

**ANALISIS PERBANDINGAN ALGORITMA TEMPORAL KEY INTEGRITY
PROTOCOL (TKIP) DENGAN ADVANCED ENCRYPTION
STANDARD (AES) PADA ENKRIPSI WI-FI
PROTECTED ACCESS (WPA)**

SKRIPSI



disusun oleh

Muhammad Aryanto

17.11.1311

**PROGRAM SARJANA
PROGRAM STUDI SISTEM INFORMASI
FAKULTAS ILMU KOMPUTER
UNIVERSITAS AMIKOM YOGYAKARTA
YOGYAKARTA**

2021

**ANALISIS PERBANDINGAN ALGORITMA TEMPORAL KEY
INTEGRITY PROTOCOL (TKIP) DENGAN ADVANCED
ENCRYPTION STANDARD (AES) PADA ENKRIPSI WI-FI
PROTECTED ACCESS (WPA)**

SKRIPSI

untuk memenuhi sebagian persyaratan
mencapai gelar Sarjana
pada Program Studi Informatika



disusun oleh

Muhammad Aryanto

17.11.1311

**PROGRAM SARJANA
PROGRAM STUDI SISTEM INFORMASI
FAKULTAS ILMU KOMPUTER
UNIVERSITAS AMIKOM YOGYAKARTA
YOGYAKARTA
2021**

PERSETUJUAN

SKRIPSI

**ANALISIS PERBANDINGAN ALGORITMA TEMPORAL KEY INTEGRITY
PROTOCOL (TKIP) DENGAN ADVANCED ENCRYPTION
STANDARD (AES) PADA ENKRIPSI WI-FI
PROTECTED ACCESS (WPA)**

yang dipersiapkan dan disusun oleh

Muhammad Aryanto

17.11.1311

telah disetujui oleh Dosen Pembimbing Skripsi
pada tanggal 29 Desember 2020

Dosen Pembimbing,

Nila Feby Pristitasari, S.Kom, M.Cs

NIK. 190302161

PENGESAHAN

SKRIPSI

**ANALISIS PERBANDINGAN ALGORITMA TEMPORAL KEY INTEGRITY
PROTOCOL (TKIP) DENGAN ADVANCED ENCRYPTION
STANDARD (AES) PADA ENKRIPSI WI-FI
PROTECTED ACCESS (WPA)**

yang dipersiapkan dan disusun oleh

Muhammad Aryanto

17.11.1311

telah dipertahankan di depan Dewan Penguji
pada tanggal 18 November 2021

Susunan Dewan Penguji

Nama Penguji

Mardhiva Havaty, S.T., M.Kom

NIK. 190302108

Mulla Sullstivono, M.Kom

NIK. 190302248

Nila Feby Puspitasari, S.Kom, M.Cs

NIK. 190302161

Tanda Tangan

Skripsi ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Sarjana Komputer
Tanggal 18 November 2021

DEKAN FAKULTAS ILMU KOMPUTER

Hanif Al Fatta S.Kom, M.Kom

NIK. 190302096

PERNYATAAN

Saya yang bertandatangan dibawah ini menyatakan bahwa, skripsi ini merupakan karya saya sendiri (ASLI), dan isi dalam skripsi ini tidak terdapat karya yang pernah diajukan oleh orang lain untuk memperoleh gelar akademis di suatu institusi pendidikan tinggi manapun, dan sepanjang pengetahuan saya juga tidak terdapat karya atau pendapat yang pernah ditulis dan/atau diterbitkan oleh orang lain, kecuali yang secara tertulis diacu dalam naskah ini dan disebutkan dalam daftar pustaka.

Segala sesuatu yang terkait dengan naskah dan karya yang telah dibuat adalah menjadi tanggung jawab saya pribadi.

