BAB II
DASAR TEORI

2.1 Umum

Dengan adanya teknologi *wireless*, komunikasi dan pertukaran informasi tanpa kabel menjadi hal yang mungkin dilakukan. Kebebasan bergerak bagi pengguna bisa diberikan oleh jaringan wireless. Sehingga pengguna bisa melakukan komunikasi atau pertukaran informasi dimanapun selama masih dalam *range* cakupan jaringan.

Teknologi *wireless* (tanpa kabel) yang paling populer adalah teknologi WLAN (*Wireless Local Area Network*). Pada awalnya, terdapat bermacam-macam merek, model, dan cara pembuatan peralatan *wireless*. Banyaknya merek, model dan jenis peralatan *wireless* membuat pengguna kesulitan untuk menentukan standarisasi peralatannya. Oleh karena itu, agar memudahkan pengguna, badan IEEE (*Institute of Electrical and Electronic Engineers*) pada tahun 1997 memberi standar pada WLAN dengan nama *IEEE 802.11*.

WLAN mempunyai tiga standar yang paling banyak digunakan di dunia, yaitu IEEE 802.11a, IEEE 80211b, dan IEEE 802.11g. IEEE 802.11b dan IEEE 802.11g menggunakan frekuensi 2,4 GHz, sedangkan IEEE 802.11a menggunakan frekuensi 5 GHz. Kecepatan transfer data yang dipunyai standar 802.11b adalah 11 Mbps, sedangkan kecepatan yang dipunyai standar 802.11a dan 802.11g mencapai 54 Mbps.

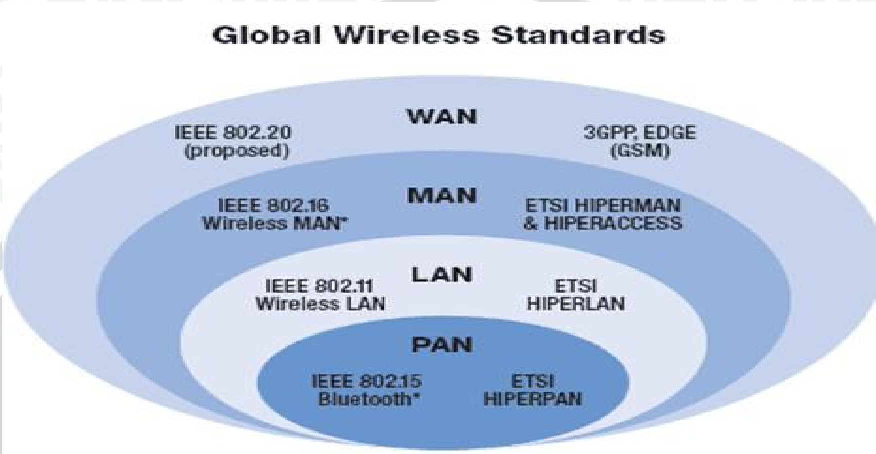
Karena menggunakan udara sebagai media propagasi, *Wireless* LAN berpotensi diakses oleh pengguna yang tidak sah. Hal ini cukup mengganggu pengguna yang lain, dan mengganggu kinerja jaringan secara keseluruhan. Untuk mengatasi ini, IEEE menciptakan metode keamanan WPA-PSK (*Wi-Fi Protected Access-Pre Shared Key*) dan WPA2-PSK (*Wi-Fi Protected Access2-Pre Shared Key*). WPA-PSK menggunakan algoritma RC4 untuk enkripsi data, sedangkan pada WPA2-PSK menggunakan algoritma AES.

2.2 Jenis-jenis Jaringan *Wireless*

Jaringan *wireless* dikelompokkan dalam beberapa kategori menurut *range* cakupan (*coverage*) yang bisa dijangkaunya. Beberapa jenis jaringan wireless menurut cakupan areanya adalah sebagai berikut :

- *Wireless Personal Area Network (WPAN).*
- *Wireless Local Area Network (WLAN).*
- *Wireless Metropolitan Area Network (WMAN).*
- *Wireless Wide Area Network (WWAN).*

Jenis-jenis standar jaringan *wireless* ditunjukkan pada gambar 2.1.



Gambar 2.1 Jenis-jenis standar Jaringan Wireless

[Sumber: *www.rfidc.com*/images/technology_intros/

introductiontowireless_standards_clip_image002.jpg]

Setiap jenis jaringan *wireless* memiliki sifat yang saling melengkapi sesuai kebutuhan pengguna. Jenis-jenis jaringan *wireless* ditunjukkan pada Tabel 2.1.

