Hak cipta dan penggunaan kembali:

Lisensi ini mengizinkan setiap orang untuk menggubah, memperbaiki, dan membuat ciptaan turunan bukan untuk kepentingan komersial, selama anda mencantumkan nama penulis dan melisensikan ciptaan turunan dengan syarat yang serupa dengan ciptaan asli.

Copyright and reuse:

This license lets you remix, tweak, and build upon work non-commercially, as long as you credit the origin creator and license it on your new creations under the identical terms.

Team project ©2017
Dony Pratidana S. Hum | Bima Agus Setyawan S. IIP

IMPLEMENTASI ALGORITMA AES-128 PADA APLIKASI BROADCASTME MENGGUNAKAN TEKNOLOGI IBEACON BERBASIS IOS

SKRIPSI

Diajukan sebagai salah satu syarat untuk memperoleh gelar

Sarjana Komputer (S. Kom.)

Oleh:

Hary Sutanto

11110110089

PROGRAM STUDI TEKNIK INFORMATIKA

FAKULTAS TEKNOLOGI INFORMASI DAN KOMUNIKASI

UNIVERSITAS MULTIMEDIA NUSANTARA

TANGERANG

2015

LEMBAR PENGESAHAN SKRIPSI

IMPLEMENTASI ALGORITMA AES-128 PADA APLIKASI BROADCASTME MENGGUNAKAN TEKNOLOGI IBEACON BERBASIS IOS

Oleh

Nama	: Hary Sutanto
NIM	: 11110110089
Fakultas	: Teknologi Informasi dan Komunikasi
Program Studi	: Teknik Informatika

Tangerang, 18 Februari 2015

Ketua Sidang

Seng Hansun, S.Si., M.Cs.

Dosen Penguji

Nanang Krisdianto, S.T., M.Kom.

Dosen Pembimbing I,

Dodick Z. Sudirman, S.Kom., M.T.I.

Mengetahui,

Maria Irmina Prasetiyowati, S.Kom., M.T.
Ketua Program Studi Teknik Informatika

PERNYATAAN TIDAK MELAKUKAN PLAGIAT

Dengan ini, saya

Nama	: Hary Sutanto
NIM	: 11110110089
Fakultas	: Teknologi Informasi dan Komunikasi
Program Studi	: Teknik Informatika

menyatakan bahwa skripsi yang berjudul *"Implementasi Algoritma AES-128 pada Aplikasi BroadcastMe Menggunakan Teknologi iBeacon Berbasis iOS"* ini adalah karya ilmiah buatan saya sendiri, bukan plagiat dari karya ilmiah yang ditulis oleh orang lain atau lembaga lain, dan semua karya ilmiah orang lain atau lembaga lain yang dirujuk dalam skripsi ini telah disebutkan sumber kutipannya serta dicantumkan di dalam Daftar Pustaka.

Jika di kemudian hari terbukti ditemukan kecurangan/ penyimpangan, baik dalam pelaksanaan skripsi maupun dalam penulisan laporan skripsi, saya bersedia menerima konsekuensi dinyatakan TIDAK LULUS untuk mata kuliah Skripsi yang telah saya tempuh.

Tangerang, 27 Januari 2015

Hary Sutanto

KATA PENGANTAR

Puji syukur penulis panjatkan kepada Tuhan Yang Maha Esa, karena berkat Anugerah dan Rahmat-Nya lah, penulis dapat menyelesaikan laporan skripsi ini, yang dimana laporan ini menjadi syarat mutlak untuk memperoleh gelar Sarjana Komputer (S.Kom.) di Universitas Multimedia Nusantara. Dalam mengerjakan tugas skripsi ini, penulis mendapatkan bantuan serta dukungan dari berbagai pihak. Pada kesempatan ini penulis memberikan ucapan terima kasih kepada pihak-pihak yang telah membantu dan mendukung penulis, yaitu:

1. Dr. Ninok Leksono, Rektor Universitas Multimedia Nusantara, yang memberi inspirasi bagi penulis untuk berprestasi.
2. Maria Irmina Prasetiyowati, S.Kom., M.T., Ketua Program Studi Teknik Informatika Universitas Multimedia Nusantara, yang menerima penulis dengan baik untuk berkonsultasi dan selalu memotivasi untuk maju.
3. Dodick Z. Sudirman, S.Kom., M.T.I., yang membimbing pembuatan skripsi dan telah mengajar penulis tata cara menulis karya ilmiah dengan benar.
4. Erlan Arief, Verawati, Herlina Sutanti, serta anggota keluarga lainnya yang tak henti-henti memberikan dukungan serta memfasilitasi segala kebutuhan penulis dalam pengerjaan tugas ini.
5. F.X. Syahasta A.T., Rendy Halim, Theoshimi Narada, dan seluruh teman-teman penulis yang selalu memberikan dukungan, masukan dan bantuan selama pengerjaan tugas skripsi ini.

Implementasi Algoritma ..., Hary Sutanto, FTI UMN, 2015

Semoga skripsi ini dapat bermanfaat, baik sebagai sumber informasi maupun sumber inspirasi bagi para pembaca.

Tangerang, 27 Januari 2015

Hary Sutanto

IMPLEMENTASI ALGORITMA AES-128 PADA APLIKASI BROADCASTME MENGGUNAKAN TEKNOLOGI IBEACON BERBASIS IOS

ABSTRAK

Penelitian ini membahas implementasi algoritma *Advanced Encryption System* (AES) pada aplikasi BroadcastMe yang menggunakan teknologi iBeacon berbasiskan sistem operasi iOS. Tujuan dari implementasi algoritma ini adalah untuk mengamankan informasi atau pesan sebelum di-*broadcast* ke pengguna perangkat iOS lainnya menggunakan iBeacon. Aplikasi juga diuji apakah telah berhasil mengamankan informasi menggunakan aplikasi lainnya, yaitu Wireshark. Penelitian ini melibatkan 32 responden untuk menguji apakah responden berhasil mengirimkan pesan dan menerima pesan menggunakan aplikasi ini. Selain itu, responden juga diminta untuk mengisi kuesioner berdasarkan *Post-Study System Usability Questionnaire* (PSSUQ) untuk mengukur empat kategori yaitu kepuasan secara keseluruhan terhadap aplikasi (OVERALL), kegunaan dari sistem (SYSUSE), kualitas dari informasi yang diberikan (INFOQUAL), dan kualitas antarmuka dari aplikasi (INTERQUAL). Dari penelitian didapatkan hasil bahwa pesan yang dikirimkan telah berhasil diamankan menggunakan algoritma AES, dan responden merasa cukup puas terhadap OVERALL aplikasi yang dibuat di penelitian ini.

Kata Kunci: AES, *broadcast*, enkripsi, iBeacon, iOS, kriptografi

IMPLEMENTATION OF AES-128 ALGORITHM IN BROADCASTME USING IBEACON TECHNOLOGY BASED ON IOS

ABSTRACT

This research discusses the implementation of the Advanced Encryption System (AES) in BroadcastMe app which uses iBeacon technology on iOS operating system. The goal of this research is to secure the message before being sent to other iOS devices using iBeacon. BroadcastMe app was tested using another application named Wireshark to ensure that the message is secured. This research involved 32 respondents to test whether they can send the message and receive the message using this app. Respondents also were asked to fill a questionnaire based on Post-Study System Usability Questionnaire (PSSUQ) to measure four categories which are overall summarative (OVERALL), system usefulness (SYSUSE), information quality (INFOQUAL), and interface quality (INTERQUAL). The results of this research are that the message has been successfully secured using the AES algorithm, and the respondents rate that they are satisfied enough for the OVERALL of the app.