Yogyakarta,



Muhammad Aryanto

NIM. 17.11.1311

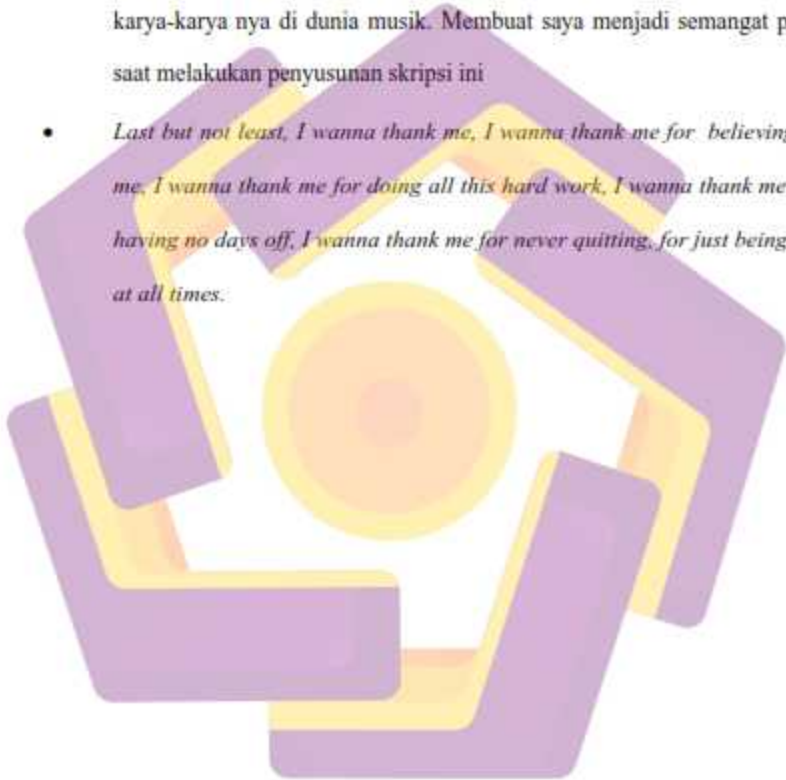
MOTTO

- ❖ Segala sesuatu diawali dengan mengucapkan “Bismillah” kemudian diakhiri dengan “Alhamdulillah”
- ❖ Berusaha, bekerja, berdoa, bersyukur
- ❖ Bawalah Allah SWT didalam hatimu maka hidupmu akan terasa nyaman
- ❖ Bersabarlah karena Allah SWT mempunyai rencana yang jauh lebih indah daripada apa yang kamu rencanakan
- ❖ Sampaikanlah dariku, meskipun satu ayat (HR. Bukhori no.3461)
- ❖ Jangan pedulikan omongan orang lain, karena belum tentu ia paham dengan kondisimu saat ini
- ❖ Jagalah ucapanmu ketika bertemu orang yang lebih tua darimu dan dengarkanlah dengan baik dari orang yang lebih muda darimu
- ❖ Sekali kamu pilih dengan tujuanmu maka janganlah merasa lelah untuk menggapainya
- ❖ Jadilah orang yang bertanggung-jawab dengan apa yang telah kamu perbuat
- ❖ Jangan berhenti ketika kamu merasa lelah. Berhenti lah ketika kamu sudah menyelesaikannya
- ❖ Doakan orang tuamu, saudaramu, temanmu, gurumu, karena kita tidak tahu apa yang akan terjadi di masa yang akan datang
- ❖ Apa yang kamu tanam itulah yang kamu dapat
- ❖ Kita tidak akan tahu hasilnya kalau kita tidak mencoba terlebih dahulu

PERSEMBAHAN

- Puja dan puji syukur penulis ucapkan kepada Allah SWT berkat rahmat serta hidayah nya penulis dapat menyelesaikan penelitian ini. Sholawat serta salam penulis ucapkan kepada Rasulullah SAW beserta keluarga nya dan juga para sahabat nya.
- Skripsi ini saya persembahkan untuk orang tua saya, keluarga saya, keluarga besar saya, kerabat terdekat saya, karena atas doa-doa mereka penelitian ini dapat terselesaikan dengan baik
- Skripsi ini saya persembahkan juga untuk Alm. Kakek serta nenek saya dan juga buyut saya yang saya yakin mereka bangga mempunyai cucu seperti saya yang dapat menyelesaikan skripsi ini untuk mendapatkan gelar sarjana
- Terima kasih saya ucapkan kepada Ibu Nila Feby Puspitasari, S.Kom, M.Cs selaku dosen pembimbing saya sehingga dapat menyelesaikan skripsi ini
- Terima kasih untuk kakak saya tercinta Fitri Lutfi Anjar Sari S.E yang super sabar membantu adik nya dalam menyelesaikan skripsi ini
- Terima kasih untuk teman-teman saya mas tedi susanto, yusuf yao, mas Taufik indardi, dimas dn, aditia ferdiansyah dan Jayanto Squad yang turut berkontribusi dalam menyelesaikan skripsi ini.
- Terima kasih juga untuk pacar saya tercinta yang super duper galak, dan cerewet yang selalu menyemangati saya untuk segera menyelesaikan skripsi ini.

