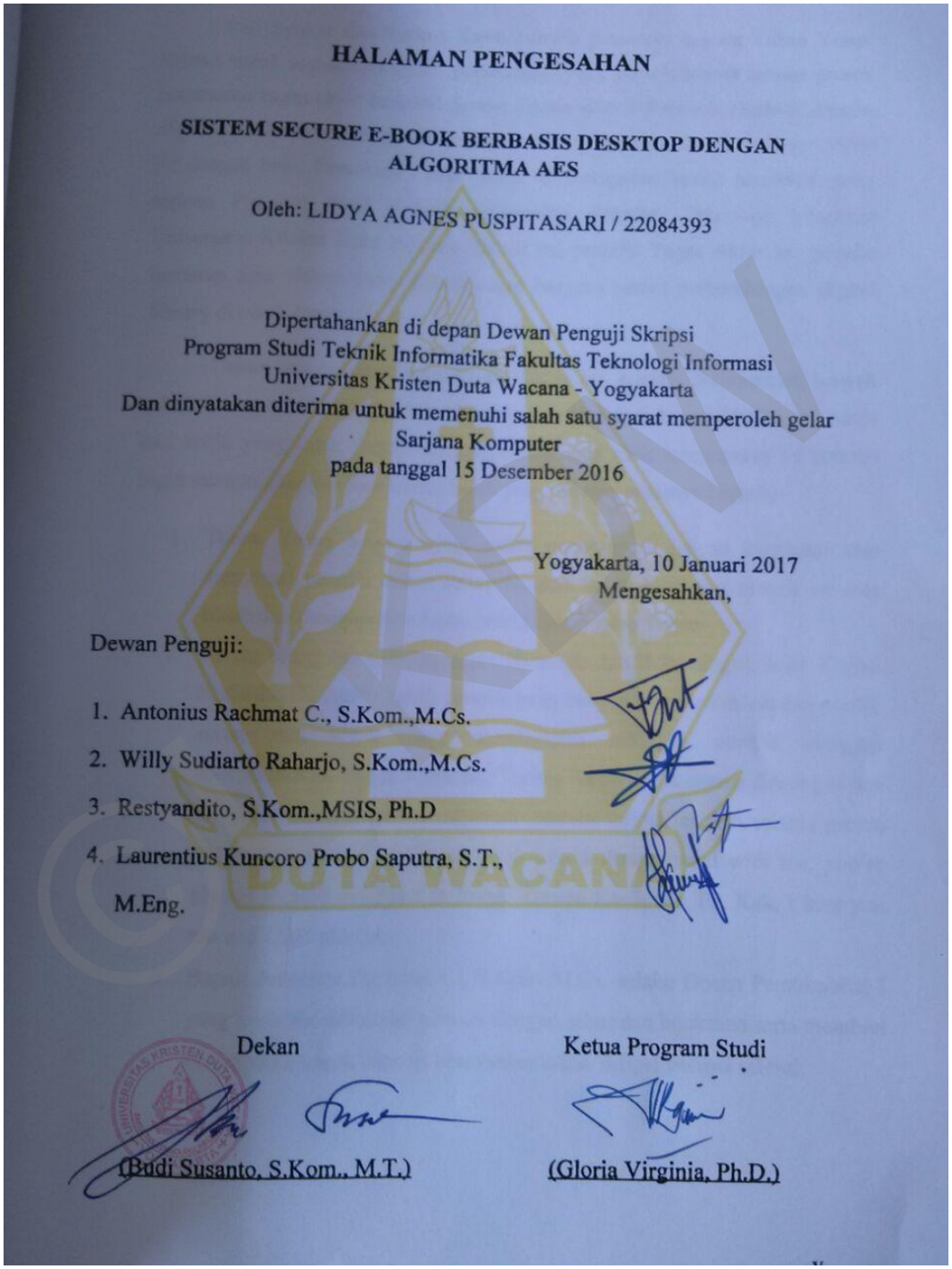
Dosen Pembimbing I

Antonius Rachmat C, S.Kom,M.Cs

Dosen Pembimbing II

Wiby Sudiarto Rahardjo, S.Kom,M.Cs

HALAMAN PENGESAHAN



HALAMAN PENGESAHAN

SISTEM SECURE E-BOOK BERBASIS DESKTOP DENGAN ALGORITMA AES

Oleh: LIDYA AGNES PUSPITASARI / 22084393

Dipertahankan di depan Dewan Penguji Skripsi
Program Studi Teknik Informatika Fakultas Teknologi Informasi
Universitas Kristen Duta Wacana - Yogyakarta
Dan dinyatakan diterima untuk memenuhi salah satu syarat memperoleh gelar
Sarjana Komputer
pada tanggal 15 Desember 2016