Keyword: AES, broadcast, cryptography, encryption, iBeacon, iOS

DAFTAR ISI

LEMBAR PENGESAHAN SKRIPSI ..... **ii**
LEMBAR PERNYATAAN TIDAK MELAKUKAN PLAGIAT ..... **iii**
KATA PENGANTAR ..... **iv**
ABSTRAK ..... **vi**
ABSTRACT ..... **vii**
DAFTAR ISI ..... **viii**
DAFTAR GAMBAR ..... **x**
DAFTAR TABEL ..... **xii**
DAFTAR LAMPIRAN ..... **xiii**
BAB I PENDAHULUAN **1**
1.1. Latar Belakang Masalah 1
1.2. Rumusan Masalah 3
1.3. Batasan Masalah 3
1.4. Tujuan Penelitian 4
1.5. Manfaat Penelitian 4
1.6. Sistematika Penulisan Laporan Penelitian 4
BAB II LANDASAN TEORI **6**
2.1. iOS 6
2.1.1. Cocoa Touch Layer 7
2.1.2. Media Layer 8
2.1.3. Core Services Layer 8
2.1.4. Core OS Layer 9
2.2. Advanced Encryption Standard (AES) 9
2.2.1. Key Expansion 12
2.2.2. Add Round Key 16
2.2.3. Sub Bytes 17
2.2.4. Shift Rows 22
2.2.5. Mix Columns 23
2.2.6. Inverse Shift Rows 27
2.2.7. Inverse Sub Bytes 28

Implementasi Algoritma ..., Hary Sutanto, FTI UMN, 2015

2.2.8. Inverse Mix Columns 29
2.3. iBeacon 29
2.4. Cipher Block Chaining (CBC) 31
2.5. Padding 33
BAB III METODE PENELITIAN DAN PERANCANGAN SISTEM 35
3.1. Metode Penelitian 35
3.2. Perancangan Sistem 36
3.2.1. BroadcastMe 36
3.2.2. Search Beacon 37
3.2.3. CBC Decrypt With AES 128 40
3.2.4. AES 128 Decipher 41
3.2.5. Show Beacon Page 42
3.2.6. CBC Encrypt With AES 128 43
3.2.7. AES 128 Cipher 44
BAB IV IMPLEMENTASI DAN HASIL PENELITIAN 46
4.1. Spesifikasi Sistem 46
4.1.1 Spesifikasi untuk Mengembangkan Sistem 46
4.1.2. Spesifikasi untuk Menguji Sistem 47
4.1.3. Spesifikasi Minimum untuk Menjalankan Sistem 47
4.1.4. Rekomendasi Spesifikasi untuk Menjalankan Sistem 47
4.2. Implementasi Sistem 47
4.3. Pengujian Sistem 51
4.4. Pengumpulan Sampel 53
4.5. Analisis Sampel 54
BAB V SIMPULAN DAN SARAN 55
5.1. Simpulan 55
5.2. Saran 55
DAFTAR PUSTAKA 57