- Terima kasih untuk teman-teman S1 Informatika 06 angkatan 17 yang telah membantu dan juga menginspirasi selama perkuliahan reguler berlangsung. Senang bisa berkenalan dengan kalian.
- Terima kasih kepada Vita Alvia, Syahiba Saufa, Happy Asmara, berkat karya-karya nya di dunia musik. Membuat saya menjadi semangat pada saat melakukan penyusunan skripsi ini
- *Last but not least, I wanna thank me, I wanna thank me for believing in me, I wanna thank me for doing all this hard work, I wanna thank me for having no days off, I wanna thank me for never quitting, for just being me at all times.*



KATA PENGANTAR

Puji serta syukur atas kehadiran Allah SWT atas limpahan Rahmat dan Karunia-nya, sholawat serta salam saya ucapkan atas Rasulullah SAW beserta keluarga nya dan juga para sahabat nya. Sehingga penulis dapat menyelesaikan skripsi ini dengan judul : “Analisa Perbandingan Algoritma TKIP dan Algoritma AES pada WPA”.

Tujuan penulisan skripsi ini untuk memenuhi salah satu syarat untuk menyelesaikan studi serta memperoleh gelar Sarjana Komputer (S.Kom) pada Program Studi Informatika Fakultas Ilmu Komputer Universitas Amikom Yogyakarta. Saya menyadari bahwa penelitian saya masih jauh dari kesempurnaan oleh sebab itu penulis mengharapkan kritikan dan saran yang bersifat membangun untuk membuat penelitian ini menjadi lebih baik lagi.

Terselesaikannya skripsi ini tidak terlepas dari bantuan banyak pihak sehingga dengan rendah hati dan sangat hormat dari penulis ingin menyampaikan rasa terima kasih yang sebesar-besarnya bagi semua pihak yang sudah turut membantu atas tercapainya penyusunan skripsi ini, terlebih ucapan terima kasih saya sampaikan kepada yang saya hormati :

1. Kedua orang tua saya Bapak Salim dan Ibu Sumarmi Lutfi Anjar Sari yang tiada henti memberikan kasih sayang yang tulus, pengorbanan beliau yang luar biasa, doa-doa yang tidak pernah berhenti, dan juga harapan yang mereka beri dipundak penulis untuk menaikkan derajat keluarga.

2. Kakak saya tercinta Fitri Lutfi Anjar Sari S.E yang selalu mensupport, membantu, dan juga mendoakan sehingga penulis dapat menyelesaikan skripsi ini
3. Bapak Prof. Dr.M.Suyanto,MM. selaku Rektor Universitas Amikom Yogyakarta
4. Bapak Hanif Al Fatta, S.kom, M.Kom. selaku Dekan Fakultas Ilmu Komputer Universitas Amikom Yogyakarta
5. Ibu Nila Feby Puspitasari S.kom, M.Cs. selaku Dosen pembimbing yang telah berkenan meluangkan waktu dan memberikan ilmu serta saran yang tiada henti atas permasalahan yang saya alami dalam penulisan skripsi ini.
6. Seluruh Bapak/Ibu dosen Fakultas Ilmu Komputer yang telah memberikan ilmu dan juga pengetahuan di dunia informatika yang sangat bermanfaat selama masa perkuliahan regular berlangsung.
7. Seluruh teman-teman seangkatan, khusus nya S1 Informatika 06 angkatan 2017 yang telah mengisi hari-hari menjadi lebih menyenangkan karena dapat bertukar pikiran, membagikan pengalaman dan juga berdiskusi untuk satu tujuan

