

ABSTRAK

Seiring dengan kebutuhan manusia akan komunikasi yang mudah dan cepat, dibuat sebuah aplikasi *native* pada iOS dan kompatibel terhadap iDevice, yaitu aplikasi *Voice Chat* yang menggunakan *Bluetooth* sebagai jalur transmisi data *peer to peer*, dan menggunakan algoritma enkripsi *AES-256* untuk menjaga integritas data.

Aplikasi *Voice Chat* dibuat pada komputer Macintosh dengan sistem operasi Mac OS X Snow Leopard menggunakan *iOS Software Development Kit* (*iOS SDK*) yang telah disediakan oleh Apple, dan ditulis menggunakan bahasa pemrograman Objective-C. Aplikasi *Voice Chat* mampu menjadi pengganti fitur komunikasi suara jarak dekat pada iDevice tanpa harus mengeluarkan biaya tambahan.

ABSTRACT

As an answer to human's need for a fast and easy communication, a native iOS application is created. The application is a Voice Chat application using Bluetooth as a peer to peer data transmission media, and AES-256 encryption algorithm to protect data integrity.

Voice Chat Application created on a Macintosh Computer with Mac OS X Snow Leopard using iOS Software Development Kit (iOS SDK) and written using Objective-C programming language. This Voice Chat Application is created to provide short range communication service in iDevice with no additional cost.

DAFTAR ISI

KATA PENGANTAR.....	i
ABSTRAK.....	iii
<i>ABSTRACT</i>	iv
DAFTAR ISI.....	v
DAFTAR GAMBAR.....	viii
DAFTAR TABEL.....	ix
BAB I PENDAHULUAN.....	1
1.1. Latar Belakang.....	1
1.2. Identifikasi Masalah.....	2
1.3. Tujuan.....	2
1.4. Pembatasan Masalah.....	2
1.5. Sistematika Pembahasan.....	3
BAB II LANDASAN TEORI.....	5
2.1. Macintosh.....	5
2.2. Mac OS X.....	6
2.3 Aplikasi <i>Native</i>	6
2.4. Sistem Operasi iOS.....	7
2.5. Objective-C.....	7
2.6. <i>iOS Software Development Kit (iOS SDK)</i>	7
2.7. <i>Xcode Developer Tools</i>	8
2.8. <i>GameKit</i>	8
2.9. <i>Voice Chat</i>	9

2.10. <i>Bluetooth</i>	10
2.10.1. Protokol.....	14
2.10.2. Jarak Maksimal Fasilitas <i>Bluetooth</i>	15
2.11. Algoritma Enkripsi <i>AES-256</i>	16
2.11.1. Proses Enkripsi <i>AES</i>	18
2.11.1.1. <i>AddRoundKey</i>	19
2.11.1.2. <i>SubBytes</i>	19
2.11.1.3. <i>Shiftrows</i>	21
2.11.1.4. <i>MixColumns</i>	22
2.11.2. Proses Dekripsi <i>AES</i>	23
2.11.2.1. <i>InvShiftRows</i>	24
2.11.2.1. <i>InvSubBytes</i>	24
2.11.2.3. <i>InvMixColumns</i>	25
BAB III PERANCANGAN DAN IMPLEMENTASI.....	26
3.1. Deskripsi Singkat.....	26
3.2. Visi.....	26
3.3. Blok Diagram.....	28
3.4. Alir Aplikasi.....	29
3.5. <i>Application Delegate</i>	32
3.6. Membuat <i>Project</i> di Xcode.....	33
3.7. Cara Kerja Aplikasi <i>Voice Chat</i>	33
3.8. <i>NSDataAES256</i>	36

BAB IV DATA PENGAMATAN DAN ANALISA DATA.....	37
4.1. <i>Screen Capture</i>	38
4.2. Pengujian algoritma enkripsi dan dekripsi.....	44
BAB V KESIMPULAN DAN SARAN.....	45
5.1. Kesimpulan	45
5.2. Saran.....	46
DAFTAR PUSTAKA.....	47
Lampiran <i>Source Code</i>	A-1

DAFTAR GAMBAR

Gambar 2.1.	<i>Bluetooth Radio Frequency</i>	11
Gambar 2.2.	<i>Wireless Piconet and Frequency Hopping</i>	12
Gambar 2.3.	Proses <i>Input Bytes</i> , <i>State Array</i> , dan <i>Output Bytes</i>	17
Gambar 2.4.	Ilustrasi Proses Enkripsi <i>AES</i>	18
Gambar 2.5.	<i>AddRoundKey</i>	19
Gambar 2.6.	<i>S-Box SubBytes</i>	20
Gambar 2.7.	Pengaruh Pemetaan pada setiap <i>byte</i> dalam <i>state</i>	21
Gambar 2.8.	<i>Transformasi ShiftRows</i>	21
Gambar 2.9.	Ilustrasi Proses Dekripsi <i>AES</i>	23
Gambar 2.10.	<i>Transformasi InvShiftRows</i>	24
Gambar 2.11.	<i>Inverse S-Box SubBytes</i>	25
Gambar 3.1.	<i>Flowchart</i>	30
Gambar 4.1.	<i>Main Screen</i>	38
Gambar 4.2.	<i>Turn On The Bluetooth</i>	39
Gambar 4.3.	<i>Searching</i>	39
Gambar 4.4.	<i>Connecting</i>	40
Gambar 4.5.	<i>Waiting For Response</i>	40
Gambar 4.6.	<i>Feedback</i>	41
Gambar 4.7.	<i>Declined</i>	41
Gambar 4.8.	<i>Disconnected</i>	42

DAFTAR TABEL

Tabel 2.1. Protokol.....	14
Tabel 4.1. iDevice dan iOS yang digunakan untuk pengujian.....	37
Tabel 4.2. Pengujian Hasil Enkripsi dan Dekripsi.....	44