Yogyakarta, 10 Januari 2017
Mengesahkan,

Dewan Penguji:

1. Antonius Rachmat C., S.Kom.,M.Cs.
2. Willy Sudiarto Raharjo, S.Kom.,M.Cs.
3. Restyandito, S.Kom.,MSIS, Ph.D
4. Laurentius Kuncoro Probo Saputra, S.T., M.Eng.

Dekan

(Budi Susanto, S.Kom., M.T.)

Ketua Program Studi

(Gloria Virginia, Ph.D.)

UCAPAN TERIMA KASIH

Puji Syukur dan Terima Kasih penulis panjatkan kepada Tuhan Yesus Kristus untuk segala berkat dan pertolongan yang penulis terima selama proses pembuatan tugas akhir berjudul *Sistem Secure eBook Berbasis Desktop dengan Algoritma AES* ini sehingga akhirnya penulis mampu menyelesaikan Tugas Akhir ini dengan baik. Penulisan Tugas Akhir ini merupakan syarat perolehan gelar sarjana Program Studi Teknik Informatika Fakultas Teknologi Informasi Universitas Kristen Duta Wacana. Selain itu, melalui Tugas Akhir ini, penulis berharap agar sistem yang dibuat dapat berguna untuk perkembangan *digital librar*y di masa depan.

Dalam proses pembuatan Tugas Akhir ini, penulis memperoleh banyak sekali bantuan baik secara fisik maupun mental dalam bentuk dukungan, saran dan kritik yang tidak ternilai harganya. Sehingga pada kesempatan ini penulis ingin mengungkapkan rasa terima kasih yang sebesar-besarnya kepada:

1. Tuhan Yesus Kristus yang sudah memberkati dengan kesehatan dan menyertai penulis dalam setiap langkah tanpa henti dan menghibur saat susah dan mengajarkan hidup selalu dalam jalan Tuhan.
2. Kedua orang tua penulis, Agus Handoyo dan Retnaningsih serta Karina Mayasita H. selaku kakak penulis yang banyak memberi dukungan moriil, saran dan kritik yang membangun sehingga penulis sanggup menyelesaikan Tugas Akhir ini. Terima Kasih untuk semua dukungan doa dan kasih sayang tulus yang selalu penulis terima terlebih selama proses pembuatan skripsi ini. Eventhough you'd disappointed with me, you're always remind me that I'm loved. Terima Kasih Ma, Pa, Kak, I love you too and GBU always.
3. Bapak Antonius Rachmat C., S.Kom.,M.Cs. selaku Dosen Pembimbing I yang telah membimbing penulis dengan sabar dan bijaksana serta memberi kesempatan untuk penulis bisa melanjutkan skripsi sampai selesai.

4. Bapak Willy Sudiarto R, S.Kom.,M.Cs. selaku Dosen Pembimbing II yang telah membimbing penulis dengan sabar dan bijaksana serta memberi saran dengan baik dan pengertian.
5. Ibu Gloria Virginia, S.Kom., MAI, Ph.D selaku Kaprodi Teknik Informatika untuk pengertiannya terhadap masalah penulis serta menanggapi dengan kata-kata yang halus.
6. Bapak Restyandito, S.Kom., MSIS., Ph.D. dan Bapak Laurentius Kuncoro Probo Saputra, S.T., M.Eng. selaku dosen penguji ketika penulis melakukan pendadaran. Terima kasih sudah menguji penulis dengan sabar dan bijaksana.
7. Mbak Rachel untuk kesabarannya berbagi ilmu dan nasehat serta pengertiannya untuk penulis. Semoga Tuhan Memberkati.
8. Secara khusus untuk teman-teman penulis Putri Hayuningtyas, Cicilia Rini Astuti, Renny Puspita Hardini, Agung Prasetyo, Valery Nicolay serta Apriliana Lolita yang selalu mendampingi dan memberikan semangat selama penulis mengerjakan skripsi.
9. Serta semua pihak yang tidak dapat penulis sebutkan satu per satu.

