

## DAFTAR ISI

HALAMAN SAMPUL .....	i
HALAMAN PENGESAHAN .....	iii
HALAMAN PERNYATAAN.....	iv
KATA PENGANTAR.....	v
DAFTAR ISI .....	vii
DAFTAR GAMBAR.....	ix
DAFTAR TABEL .....	xi
DAFTAR SINGKATAN .....	xii
INTISARI .....	xiii
ABSTARCT .....	xiv
BAB I PENDAHULUAN .....	15
1.1 Latar Belakang .....	15
1.2 Rumusan Masalah .....	16
1.3 Batasan Masalah.....	17
1.4 Tujuan Penelitian .....	17
1.5 Manfaat Penelitian .....	18
1.6 Sistematika Penulisan .....	18
BAB II TINJAUAN PUSTAKA .....	20
2.1 Konsep <i>Wireless Sensor Network</i> .....	25
2.2 Arduino UNO.....	26
2.3 Sensor <i>Passive Infra Red</i> (PIR) HC-SR501 .....	27
2.4 Xbee S2, Xbee <i>Shield</i> dan <i>Adapter</i> Xbee.....	28
2.5 <i>Protocol</i> ZigBee .....	29
2.5.1 Konsep Protokol Zigbee .....	30
2.6 <i>Software</i> X-CTU .....	31
2.7 <i>Advanced Encryption Standard</i> (AES) .....	31
2.7.1 Konsep Enkripsi <i>Advanced Encryption Standard</i> .....	33
2.8 Hipotesis.....	36
BAB III BAHAN DAN METODE PENELITIAN .....	37

3.1 Bahan.....	37
3.2 Peralatan .....	37
3.3 Prosedur Penelitian.....	40
3.3.1 Metode Penelitian .....	40
3.3.2 Perancangan Alat dan Sistem Pengujian .....	41
3.3.2.1 Perancangan Topologi Xbee S2.....	41
3.3.2.2 Perancangan Topologi Keamanan Enkripsi AES .....	43
3.3.2.3 Konfigurasi Arduino UNO .....	45
3.3.2.4 Konfigurasi Xbee S2 di XCTU .....	47
3.3.2.5 Konfigurasi Server <i>Wireless Sensor Network</i> .....	48
3.3.2.6 Konfigurasi <i>Grafics User Interface</i> .....	51
3.4 Pengujian Hipotesis Penelitian.....	52
3.4.1 Proses Pengiriman Informasi di Perangkat <i>Wireless Sensor Network</i> .....	52
3.4.2 Proses dan Penggunaan Enkripsi AES 128 bit .....	53
BAB IV ANALISA HASIL DAN PEMBAHASAN .....	57
4.1 Pengujian Kinerja Sensor PIR dalam Konsep WSN.....	57
4.2 Proses Algoritme Enkripsi dan Dekripsi AES 128 bit di Arduino UNO.....	61
4.2.1 Proses Enkripsi AES 128 bit .....	63
4.2.2 Proses Dekripsi AES 128 bit .....	67
4.3 Proses Simulasi Enkripsi dan Dekripsi AES 128 bit Data Sensor PIR.....	71
4.4 Proses Algoritme <i>Encode</i> dan <i>Decode</i> Base64 .....	76
4.5 Analisis Uji Enkripsi AES 128 bit dan Pengaruh Penerapan AES .....	77
BAB V PENUTUP .....	78
5.1 Kesimpulan .....	78
5.2 Saran.....	78
DAFTAR PUSTAKA.....	79
LAMPIRAN .....	81