Yogyakarta, November 2021

Penulis



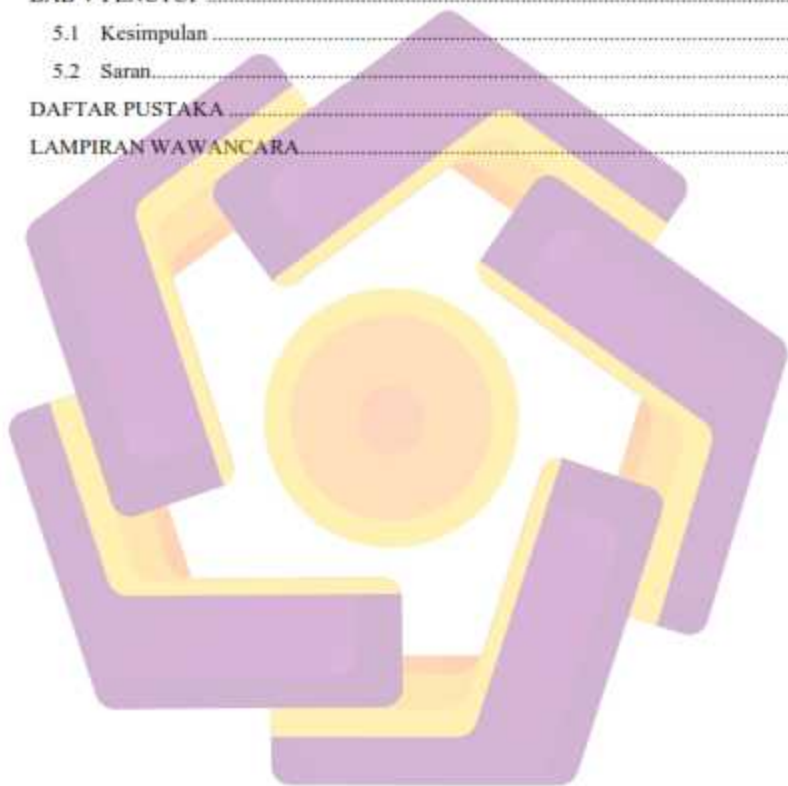
(Muhammad Aryanto)

DAFTAR ISI

JUDUL.....	i
PERSETUJUAN.....	ii
PENGESAHAN.....	iii
PERNYATAAN.....	iv
MOTTO.....	v
PERSEMBAHAN.....	vi
KATA PENGANTAR.....	vii
DAFTAR ISI.....	viii
DAFTAR GAMBAR.....	ix
DAFTAR TABEL.....	x
INTISARI.....	xi
ABSTRACT.....	xii
BAB I PENDAHULUAN.....	1
1.1 Latar Belakang.....	1
1.2 Rumusan Masalah.....	3
1.3 Batasan Masalah.....	3
1.4 Maksud dan Tujuan Penelitian.....	4
1.4.1 Maksud Penelitian.....	4
1.4.2 Tujuan Penelitian.....	4
1.5 Manfaat Penelitian.....	4
1.6 Metodologi Penelitian.....	5
1.6.1 Metode Pengumpulan Data.....	5
1.6.2 Metodologi Security Policy Development Life Cycle (SPDLC).....	5
1.6.2.1 Identifikasi.....	5
1.6.2.2 Analisis.....	5
1.6.2.3 Desain.....	6
1.6.2.4 Implementasi.....	6
1.6.2.5 Audit.....	6
1.6.2.6 Evaluasi.....	6
1.7 Sistematika Penulisan.....	7
BAB II LANDASAN TEORI.....	8

2.1	Kajian Pustaka	8
2.1.1	Tabel Perbandingan Kajian Pustaka	10
2.2	Dasar Teori	12
2.2.1	Wi-Fi	12
2.2.2	Spesifikasi Wi-fi	13
2.2.3	Jenis Keamanan Wi-fi	14
2.3	WPA (Wireless Protected Acces)	15
2.3.1	AES (Advance Encryption System)	16
2.3.2	TKIP (Temporal Key Integrity Protocol)	19
2.4	AIRCRAK	22
2.4.1	FUNGSI AIRCRAK	22
BAB III METODE PENELITIAN		24
3.1	Lokasi Penelitian	24
3.2	Waktu Penelitian	24
3.3	Alat dan Bahan Penelitian	24
3.3.1	Alat	24
3.3.2	Bahan Penelitian	24
3.4	Alur Penelitian	25
3.4.1	Metode Pengumpulan Data	25
3.4.2	Metode Security Policy Development Life Cycle	25
3.4.2.1	Identifikasi	25
3.4.2.2	Analisis Hasil Pengumpulan Data	26
3.4.2.3	Analisis Permasalahan	27
3.4.2.4	Solusi Permasalahan	27
3.4.2.5	Analisa Kebutuhan	28
3.4.2.8	Desain	29
3.5	Perancangan Pengujian Terhadap Algoritma TKIP dan Algoritma AES pada WPA	30
3.5.1	Rancangan aktivitas Serangan	30
BAB IV IMPLEMENTASI DAN PEMBAHASAN		32
4.1	Daftar Perangkat pada Jaringan Wifi	32
4.2	Konfigurasi Router Dengan Algoritma TKIP	33
4.3	Scanning Jaringan Wifi	33
4.4	Hasil Pengujian Algoritma TKIP pada WPA	34