Penulis menyadari bahwa dalam pembuatan tugas akhir ini ada banyak kesalahan yang penulis lakukan baik disengaja maupun tidak sengaja oleh karena itu penulis menyampaikan permintaan maaf yang sebesar-besarnya apabila dalam pembuatan skripsi ini Penulis membuat kesalahan. Melalui tugas akhir ini penulis berharap agar penulis dapat menambah pengetahuan dan wacana yang ada.

Demikian laporan ini dibuat, mohon maaf yang setulus – tulusnya jika terdapat kata – kata yang tidak berkenan dalam penulisan laporan.

Yogyakarta, 10 Januari 2017

Lidya Agnes P.

INTISARI

Sistem *Secure e-book* Berbasis Desktop Dengan Algoritma AES

Dengan perkembangan internet dan teknologi saat ini membuat banyak hal-hal fisik berubah sifatnya menjadi elektronik salah satunya buku. Saat ini telah banyak beredar buku elektronik atau eBook dengan berbagai macam format dan aplikasi yang terkait dengan eBook tersebut. Seiring dengan hal-hal positif yang terjadi dalam setiap kemajuan teknologi, permasalahan yang menyertai pun ikut bertambah.

Dengan maraknya buku elektronik juga menyebabkan berbagai macam masalah terkait dengan kegiatan *sharing* file yang terjadi diantara banyak user sehingga menimbulkan masalah *digital rights*. Sehingga banyak pengarang memilih untuk tidak menerbitkan bukunya dalam bentuk digital. Hal inilah yang mendorong penulis untuk mengembangkan sebuah sistem yang diberi nama Fortome yang berfungsi sebagai sarana peminjaman buku elektronik dengan beberapa pencegahan yang disesuaikan agar melindungi hak cipta dari pengarang tanpa membuat user terbatas.

Dalam pembuatan aplikasi Fortome ini, penulis menggunakan beberapa studi kasus yang akan dibahas dalam subbab-subbab terperinci terkait dengan permasalahan yang mungkin muncul saat peminjaman dilakukan oleh user dan bagaimana sistem mengatasi kemungkinan kebocoran file yang dapat mengakibatkan kerugian dan masalah hak cipta bagi banyak orang terutama pengarang buku.

Dan dari hasil pengujian terhadap beberapa kasus, aplikasi ini mampu menghalangi permasalahan kebocoran file. Penulis menyadari bahwa tidak ada sistem yang sempurna. Oleh karena itu penuli mengembangkan aplikasi ini

dengan tujuan agar setidaknya permasalahan kebocoran file yang terjadi saat peminjaman buku secara *online* dapat diminimalisir.

Kata Kunci: *digital right management, enkripsi, aes, aes-128, aplikasi desktop, fortome*

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

INTISARI

Sistem *Secure e-book* Berbasis Desktop Dengan Algoritma AES

Dengan perkembangan internet dan teknologi saat ini membuat banyak hal-hal fisik berubah sifatnya menjadi elektronik salah satunya buku. Saat ini telah banyak beredar buku elektronik atau eBook dengan berbagai macam format dan aplikasi yang terkait dengan eBook tersebut. Seiring dengan hal-hal positif yang terjadi dalam setiap kemajuan teknologi, permasalahan yang menyertai pun ikut bertambah.

Dengan maraknya buku elektronik juga menyebabkan berbagai macam masalah terkait dengan kegiatan *sharing* file yang terjadi diantara banyak user sehingga menimbulkan masalah *digital rights*. Sehingga banyak pengarang memilih untuk tidak menerbitkan bukunya dalam bentuk digital. Hal inilah yang mendorong penulis untuk mengembangkan sebuah sistem yang diberi nama Fortome yang berfungsi sebagai sarana peminjaman buku elektronik dengan beberapa pencegahan yang disesuaikan agar melindungi hak cipta dari pengarang tanpa membuat user terbatas.

Dalam pembuatan aplikasi Fortome ini, penulis menggunakan beberapa studi kasus yang akan dibahas dalam subbab-subbab terperinci terkait dengan permasalahan yang mungkin muncul saat peminjaman dilakukan oleh user dan bagaimana sistem mengatasi kemungkinan kebocoran file yang dapat mengakibatkan kerugian dan masalah hak cipta bagi banyak orang terutama pengarang buku.