Tabel 2.1 Jenis-jenis Jaringan Wireless

Jenis	Jangkauan	Performa	Standar	Aplikasi
Wireless PAN	Dalam jangkauan perorangan	Sedang	Bluetooth, IEEE 802.15, IrDA	Menggantikan penggunaan kabel
Wireless LAN	Dalam gedung atau kampus	Tinggi	IEEE 802.11,Wi-Fi,	Perluasan *mobile* pada jaringan berkabel
Wireless MAN	Dalam kota	Tinggi	IEEE 802.16,dan WIMAX	Nirkabel pada perumahan dan tempat-tempat bisnis
Wireless WAN	Seluruh dunia	Rendah	Seluler, 2G, 2.5G,dan 3G	Akses mobile ke internet dari ruang outdoor

[Sumber: Jim Geier, *Wireless Networks First-Step*; 3]

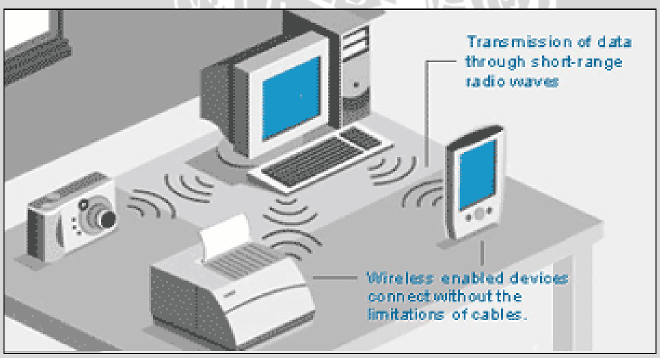
2.2.1 Wireless Personal Area Network (WPAN).

WPAN adalah jenis jaringan *wireless* yang mempunyai *range* cakupan yang terkecil di antara jenis jaringan *wireless* yang lain. *Range* cakupan maksimal yang dapat dijangkau oleh WPAN berkisar 10 sampai 15 meter. Oleh karena cakupannya yang kecil, WPAN hanya efektif untuk memenuhi kebutuhan pengguna dalam ruang yang kecil.

Pada teknologi WPAN digunakan dua jenis media untuk melakukan komunikasi antar perangkat, yaitu gelombang radio dan infra merah (IrDA). Gelombang radio lebih sering digunakan karena batasan jaraknya yang lebih jauh dan fleksibel dibanding infra merah. Untuk komunikasi yang menggunakan infra merah, persyaratan LOS (*Line Of Sight*) harus terpenuhi. LOS (*Line Of Sight*) artinya komunikasi dilakukan tanpa adanya penghalang antar perangkat.

Kelebihan dari infra merah adalah bebas dari interferensi gelombang radio. Infra merah juga memiliki *data rate* yang lebih tinggi dibanding gelombang radio. *Data rate* yang diberikan dengan media transmisi infra merah mencapai 4 Mbps, sedangkan yang dapat diberikan dengan media transmisi gelombang radio mencapai 2 Mbps.

Perangkat keras WPAN yang beredar sekarang sudah dilengkapi dengan kedua jenis media transmisi diatas. Salah satunya adalah telepon seluler yang sudah menggunakan fitur *bluetooth* dan infra merah sebagai media pertukaran data antar sesama pengguna. Implementasi teknologi WPAN ditunjukkan pada gambar *2.2*.



Gambar 2.2 Implementasi *Wireless* PAN

[Sumber:*www.i.dell.com/images/us/segments/dhs/sitelet/lmaWPAN_lg_image.gif*]

Perangkat berteknologi WPAN, seperti *digital camera*, telepon seluler dan *printer* saling berkomunikasi dengan PC (*Personal Computer*) menggunakan teknologi WPAN.

Dari gambar 2.2 diatas, PC (*Personal Computer*) dapat berkomunikasi dengan 3 piranti, yaitu kamera digital, telepon seluler, dan printer. Data bisa saling dipertukarkan diantara 3 piranti tersebut.

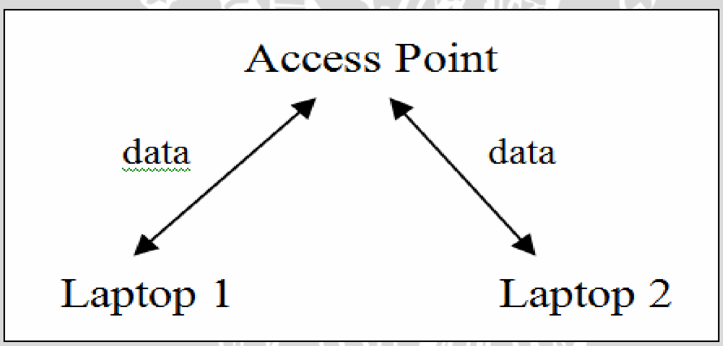
2.2.2 Wireless Local Area Network (WLAN)

Dibandingkan dengan WPAN, WLAN memiliki cakupan area yang lebih luas. Cakupan area yang dapat dijangkau WLAN mencapai 100 m. Dengan demikian, WLAN dapat diimplementasikan untuk membangun jaringan tanpa kabel dalam skala lokal, seperti dalam suatu gedung, kampus, kantor, rumah sakit dan lain-lain.

Seperti pada WPAN, media yang digunakan untuk melakukan komunikasi antar perangkat pada WLAN adalah gelombang radio dan infra merah.