4.5	Konfigurasi Router Dengan Algoritma AES.....	44
4.6	Scanning Jaringan Wifi.....	45
4.7	Hasil Pengujian Algoritma AES pada WPA.....	45
4.8	Hasil Penelitian.....	56
4.8.1	Keamanan.....	56
4.8.2	Performa.....	56
BAB V PENUTUP		57
5.1	Kesimpulan.....	57
5.2	Saran.....	58
DAFTAR PUSTAKA		59
LAMPIRAN WAWANCARA		60



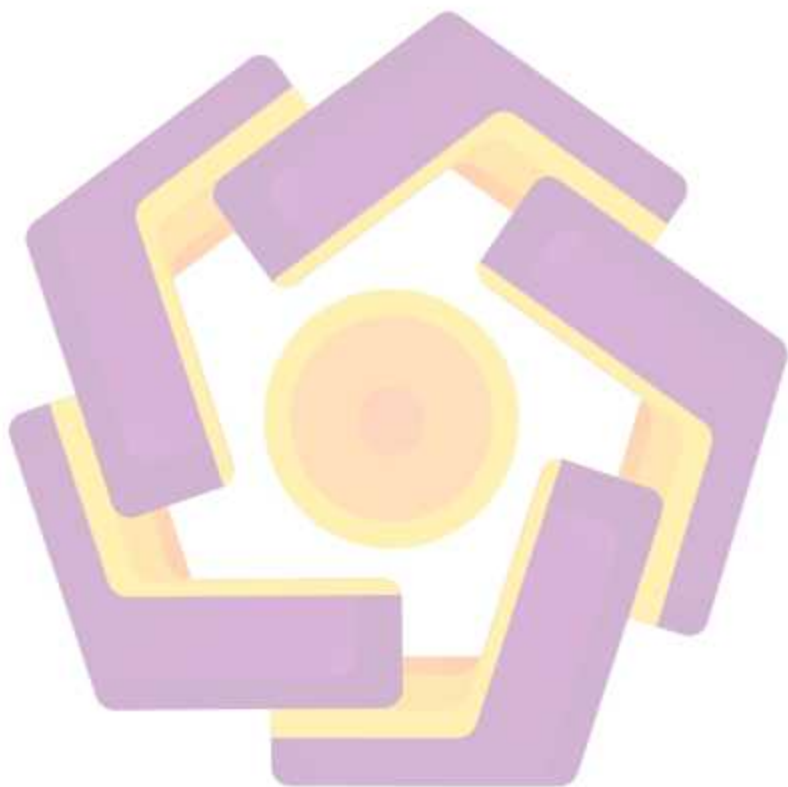
DAFTAR GAMBAR

2.1	JENIS KEAMANAN	15
2.2	ENKRIPSI AES	17
2.3	SUB BYTES	17
2.4	PROSES SUB BYTES	18
2.5	PROSES SHIFT ROWS	18
2.6	MATRIKS MIXCOLUMNS TRANSFORMATION	19
2.7	TRANSFORMASI MIXCOLUMNS	19
2.8	METODE ENKRIPSI RC4	20
2.9	MIC PADA ALGORITMA TKIP	21
2.10	DIV PADA ALGORITMA TKIP	21
2.11	KEY MIXING PADA ALGORITMA TKIP	22
2.12	TAMPILAN AIRCRACK	23
3.1	METODE SPDLC	25
3.2	TOPOLOGI WIRELESS	30
3.3	PENGUJIAN TERHADAP TKIP DAN AES	31
4.1	DAFTAR PERANGKAT PADA JARINGAN WIFI	32
4.2	KONFIGURASI ALGORITMA TKIP	33
4.3	SCANNING JARINGAN WIFI	34
4.4	HASIL PENGUJIAN 1	34
4.5	HASIL PENGUJIAN 2	35
4.6	HASIL PENGUJIAN 3	35
4.7	HASIL PENGUJIAN 4	36
4.8	HASIL PENGUJIAN 5	36
4.9	HASIL PENGUJIAN 6	37
4.10	HASIL PENGUJIAN 7	37
4.11	HASIL PENGUJIAN 8	38
4.12	HASIL PENGUJIAN 9	38
4.13	HASIL PENGUJIAN 10	39
4.14	HASIL PENGUJIAN 11	39
4.15	HASIL PENGUJIAN 12	40
4.16	HASIL PENGUJIAN 13	40
4.17	HASIL PENGUJIAN 14	41