Dan dari hasil pengujian terhadap beberapa kasus, aplikasi ini mampu menghalangi permasalahan kebocoran file. Penulis menyadari bahwa tidak ada sistem yang sempurna. Oleh karena itu penuli mengembangkan aplikasi ini

dengan tujuan agar setidaknya permasalahan kebocoran file yang terjadi saat peminjaman buku secara *online* dapat diminimalisir.

Kata Kunci: *digital right management, enkripsi, aes, aes-128, aplikasi desktop, fortome*

BAB 1

PENDAHULUAN

1.1 Latar Belakang Masalah

Kemajuan teknologi saat ini sudah mencakup banyak bidang. Salah satunya bidang pendidikan. Perpustakaan sebagai salah satu institusi yang terkait langsung dengan dunia pendidikan juga ikut terpengaruh oleh kemajuan teknologi saat ini. Hal ini dapat dilihat dari perubahan sistem perpustakaan dari perpustakaan yang dulu harus mencari satu per satu buku yang akan dibaca atau dipinjam, menjadi perpustakaan yang sudah memiliki sistem informasi katalog sehingga memudahkan pengunjung yang akan mencari buku. Contoh lainnya yaitu koleksi tugas akhir di beberapa perpustakaan dulu masih berupa cetakan dan membutuhkan jumlah rak yang semakin besar seiring dengan bertambahnya koleksi yang masuk setiap tahunnya, sekarang sebagian besar sudah berubah ke bentuk digital. Dan saat ini, sudah banyak buku-buku yang beralih dari format cetak ke format digital. Buku-buku digital ini biasa disebut *electronic book* atau *e-book*.

Pada sistem perpustakaan digital yang berkembang saat ini, tidak banyak yang menyediakan peminjaman *e-book* dikarenakan masalah *copyright* dan sekuritas *e-book* tersebut sehingga sistem perpustakaan *digital* yang ada sekarang ini sebagian besar hanya sebatas meng-*online*-kan katalog perpustakaannya saja, memberi *limited preview* dari buku yang dicari, melayani *online reading*, dsbnya. Agar dapat dipinjamkan secara *online*, *e-book* tersebut harus memiliki sistem keamanan baik di dalam *e-book* itu sendiri maupun dari segi sistem peminjaman dan transfer *file*nya.

Pada penelitian tugas akhir ini, penulis akan mencoba membuat *secure e-book* yang dapat dipinjamkan secara *online*. Aplikasi ini dinamakan Fortome. Untuk penjelasan mengenai sistem keamanan yang dibuat baik di dalam *e-book*

tersebut sendiri maupun sistem *transfer file* yang aman akan dibahas lebih lanjut dalam poin poin berikutnya.

1.2 Perumusan Masalah

Berdasarkan latar belakang yang didefinisikan pada poin sebelumnya, masalah-masalah yang akan dihadapi dalam tugas akhir adalah:

1. Bagaimana membuat *e-book* yang hanya bisa dibuka oleh aplikasi tertentu?
2. Bagaimana membuat *e-book* yang hanya bisa dibuka dalam jangka waktu tertentu?
3. Bagaimana menerapkan kriptografi untuk membuat *secure e-book*?

1.3 Batasan Masalah

Permasalahan yang akan diuji dalam tugas akhir ini akan diberikan beberapa batasan seperti yang dirinci pada poin-poin dibawah ini.

1. File *e-book* yang akan diuji adalah file ePub yang memiliki ekstensi .epub.
2. Algoritma AES yang digunakan adalah AES-128.
3. Aplikasi harus dalam keadaan *online*.
4. Proses *sign up* akun dilakukan pada aplikasi *desktop*.
5. Peminjaman dibatasi hingga 5 judul dengan kurun waktu peminjaman yaitu 1 minggu.

1.4 Tujuan Penelitian

Tujuan dari penelitian Tugas Akhir ini adalah membuat sebuah sistem yang memungkinkan peminjaman *file* ePub secara *online,* namun juga mampu mengatasi masalah-masalah sekuritas yang terjadi pada proses peminjaman tersebut, baik masalah yang muncul dari sisi *user* maupun dari sistem peminjaman itu sendiri.

1.5 Metode Penelitian

Dalam melakukan penelitian guna menyusun tugas akhir Sistem *Secure e-Book* Berbasis Desktop dengan Algoritma AES ini, penulis melakukan beberapa hal:

1. Studi Literatur

   Pada metode studi literatur, dilakukan pencarian dan pemahaman literatur yang berhubungan dengan penelitian guna dibuatnya aplikasi. Literatur yang digunakan meliputi buku referensi dan dokumentasi internet.