Implementasi Algoritma ..., Hary Sutanto, FTI UMN, 2015

DAFTAR GAMBAR

Gambar 2.1. Pembagian lapisan iOS berdasarkan teknologinya 7
Gambar 2.2. *Pseudocode* untuk enkripsi AES 11
Gambar 2.3. *Key schedule* hasil dari *Key Expansion* 12
Gambar 2.4. *Pseudocode* untuk *Key Expansion* 13
Gambar 2.5. *Rot Word* dan *Sub Word* pada *Key Expansion* 14
Gambar 2.6. Rumus untuk mendapatkan *round constant* 14
Gambar 2.7. Proses untuk mendapatkan *round key* 15
Gambar 2.8. Proses XOR *word* kolom sebelumnya 16
Gambar 2.9. *Tahap Add Round Key* 17
Gambar 2.10. Tabel S-Box versi Rijndael 18
Gambar 2.11. Table *inverse* yang digunakan untuk mendapatkan tabel S-Box ... 19
Gambar 2.12. Contoh *input* untuk perhitungan tabel S-Box 19
Gambar 2.13. *Affine Transformation* dari suatu *byte*. 20
Gambar 2.15. Perkalian antara *input* dengan baris pertama *affine matrix* 21
Gambar 2.16. Hasil perkalian *affine matrix* dengan *input* dalam *binary* 21
Gambar 2.17. Hasil S-Box dari nilai 40 22
Gambar 2.18. Substitusi *bytes* menggunakan S-Box pada tahap Sub Bytes 22
Gambar 2.19. Pergeseran baris pada *state array* di tahap *Shift Rows* 23
Gambar 2.20. Tahap *Mix Columns* pada AES 24
Gambar 2.21. Matriks pengali pada tahap *Mix Columns* 24
Gambar 2.22. *Source code* untuk algoritma perkalian antar elemen matriks 26
Gambar 2.23. *Pseudocode* untuk melakukan dekripsi 27
Gambar 2.24. Pergeseran baris pada tahap *Inverse Shift Rows* 28
Gambar 2.25. Tabel *Inverse* S-Box versi Rijndael 28
Gambar 2.26. Matriks pengali pada tahap *Inverse Mix Columns* 29
Gambar 2.27. Contoh penggunaan UUID, *major*, dan *minor* 31
Gambar 2.28. Penerapan mode operasi CBC untuk enkripsi 32
Gambar 2.29. Penerapan mode operasi CBC untuk dekripsi 32
Gambar 2.30. Enkripsi dan dekripsi menggunakan mode operasi CBC 33
Gambar 2.31. *Padding* menggunakan standar PKCS#7 34

Gambar 3.1. Diagram alir untuk sistem BroadcastMe 37
Gambar 3.2. Diagram alir untuk subproses Search Beacon 39
Gambar 3.3. Diagram alir untuk subproses CBC Decrypt With AES 128 40
Gambar 3.4. Diagram alir untuk subproses AES 128 Decipher 41
Gambar 3.5. Diagram alir untuk subproses Show Beacon Page 42
Gambar 3.6. Diagram alir untuk subproses CBC Encrypt With AES 128 43
Gambar 3.7. Diagram alir untuk subproses AES 128 Cipher 44
Gambar 3.8. Diagram alir untuk subproses Show History Page 45
Gambar 4.1. *Snippet code* untuk melakukan enkripsi 48
Gambar 4.2. *Snippet code* untuk melakukan dekripsi 48
Gambar 4.3. Tampilan sistem saat dijalankan pertama kali 49
Gambar 4.4. Peringatan yang ditampilkan apabila kolom pesan belum terisi 49
Gambar 4.5. Tampilan sistem saat sedang melakukan *broadcast*. 50
Gambar 4.6. Tampilan antarmuka untuk daftar *history*. 50
Gambar 4.7. Tampilan antarmuka saat pengguna memilih *item*. 51
Gambar 4.8. Hasil *packet sniffing* menggunakan Wireshark 52

Implementasi Algoritma ..., Hary Sutanto, FTI UMN, 2015

DAFTAR TABEL

Tabel 2.1. Istilah dalam algoritma AES 10
Tabel 3.1. Struktur dari tabel Beacon Detail 38
Tabel 4.1. Tabel rekapitulasi hasil pengujian *broadcast*.....53
Tabel 4.2. Tabel persebaran nilai dihitung per kategori penilaian 54

Implementasi Algoritma ..., Hary Sutanto, FTI UMN, 2015

DAFTAR LAMPIRAN

1. Formulir Konsultasi Skripsi (*copy*, 1 halaman)
2. Kuesioner (*copy*, 1 rangkap, 3 halaman)
3. Sampel data (1 halaman)

Implementasi Algoritma ..., Hary Sutanto, FTI UMN, 2015