WLAN bekerja dengan dua jenis konfigurasi perangkat, yaitu konfigurasi a*d-hoc* dan konfigurasi *infrastruktur*. Pada konfigurasi a*d-hoc*, komunikasi antara dua atau lebih perangkat *wireless* dilakukan tanpa melalui *access point*. Sedangkan pada konfigurasi *infrastruktur* komunikasi dilakukan melalui *access point*.

Implementasi teknologi WLAN menggunakan konfigurasi *infrastruktur* ditunjukkan pada gambar 2.3.



Gambar 2.3 Implementasi Wireless LAN

[Sumber: *www.itokwrote.files.wordpress.com/2007/08/ networks.jpg*]

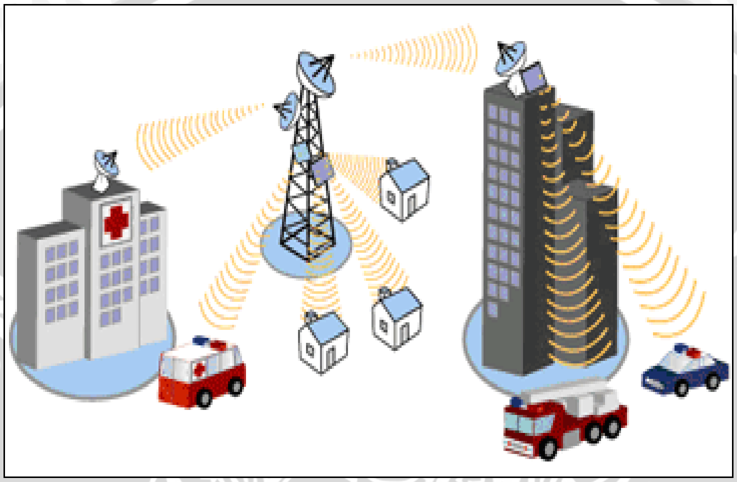
Access point bertindak sebagai pusat jaringan yang terjadi antara dua buah *laptop*. Proses pengiriman data antara dua *laptop* melewati sebuah *access point*.

2.2.3 Wireless Metropolitan Area Network (WMAN)

MAN adalah jaringan tanpa kabel dengan *range* cakupan yang lebih luas dibandingkan WLAN. Koneksi yang disediakan WMAN adalah pada kawasan perkotaan atau antar gedung. Wireless MAN dipakai karena tidak terlalu membutuhkan biaya yang besar jika dibandingkan jaringan melalui kabel tembaga atau melalui kabel serat optik.

Media transmisi yang digunakan pada WMAN sama dengan dua jenis komunikasi *wireless* sebelumnya, yaitu gelombang radio dan infra merah.

Data rate yang diberikan oleh koneksi menggunakan infra merah mencapai 100 Gbps. Sedangkan *data rate* yang dapat diberikan oleh koneksi gelombang radio sebesar 100 Kbps. Implementasi teknologi WMAN ditunjukkan pada gambar 2.4.



Gambar 2.4 Implementasi Wireless MAN

[Sumber: *www.netkrom.com/images/products/diagram_ISPAIR_medium.jpg*]

Menara *base station* yang mengatur komunikasi dengan beberapa *subscriber station*. *Base station* merupakan peralatan *outdoor* berbentuk *tower* yang berfungsi sebagai *transceiver* (*transmitter* dan *receiver*), sedangkan *subscriber station* adalah pengguna layanan WMAN yang berada pada *range* cakupan *base station*.

Pada gambar 2.4 diatas, *base station* menyediakan komunikasi dengan beberapa *subscriber station* berupa sebuah gedung, sebuah rumah sakit, beberapa rumah, dan sebuah mobil *ambulans* yang berada dalam *range* cakupan *base station*. Media transmisi yang digunakan adalah gelombang radio.

2.2.4 Wireless Wide Area Network (WWAN)

Wireless WAN merupakan komunikasi tanpa kabel dengan cakupan area yang sangat luas. Cakupan area yang bisa dijangkau WWAN adalah antar kota, antar negara, bahkan hampir seluruh dunia. *Data rate* maksimal yang bisa ditawarkan oleh WWAN mencapai 170 Kbps.

Pada WWAN, infra merah tidak lagi digunakan sebagai media transmisi, karena persyaratan LOS (*Light of Sight*) akan sangat sulit untuk terpenuhi dalam cakupan wilayah yang sangat luas. Jadi yang digunakan adalah gelombang radio. Implementasi teknologi WMAN ditunjukkan pada gambar 2.5.

Gambar 2.5 Implementasi *Wireless* WAN

[Sumber: *www.hp.com/sbso/images/oov/wireless/WWAN-broadband-how-it-works.gif*]

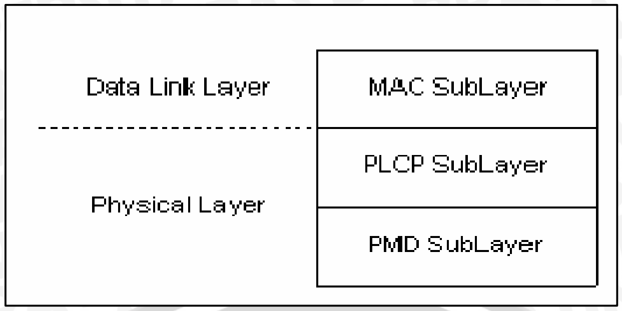
Pada gambar 2.5, dalam suatu wilayah seukuran kota, terdapat sebuah *base station* dan beberapa *repeater* (penguat sinyal) yang berfungsi menguatkan sinyal dari *base station* kepada *subscriber station* agar bisa menjangkau wilayah yang lebih luas.