2. Perancangan sistem

   Pada metode perencanaan dan perancangan, dilakukan perencanaan kebutuhan guna proses perancangan aplikasi. Perencanaan kebutuhan meliputi perancangan *database*, *data input – output*, *hardware*, *software*, *website interface*, dan dan lain lain guna penyempurnaan aplikasi yang dibuat.

3. Pembuatan sistem

   Pada Pembuatan sistem, sistem dibuat sesuai dengan rancangan yang telah dirancang sebelumnya.

4. Pengujian dan Evaluasi Sistem

   Pengujian dilakukan setelah sistem selesai dan diujikan untuk mengecek jalannya sistem dan kesalahan-kesalahan yang didapat dalam sistem untuk kemudian dievaluasi sehingga sistem dapat lebih disempurnakan lagi.

1.6 Sistematika Penulisan

Dalam penyusunan laporan tugas akhir ini, penulis membagi laporan ini dalam 3 bagian yaitu bagian awal, bagian inti, dan bagian akhir.

Pada bagian awal, penulis mengisi bab tersebut dengan halaman judul, pernyataan keaslian tugas akhir, halaman persetujuan, halaman pengesahan, ucapan terima kasih, intisari, daftar isi, daftar gambar, daftar table, daftar singkatan, dan daftar lampiran.

Pada bagian inti, penulis akan membaginya menjadi 5 bab. Bab 1 merupakan Bab Pendahuluan. Pada bab ini akan dijelaskan mengenai latar belakang penelitian, pokok-pokok masalah yang akan diteliti, serta rincian rencana penelitian yang akan dilakukan oleh penulis. Bab berikutnya adalah Bab 2 yang merupakan Bab Tinjauan Pustaka. Bab ini terbagi lagi menjadi 2 bagian yakni tinjauan pustaka dan landasan teori. Tinjauan pustaka berisi rangkuman sumber pustaka yang terkait dengan topik penelitian. Landasan teori berisi penjelasan teori-teori yang terkait dengan topik penelitian. Bab selanjutnya adalah Bab 3 yang merupakan bab mengenai Analisis dan Perancangan Sistem. Bab ini akan menguraikan rencana rancangan sistem yang akan dibuat dalam penelitian penulis. Rencana rancangan sistem yang akan diuraikan mencakup spesifikasi sistem, alur sistem dan data-data yang digunakan. Bab ini diikuti dengan Bab 4 yaitu bab mengenai Implementasi dan Analisis Sistem. Bab ini akan menjelaskan hasil dari implementasi sistem yang kemudian akan dibahas sesuai dengan teori-teori yang digunakan dalam penelitian. Bab terakhir pada bagian inti laporan ini adalah Bab 5 yaitu Kesimpulan dan Saran yang berisi uraian singkat terkait dengan hasil penelitian yang diperoleh dan saran-saran yang dapat digunakan untuk pengembangan sistem di masa depan.

Bagian akhir laporan akan digunakan untuk mencantumkan lampiran-lampiran yang digunakan dalam topik penelitian.

BAB 5

5.1 Kesimpulan

Dengan dibuatnya sistem aplikasi *secure eBook* berbasis desktop Fortome ini memudahkan *user* untuk dapat melakukan kegiatan seperti pada perpustakaan namun secara online. Tidak hanya memudahkan penggunanya dalam mengakses buku-buku secara online, namun aplikasi ini juga menawarkan keamanan karena proses peminjaman melalui aplikasi ini disertai dengan proses enkripsi dan dekripsi menggunakan algoritma AES-128. Berdasarkan hasil Implementasi dan pengujian sistem yang dilakukan oleh penulis dapat disimpulkan beberapa hal yaitu:

1. Algoritma enkripsi AES-128 dapat diterapkan dengan benar. Hal ini dibuktikan dari proses enkripsi dan dekripsi file .ePub yang dapat ditampilkan kembali melalui aplikasi Fortome ini.
2. Algoritma AES menjaga keamanan file *ebook* karena untuk mengenkripsi dan mendekripsi buku menggunakan kunci yang sama, namun setiap peminjaman memiliki kunci berbeda.
3. Aplikasi ini mampu melakukan pengecekan dan pencegahan apabila status Member yang melakukan peminjaman tidak aktif.
4. Aplikasi ini memerlukan koneksi internet aktif karena aplikasi perlu melakukan pengecekan dengan *database server* secara berkala.
5. Aplikasi ini mampu mengatasi kondisi dimana waktu peminjaman telah habis, namun buku dalam kondisi sedang dibaca / terbuka.
6. Aplikasi ini mampu mengatur hak akses buku sehingga buku yang berstatus terbatas tidak dapat dipinjam.
7. Namun sayangnya aplikasi ini memiliki kendala apabila *member* menggunakan akun mereka di komputer yang berbeda. Agar dapat membaca buku yang mereka inginkan, Member harus melakukan download ulang agar dapat masuk pada tabel *history* peminjaman.

Penulis menyadari bahwa dalam pembuatan aplikasi ini masih terdapat banyak kekurangan sehingga penulis menerima kesan dan pesan yang disampaikan oleh pengguna agar aplikasi ini dapat berguna dan berkembang menjadi lebih baik.

5.2 Saran

Sistem aplikasi ini tentunya masih dapat dikembangkan lebih lanjut. Sistem aplikasi ini dapat dikembangkan pula dengan mengembangkan sistem aplikasi berbasis web sehingga dapat mengatasi kekurangan dari sistem aplikasi ini dimana aplikasi harus diinstall pada komputer client terlebih dahulu agar dapat digunakan. Selain itu, perlu diadakan penelitian lebih lanjut terkait dengan pertumbuhan data yang dapat mengakibatkan ukuran *database* membengkak dan mengurangi kualitas performa aplikasi. Saran lain yang dapat digunakan untuk pengembangan aplikasi ini kedepannya adalah mengatasi permasalahan dimana satu akun masih belum bisa fleksibel digunakan dari komputer manapun. Dengan adanya perbaikan pada masalah ini, diharapkan aplikasi Fortome dapat berguna di masa depan.

DAFTAR PUSTAKA

Ainsworth, H. (n.d.). Epub Format Construction Guide. Retrieved October 12, 2016, from http://www.hxa.name/articles/content/epub-guide_hxa7241_2007.html

Berent, A. (n.d.). Advanced Encryption Standard by Example. Retrieved December 4, 2016, from http://www.adamberent.com/documents/AESbyExample.htm

Daemen, J., & Rijmen, V. (2002). *The Design of RijndaeL: AES - The Advanced Encryption Standard* [PDF]. Springer.

Hamsah, M. (2011). PEMBUATAN APLIKASI SECURE E-BOOK UNTUK KARYA ILMIAH PENS-ITS. *PEMBUATAN APLIKASI SECURE E-BOOK UNTUK KARYA ILMIAH PENS-ITS*. Retrieved December 20, 2016, from https://www.pens.ac.id/uploadta/abstrakdetail.php?id=1588

Ilyas, I. A., & Widodo, S. (2014). KRIPTOGRAFI FILE MENGGUNAKAN METODE AES DUAL PASSWORD. *Prosiding KOMMIT*. Retrieved December 20, 2016, from http://ejournal.gunadarma.ac.id/index.php/kommit/article/view/1041

Kretzschmar, U. (2009). *AES128 – A C Implementation for Encryption and Decryption* (Rep.).

Lusiana, V. (2011). IMPLEMENTASI KRIPTOGRAFI PADA FILE DOKUMEN MENGGUNAKAN ALGORITMA AES-128. *Jurnal Dinamika Informatika*, *3*(2). Retrieved from http://www.unisbank.ac.id/ojs/index.php/fti2/article/view/1313

Maffeis, S. (1998). Client/Server Term Definition. In Encyclopedia of Computer Science.

Moser, J. (2009, September 22). A Stick Figure Guide to the Advanced Encryption Standard. Retrieved December 4, 2016, from http://www.moserware.com/2009/09/stick-figure-guide-to-advanced.html

N. (2001). *Federal Information Processing Standards Publication 197* (Publication No. 197). National Institute of Standards and Technology.

Paar, C., & Pelzl, J. (2010). *Understanding Cryptography* (1st ed.) [PDF]. Springer.

Zabala, E. (n.d.). Rijndael Cipher [Cartoon]. In *Http://www.formaestudio.com/rijndaelinspector/archivos/Rijndael_Animation_v4_eng.swf*. Retrieved December 4, 2016, from http://www.formaestudio.com/rijndaelinspector/archivos/Rijndael_Animation_v4_eng.swf