4.18 HASIL PENGUJIAN 15.....	41
4.19 HASIL PENGUJIAN 16.....	42
4.20 HASIL PENGUJIAN 17.....	42
4.21 HASIL PENGUJIAN 18.....	43
4.22 HASIL PENGUJIAN 19.....	43
4.23 HASIL PENGUJIAN 20.....	44
4.24 KONFIGURASI ALGORITMA AES.....	44
4.25 SCANNING JARINGAN WIFI.....	45
4.26 HASIL PENGUJIAN 1.....	46
4.27 HASIL PENGUJIAN 2.....	46
4.28 HASIL PENGUJIAN 3.....	47
4.29 HASIL PENGUJIAN 4.....	47
4.30 HASIL PENGUJIAN 5.....	48
4.31 HASIL PENGUJIAN 6.....	48
4.32 HASIL PENGUJIAN 7.....	49
4.33 HASIL PENGUJIAN 8.....	49
4.34 HASIL PENGUJIAN 9.....	50
4.35 HASIL PENGUJIAN 10.....	50
4.36 HASIL PENGUJIAN 11.....	51
4.37 HASIL PENGUJIAN 12.....	51
4.38 HASIL PENGUJIAN 13.....	52
4.39 HASIL PENGUJIAN 14.....	52
4.40 HASIL PENGUJIAN 15.....	53
4.41 HASIL PENGUJIAN 16.....	53
4.42 HASIL PENGUJIAN 17.....	54
4.43 HASIL PENGUJIAN 18.....	54
4.44 HASIL PENGUJIAN 19.....	55
4.45 HASIL PENGUJIAN 20.....	55

DAFTAR TABEL

2.1	STUDIE LITERATUR	12
2.2	SPESIFIKASI WIFI.....	14
3.1	ANALISA PENGUMPULAN DATA	26
3.2	SPESIFIKASI SOFTWARE.....	28
3.3	SPESIFIKASI HARDWARE.....	29



INTISARI

Pengaruh perkembangan teknologi membuat kebutuhan jaringan internet menjadi sangat penting dikarenakan dengan penggunaan internet masyarakat dapat mencari segala sesuatu informasi yang dibutuhkan. Dalam penggunaan internet pada jaringan wifi membutuhkan mekanisme keamanan jaringan. Keamanan jaringan wifi terdiri dari beberapa jenis, yaitu diantaranya adalah WEP, WPA, WPA2-PSK.

Penelitian ini akan melakukan analisis perbandingan pada algoritma TKIP dan AES yang ada pada jenis keamanan WPA dengan menggunakan metode SPDLC (*Security Policy Development Life Cycle*) Didalam metode SPDLC terdiri dari identifikasi, analisis, desain, implementasi, audit, dan evaluasi. Implementasi yang dilakukan pada penelitian ini menggunakan sebuah tools "Aircrack-ng" sebagai media dalam melakukan penetrasi terhadap jenis keamanan yang akan di uji.

Hasil dari penelitian ini adalah perbandingan yang dilakukan antara algoritma TKIP dan algoritma AES membuktikan bahwa algoritma AES pada WPA lebih unggul dalam mengamankan jaringan. Maka kesimpulan yang dapat diambil pada saat melakukan implementasi perbandingan algoritma TKIP dan AES pada WPA adalah kedua jenis algoritma ini masih dapat dilakukan peretasan.

kata kunci : Internet, WEP, WPA, WPA2-PSK, TKIP, AES, Aircrack-ng

ABSTRACT

The influence of technological developments makes the need for internet networks very important because with the use of the internet people can find all the information needed. In the use of the internet on wifi networks requires a network security mechanism. Wifi network security consists of several types, namely wep, WPA, WPA2-PSK.

This research will conduct comparative analysis on existing TKIP and AES algorithms in wpa security types using the SPDLC (Security Policy Development Life Cycle) method in the SPDLC method consisting of identification, analysis, design, implementation, audit, and evaluation. The implementation carried out in this study uses a tool "Aircrack-ng" as a medium in penetrating the type of security to be tested.

The result of this study is a comparison made between the TKIP algorithm and the AES algorithm proves that the AES algorithm on WPA is superior in securing the network. So the conclusion that can be taken when implementing the comparison of TKIP and AES algorithms on WPA is that these two types of algorithms can still be hacked.

keywords: Internet, WEP, WPA, WPA2-PSK, TKIP,