## DAFTAR GAMBAR

Gambar 2. 1 Diagram <i>Home Security System</i> (Suresh.S, 2016).....	20
Gambar 2. 2 AES <i>Encryption Block</i> Diagram (Nasser, 2016) .....	21
Gambar 2.3 AES <i>Algorithm</i> (Panda, 2015) .....	22
Gambar 2. 4 Proses Enkripsi dan Dekripsi AES (Gupta, 2013).....	23
Gambar 2. 5 Arsitektur <i>Wireless Sensor Network</i> (Sumaryono, 2012).....	26
Gambar 2. 6 Arduino UNO (Arduino.cc, 2017).....	27
Gambar 2. 7 Sensor PIR ( <i>Passive Infra Red Receiver</i> ). .....	28
Gambar 2. 8 Perangkat Xbee S2 (Ling, 2015). .....	28
Gambar 2. 9 Shield Xbee S2 (Ling, 2015). .....	29
Gambar 2. 10 Adapter Xbee S2 (Ling, 2015).....	29
Gambar 2. 11 Arsitektur Protokol Zigbee .....	30
Gambar 2. 12 <i>Software DIGI XCTU</i> (Ling, 2015).....	31
Gambar 2. 13 S-AES <i>Encryption dan Decryption</i> (Stallings, 2016).....	34
Gambar 3. 1 Bagan Alir Metode Penelitian .....	40
Gambar 3. 2 Perancangan Topologi Jaringan Xbee S2 .....	41
Gambar 3. 3 Bagan Alir Sensor PIR .....	42
Gambar 3. 4 Perancangan Topologi Keamanan Enkripsi AES .....	43
Gambar 3. 5 Bagan Alir Algoritme AES pada Sistem <i>Smart Home Security</i> .....	45
Gambar 3. 6 Konfigurasi Arduino UNO .....	46
Gambar 3. 7 konfigurasi Xbee S2 <i>Coordinator</i> .....	47
Gambar 3. 8 konfigurasi Xbee S2 Router AT .....	48
Gambar 3. 9 Konfigurasi Apache Web Server .....	49
Gambar 3. 10 Konfigurasi <i>Database MySQL</i> .....	50
Gambar 3. 11 Konfigurasi Python <i>Serial Port</i> USB.....	51
Gambar 3. 12 Konfigurasi GUI <i>Web</i> .....	52
Gambar 3. 13 Alur Simulasi Pengiriman Data Kondisi Rumah Secara <i>Real Time</i> .....	53
Gambar 3. 14 Alur Proses Enkripsi AES 128 bit dan <i>Encode</i> Base64.....	55
Gambar 3. 15 Alur Simulasi Pengiriman Data ke Pengguna dengan AES 128 bit .....	56
Gambar 4. 1 Hasil Topologi Xbee S2.....	57
Gambar 4. 2 Skema Pengujian Sensor PIR .....	58
Gambar 4. 3 Hasil Pengujian Radio <i>Range Test</i> Xbee S2.....	60

Gambar 4. 4 Diagram Algoritme Simetri .....	61
Gambar 4. 5 Skema Enkripsi dan Dekripsi dengan Mode Operasi ECB .....	62
Gambar 4. 6 Diagram Proses Enkripsi .....	63
Gambar 4. 7 Proses Standar <i>Round</i> AES.....	64
Gambar 4. 8 Ilustrasi Proses Transformasi <i>SubBytes</i> .....	65
Gambar 4. 9 Ilustrasi Proses Transformasi <i>ShiftRow</i> .....	66
Gambar 4. 10 Ilustrasi Proses Transformasi <i>MixColom</i> .....	66
Gambar 4. 11 Ilustrasi Proses Transformasi <i>AddRoundKey</i> .....	67
Gambar 4. 12 Diagram Proses Dekripsi .....	68
Gambar 4. 13 Ilustrasi Proses Dekripsi AES 128 bit 10 <i>Round</i> .....	69
Gambar 4. 14 Proses Konversi ke Array, <i>Hexadecimal</i> dan Binary .....	71
Gambar 4. 15 Proses <i>AddRoundKey</i> .....	72
Gambar 4. 16 Proses <i>SubByte</i> dengan S-Box AES .....	72
Gambar 4. 17 Proses <i>ShiftRow</i> .....	72
Gambar 4. 18 Proses <i>MixColumn</i> .....	73
Gambar 4. 19 Proses Pertama <i>AddRoundKey</i> dan <i>ExpantionKey</i> .....	74
Gambar 4. 20 Proses Kedua <i>AddRoundKey</i> dan <i>ExpantionKey</i> .....	75