Base station berguna menghubungkan jaringan internet dengan *subcriber station* dan beberapa *repeater*. *Subscriber station* adalah pengguna yang menggunakan layanan WWAN, yaitu berupa *mobile users* (laptop *Wi-Fi* dan *Wi-Fi phone*), *home users (PC)*, *business users* (PC dan *laptop Wi-Fi*).

Bentuk komunikasi teknologi WWAN mempunyai kesamaan dengan teknologi WPAN, WLAN, maupun WMAN, tetapi mempunyai *range* cakupan jaringan yang lebih luas.

2.3 Layer Protokol Pada WLAN

Layer pada protokol yang digunakan pada standar IEEE 802.11 hanya dua layer yaitu lapisan *physica*l dan *data link*. Lapisan *physical* (PLCP dan PMD *sub layer*) dan *Medium Access Controller* (MAC) pada lapisan *data-link*.



Gambar 2.6 *Layer* pada Wifi 802.11b/g

[Sumber : http://www.cis.ohio-state.edu/~jain/cis788-99/*wireless*_lans/index.html]

Layer terendah kedua dari model OSI (layer 2) adalah *data link layer*. *Data link layer* merupakan fungsi primer dalam teknologi pengkabelan dan W*ireless Local Area Networking* (WLAN).

Lapisan *data link* sendiri memiliki dua sublayer, yaitu LLC (*Logical Link Control*) dan MAC (*Medium Access Control*), tetapi untuk 802.11 hanya memiliki satu sub layer yaitu MAC (*Medium Access Control*)

Secara umum frame 802.11 tersusun dari frame-frame sebagai berikut :

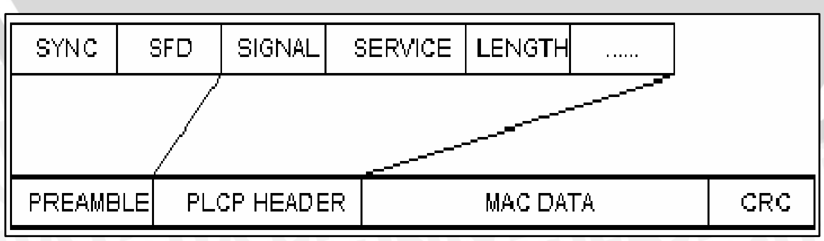
Preamble	PLCP Header	MAC Data	CRC

Gambar 2.7 Bentuk frame 802.11
[Sumber **:** Stallings :chapter 14]

2.3.1 Physical Layer 802.11

2.3.1.1 PLCP Sub Layer

PLCP (*Physical Layer Convergence Protocol*) frame format adalah metode *mapping* dari 802.11 PHY *sub layer Service Data Unit* (PSDU) kedalam format *frame* yang memungkinkan untuk mengirim dan menerima data antar dua perangkat yang menggunakan assosiasi *physical medium dependent system.*



Gambar 2.8 PLCP *frame format* secara umum
Sumber : http://www.cis.ohiostate.edu/~jain/cis788-99/*wireless*_lans/index.html

Format frame dari lapisan fisik (PHY) adalah sebagai berikut :

- Sebuah frame diawali dengan *Field Preamble* (pembukaan), terdiri atas :
  - **SYNC** yang berfungsi untuk sinkronisasi penerimaan sinyal
  - ***Start Frame Delimiter* (SFD)** yang menyatakan permulaan *frame*
- *Field Header*, terdiri atas :
  - ***Signal,*** *field* ini menyatakan kepada lapisan PHY mengenai modulasi yang digunakan dalam pengiriman
  - ***Service,*** *field* ini disediakan untuk penggunaan yang akan datang
  - ***Length,*** *field* ini menyatakan berapa mikro detik waktu yang dibutuhkan untuk mengirimkan *payload* (data bersifat variabel).
  - ***Cyclic Redudancy Check* (CRC),** dalam *field* ini, *field signal, field length* dan *field Service* dikawal oleh *Frame check sequence* untuk memastikan tidak terjadi kesalahan (*error*) dalam *frame.*
- *Field Data Payload.*

  Data payload disebut juga dengan *MAC Protocol Data Unit* (MPDU), merupakan sejumlah unit data atau *frame* MAC yang dikirimkan dari lapisan MAC ke lapisan fisik (PHY). Besarnya dapat bervariasi tergantung besarnya data yang terdapat dalam *frame MAC.*

2.3.1.2 PMD Sub Layer

Physical Media Dependent (PMD), melayani *wireless encoding*, yaitu berfungsi menyediakan metode pengiriman dan penerimaan proses modulasi dan demodulasi dari frame transmisi yang melalui media *wireless. Bit-bit* data diambil dari PLCP *Sub Layer* dan kemudian dimodulasikan dengan teknik DSSS maupun OFDM. Frekuensi *carrier* yang digunakan antara 2.400 sampai 2.483 Ghz frekuensi ini adalah frekuensi bebas jika digunakan untuk bidang industri, pendidikan dan kedokteran atau ISM (*Industry, Scientific, Medical*). Adapun frekuensi itu terdiri dari sebelas kanal frekuensi dengan *guard band* antar kanal sebesar 5 MHz.

2.3.2 Data Link Layer 802.11

2.4.2.1 Lapisan Medium Access Controller (MAC)

Medium Access Controller (MAC) bekerja pada lapisan *data-link* dan berfungsi menjaga validitas lalu-lintas data. Paket data (*payload*) pada frame MAC yang dikirimkan disebut MAC *Protocol Data Unit* (MPDU).

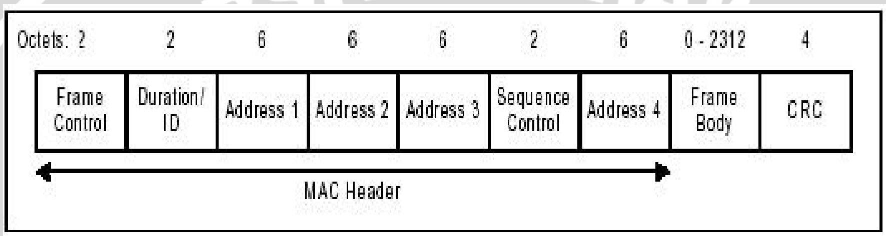
PLCP Preamble	PLCP Header	MAC Header	Frame Payload	FCS
18 *byte*	6 *byte*	30 *byte*	≤2304 *byte*	4 *byte*

MPDU

PPDU

Gambar 2.9 Bentuk Frame dari WiFi 802.11b/g
[**Sumber :** Rohde, 2002: 9]

MAC frame memiliki empat *address* yang terdiri dari : *Basic Service Set Identification* (BSSID), (*Source Address*/SD) atau alamat sumber, (*Recipient Address*/RA) atau alamat tujuan, serta stasiun *transmitter* dan *receiver*



Gambar 2.10 Format Frame MAC
[Sumber : *BreezeCom*, 1997]

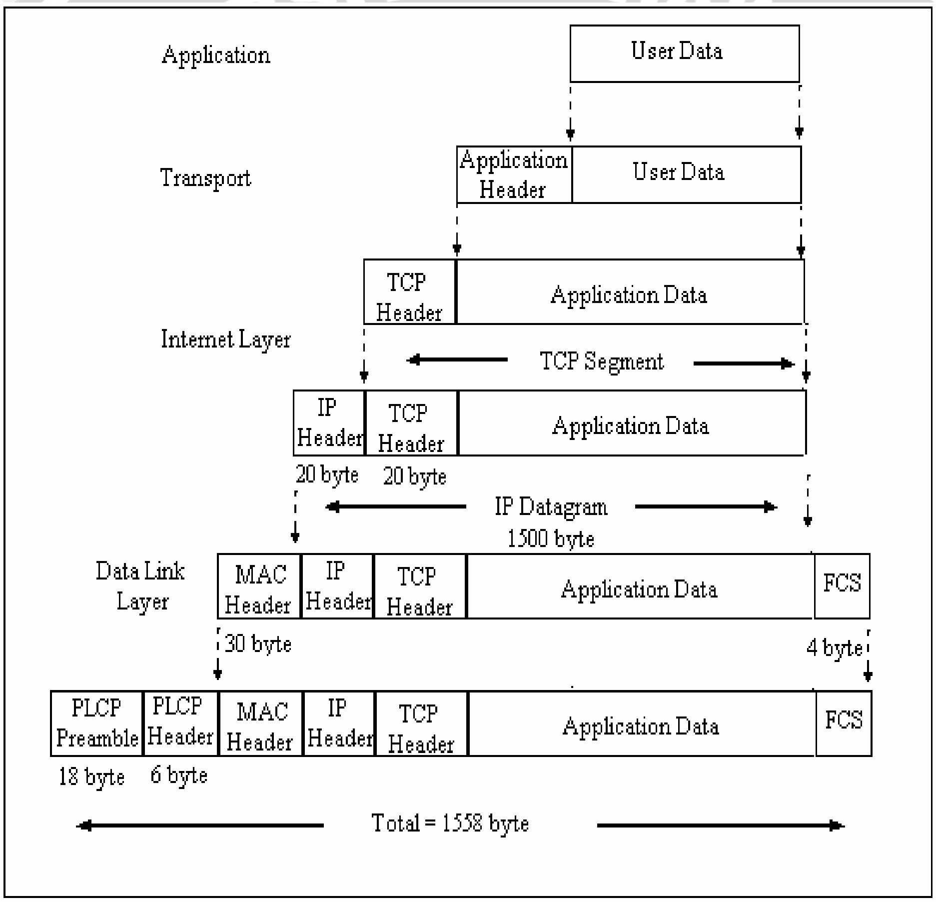
Pada lapisan *Data Link* dari WLAN ini, datagram atau paket data pada IP layer akan ditambahkan MAC *header* 30 *byte* dan *Frame Check Squence* (FCS) 4 byte. Kemudian pada lapisan *Physical* akan ditambahkan PLCP preamble 18 *byte* dan PLCP header 6 *byte*. Sedangkan ukuran paket MPDU sebesar 1500 *byte*. Sehingga total paket sebesar 1558 *byte* atau 12464 *bit*.