## DAFTAR TABEL

Tabel 2. 1 Ringkasan Uraian Penelitian .....	24
Tabel 2. 2 Perbandingan Jumlah <i>Round</i> dan <i>Key</i> (Ariyus, 2006). ....	32
Tabel 3. 1 Spesifikasi Server <i>Wireless Sensor Network</i> .....	37
Tabel 3. 2 Spesifikasi <i>Board</i> Arduino UNO .....	38
Tabel 3. 3 Spesifikasi Sensor PIR HC-SR510.....	38
Tabel 3. 4 Spesifikasi <i>Module</i> Xbee S2.....	39
Tabel 3. 5 Struktur Tabel <i>Database</i> MySQL .....	50
Tabel 3. 6 Macam Algoritme Kriptografi Simetri (Munir, 2004) .....	54
Tabel 4. 1 Hasil pengujian Jarak Jangkauan Sensor PIR .....	59
Tabel 4. 2 Hasil Pengujian Sudut Jangkauan Sensor PIR .....	59
Tabel 4. 3 Data Pesan yang Akan dienkripsi AES 128 bit .....	63
Tabel 4. 4 <i>Rounds</i> dan <i>Key Length</i> (bytes) .....	64
Tabel 4. 5 Substitusi S-box AES (Stallings, 2016) .....	65
Tabel 4. 6 Matriks Publik <i>Keys</i> untuk Enkripsi Data <i>MixColumns</i> .....	66
Tabel 4. 7 Substitusi <i>Inverse</i> S-box AES (Stallings, 2016) .....	69
Tabel 4. 8 Matriks <i>Publik Keys</i> untuk Dekripsi Data <i>MixColumns</i> .....	70
Tabel 4. 9 Data <i>Plaintext</i> dan <i>Cipherkey</i> .....	71
Tabel 4. 10 Hasil Enkripsi AES 128 bit .....	76
Tabel 4. 11 Proses Hasil <i>encode</i> Base64 .....	77
Tabel 4. 12 Hasil Penerapan Enkripsi dan Dekripsi AES 128 bit .....	77

## DAFTAR SINGKATAN

AES	: <i>Advanced Encryption Standard</i>
ASCII	: <i>American Standard Code for Information Interchange</i>
API	: <i>Application Programming Interface</i>
CBC	: <i>Cipher Block Chaining</i>
CFB	: <i>Cipher Feedback</i>
CCTV	: <i>Closed-Circuit Television</i>
DES	: <i>Data Encryption Standard</i>
ECB	: <i>Electronic Code Book</i>
FTDI USB	: <i>Future Technology Devices International Universal Serial Bus</i>
GHz	: <i>Gigahertz</i>
GSM	: <i>Group Special Mobile</i>
ICSP	: <i>Called In-Circuit Serial Programming</i>
IEEE	: <i>Institute of Electrical and Electronics Engineers</i>
IDE	: <i>Integrated Development Environment</i>
IoT	: <i>Internet of Thing</i>
MIC	: <i>Message Integrity Checks</i>
OSI layer	: <i>Open System Interconnection Layer</i>
OFB	: <i>Output Feedback</i>
PHP/HTML	: <i>Personal Home Page/Hyper Text Markup Language</i>
PWM	: <i>Pulse-Width Modulation</i>
RSSI	: <i>Received Signal Strength Indicator</i>
PIR	: <i>Sensor Passive Infra Red</i>
OS	: <i>Sistem Operasi</i>
TB	: <i>Tera Byte</i>
WSN	: <i>Wireless Sensor Netwok</i>