2.4 Model OSI dan TCP/IP

Dalam merencanakan suatu jaringan komputer selain membutuhkan perangkat keras juga membutuhkan perangkat lunaknya. Perangkat lunak suatu jaringan komputer ini berdasarkan pada protokol yang digunakan. Protokol adalah suatu aturan yang mendefinisikan beberapa fungsi yang ada dalam sebuah jaringan komputer, misalnya mengirim pesan, data, informasi dan fungsi lain yang harus dipenuhi dari sisi pengirim (*transmiter*) dan sisi penerima (*receiver*) agar komunikasi dapat berlangsung dengan benar

2.4.1 Model Referensi TCP/IP

TCP/IP adalah singkatan dari *Transmission Control Protocol/Internet Protocol*. TCP/IP merupakan dasar dari perkembangan Internet, dalam TCP/IP setiap data yang dilewatkan ke masing-masing layer direduksi atau ditambahkan suatu *header* kontrol. Setiap layer memperlakukan semua informasi yang terimanya sebagai data dan menambahkannya suatu *header* diawal informasi tersebut ketika data ini akan dilewatkan pada layer dibawahnya. Penambahan informasi pengirim ini disebut enkapsulasi (*encapsulation*). Hal ini berlaku sebaliknya ketika informasi ini bergerak dari jaringan ke layer teratas. Berikut ini proses enkapsulasi yang terjadi pada integrasi protokol TCP/IP dan WLAN.



Gambar 2.11 Integrasi TCP/IP dan WLAN

[Sumber **:** *www.wlana.org*]

Dalam TCP/IP hanya terdapat lima lapisan sebagai berikut :

a. *Application Layer* : Model TCP / IP tidak memiliki *session layer* dan *presentation layer*. *Aplication layer* berada di puncak model TCP / IP. Layer ini berisi layer-layer tingkat tinggi, yaitu Telnet, FTP, SMTP, HTTP, *Domain Name Service* (DNS), HTTP, WWW dan masih banyak lainnya.

b. *Transport Layer* : Ada dua jenis *transport layer* yaitu TCP dan UDP (*User Datagram Protokol*). TCP berfungsi memecah data menjadi paket-paket dan meneruskan ke *Internet layer*.

c. *Internet Layer* : Mengirimkan paket-paket IP yang berisikan informasi tujuan paket tersebut. Disini diperlukan *routing* paket untuk menghindari terjadinya kemacetan pada waktu tranmisi data.

d. *Network Access Layer* : Berkaitan dengan *logical interface* diantara suatu ujung sistem dan jaringan.

e. *Physical Layer* : Menentukan karakteristik-karakteristik media transmisi, rata-rata pensinyalan , serta skema pengkodean sinyal (*signal encoding scheme*).

Tabel 2.2 Proses *encapsulation*

Lapisan	Proses Encapsulation
Application, Presentation, Session	Informasi diubah menjadi data
Transport	Data diubah menjadi segmen / data stream
Network	Segmen diubah menjadi paket / datagram
Data-link	Paket diubah menjadi frame
Physical	Frame diubah menjadi bit

[Sumber : *Cisco Router : 4*]

2.4.2 Model Referensi OSI

Salah satu standar dalam protokol jaringan yang dikembangkan oleh ISO (*International Standard Organization*) adalah model referensi OSI (*Open System Interconnection*). OSI bukanlah protokol tetapi merupakan model untuk memahami dan mendesain suatu arsitektur jaringan yang fleksibel. Model ini memberikan Gambaran tentang fungsi, tujuan dan kerangka kerja suatu struktur model referensi untuk proses yang bersifat logis dalam sistem komunikasi. Adapun layer-layer pada OSI dan fungsi dari masing-masing lapisan adalah sebagai berikut

1. **Layer 7: *Application Layer***
   - Layer ini mendukung aplikasi proses pemakaian pada bagian terakhir dari *users* untuk komunikasi dan transfer data dalam suatu jaringan.

- Berfungsi mengenali *data syntax* dan *user authentication*. Layer ini menyediakan pelayanan aplikasi untuk pengiriman file, e-mail dan pelayanan *software* jaringan lainnya. FTP adalah aplikasi yang berada pada tingkat aplikasi.

2. **Layer 6: *Presentation Layer***
   - Presentation layer ini berfungsi untuk mengubah bentuk data agar bisa di baca oleh lapisan diatas maupun dibawahnya.
   - Menentukan arsitektur sesuai dengan format transfer data.
   - Melakukan proses enkoding dan dekoding data, kompresi dan dekompresi data.
3. **Layer 5: *Session Layer***
   - Lapisan ini mengatur, menetapkan proses penyambungan dan pemutusan hubungan antar *users*.
   - Melaporkan kesalahan lapisan diatasnya.
4. **Layer 4: *Transport Layer***
   - Mengatur pegiriman pesan/transfer data *end-to-end* dalam jaringan.
   - Menyediakan pengiriman paket yang berurutan melalui mekanisme perbaikan *error* dan *flow control*.
   - Menyediakan transfer data antar sistem.
5. **Layer 3: *Network Layer***
   - Lapisan ini menyediakan proses *switching* dan *routing* yang membentuk *logical path* yang disebut *virtual circuits*, untuk mentransmisikan data dari *node* ke *node*.
   - Melakukan proses routing dan proses selanjutnya seperti *addressing*, *internetworking*, *error handling*, *congestion control* dan *packet sequencing*
   - Mengarahkan jalur paket sesuai dengan alamat dalam jaringan.
6. **Layer 2: *Data Link Layer***
   - Pada layer ini data di *encode* dan *decode* menjadi berupa bit-bit yang digunakan untuk mendeteksi *error* paket data yang terjadi pada *physical layer* dengan menambahkan *flow control* dan *frame synchronization*.
   - Data link layer di bagi menjadi dua sub layer yaitu *Medium Access Control* (MAC) layer dan *Logical Link Control* (LLC) layer

7. **Layer 1: *Physical Layer***
   - Tingkat ini adalah perangkat keras komunikasi, yang menetapkan karakteristik fisik jaringan seperti koneksi, pewaktuan dan level tegangan.
   - Menetapkan peralatan fisik pada pengiriman data pada semua peralatan dalam jaringan.

2.5 Konfigurasi Jaringan WLAN

Standar IEEE 802.11 memiliki dua konfigurasi jaringan yaitu *ad-hoc* dan *infrastruktur*. Istilah lain yang sering dipakai adalah *Independent Basic Service Set* (*Independent* BSS) untuk *ad-hoc* dan *Extended Service Set* (ESS) untuk infrastruktur.

2.5.1 Konfigurasi *ad-hoc*

Pada konfigurasi *ad-hoc*, setiap *Mobile Station (*MS) dapat saling berkomunikasi secara langsung dan membentuk jaringan secara bebas tanpa harus melalui pusat jaringan. Tidak ada struktur tertentu dalam jaringan tersebut, tidak ada titik yang tetap. Media yang digunakan pada konfigurasi *ad-hoc* adalah gelombang radio. Konfigurasi *ad-hoc* ditunjukkan pada gambar 2.6.

Gambar 2.12 Model konfigurasi *Ad-Hoc.*

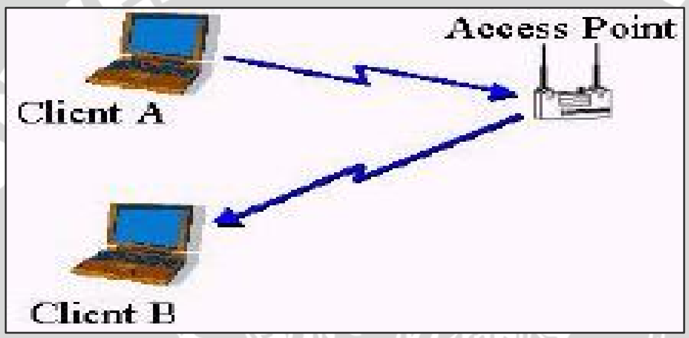
[Sumber: www.jmzacharias.com/wifi_files/image017.gif]

Pada gambar 2.6 diatas terdapat dua buah *laptop* dan sebuah PC yang terhubung secara *wireless* dengan konfigurasi *ad-hoc*. Agar bisa berkomunikasi, setiap perangkat harus mempunyai *wireless* NIC (*Network Interface Card*). Wireless NIC bisa berupa USB (*Universal Serial Bus*) *adapter*, *PC Card*, atau *PCI* (*Peripheral Card Interface*) *Adapter*.

Kedua laptop mempunyai perangkat *wireless* yang berbeda. *Laptop* pertama menggunakan *wireless USB Adapter*, sedangkan *laptop* kedua menggunakan *wireless PC card*. Pada PC (*Personal Computer*) menggunakan *wireless* PCI *Adapter*.

2.5.2 Konfigurasi Infrastruktur

Perangkat yang digunakan pada konfigurasi infrastruktur adalah *access point* (AP). AP digunakan sebagai titik akses untuk melakukan komunikasi (mengirim dan menerima data) antar *user* dalam jaringan infrastruktur. Saat AP menerima data, AP akan mengirimkan kembali data berupa sinyal radio ini ke perangkat *wireless* yang berada dalam range cakupan AP. Konfigurasi *infrastruktur* ditunjukkan pada gambar 2.13 di bawah ini.



Gambar 2.13 Model Konfigurasi Infrastruktur

[Sumber : Department of Computer Science University of Maryland]

Pada gambar 2.13 terdapat *access point* yang terhubung dengan dua laptop, yang selanjutnya disebut *client A* dan *client B*. *Access point* berfungsi menghubungkan perangkat *wireless* dengan jaringan kabel (LAN).

2.6 Delay

Definisi umum dari *delay* adalah waktu yang dibutuhkan untuk mengirimkan data dari sumber sampai ke tujuan.

2.6.1 Delay enkripsi

Delay enkripsi merupakan waktu yang dibutuhkan untuk mengenkripsi data. *Delay* enkripsi ini dipengaruhi *prosesor* yang digunakan, semakin cepat kinerja *prosesor* maka semakin sedikit nilay *delay* enkripsinya. *Delay* enkripsi dapat dirumuskan sebagai berikut :

$$t_{enkripsi} = \frac{L}{V} \tag{2.1}$$

dengan :

$t_{enkripsi}$ = *delay* enkripsi (s)

L = panjang data yang dienkripsi (*bit*)

V = kecepatan enkripsi (*bit/s*)

2.6.2 Delay propagasi

Delay propagasi adalah waktu perambatan atau perjalanan yang dibutuhkan oleh data atau paket dari satu *node* ke *node* yang lain melalui sebuah media transmisi. Kecepatan transmisi tergantung pada media transmisi antara pengirim dan penerima, serta jarak antara *node-node* tersebut. Besarnya *delay* propagasi dapat dirumuskan sebagai berikut :

$$t_{prop} = \frac{d}{c} \tag{2.2}$$

dimana :

t_{prop} = waktu propagasi (s)

d = jarak antara *Access Point* ke *Client* (m)

c = kecepatan gelombang elektromagnetik (m/s)

Delay propagasi dipengaruhi jarak antara *access point* ke *client,* sehingga semakin jauh jarak antar keduanya, maka *delay* propagasinya semakin besar.

2.6.3 Delay proses

Delay proses adalah waktu yang diperlukan untuk memproses paket data dari pengirim ke penerima. Delay proses pada jaringan WLAN berupa delay enkapsulasi dan dekapsulasi. Berikut ini adalah format data pada WLAN saat terjadi pemrosesan data dari pengirim ke penerima.

2.6.3.1 Format Data Pada Network Layer

Data yang berasal dari layer aplikasi pada layer *network* ditambahkan header IP dan header TCP, sehingga format datanya berubah. Besarnya header IP ini adalah 20 *byte* dan header TCP adalah 20 *byte*. Format data yang telah berubah tersebut dapat digambarkan sebagai berikut :

IP Header (20 *byte*)	TCP Header (20 *byte*)	*Application Data* (1460 *byte*)

Gambar 2.14 Format data pada Layer *Network*

(Sumber : www.wlana.org)

2.6.3.2 Format Data Pada Data Link Layer

Setelah melewati protokol TCP/IP, data diteruskan ke layer data link. Pada layer ini, data yang berasal dari protokol TCP/IP ditambahkan header MAC sebesar 30 byte dan ditambahkan FCS (*Frame Check Sequence*) sebesar 4 byte. Sehingga format data berubah menjadi :

MAC Header (30 *byte*)	IP Header (20 *byte*)	TCP Header (20 *byte*)	*Application Data* (1460 *byte*)	FCS (4 *byte*)

Gambar 2.15 Format data pada Layer Data Link

(Sumber : www.wlana.org)

2.6.3.3 Format Data Pada Physical Layer

Setelah melewati layer *data link*, data diteruskan ke layer *physical*. Dalam protokol ini data ditambahkan PLCP (*Physical Layer Convergence Protocol) Preamble* dan PLCP *Header* yang besarnya 18 *byte* dan 6 *byte.* Sehingga format datanya menjadi sebagai berikut :

PLCP *Preamble* (18 *byte*)	PLCP *Header* (6 *byte*)	MAC *Header* (30 *byte*)	IP *Header* (20 *byte*)	TCP *Header* (20 *byte*)	*Application Data* (1460 *byte*)	FCS (4 *byte*)

Gambar 2.16 Format Data Layer Physical WLAN

(Sumber : www.wlana.org)

Ketika data dikirim dari sumber melewati layer aplikasi menuju layer *network*, data akan diubah menjadi segmen. Pada layer ini, data akan mengalami penambahan header TCP dan header IP (gambar 2.14). Jika data yang akan dikirim sebesar 1460 byte, maka besarnya message data ($W_{message}$) dapat diperoleh sebagai berikut:

$$\begin{aligned} W_{message} &= W_{data} + Header_{TCP} + Header_{IP} \\ &= 1460\ byte + 20\ byte + 20\ byte \\ &= 1500\ byte \end{aligned}$$

Dari layer *network*, data dikirim ke layer *data link* dan mengalami penambahan header MAC dan FCS (gambar 2.15). Pada layer ini message data diubah manjadi *frame*. Sehingga besarnya data menjadi :

$$W_{frame} = W_{message} + Header\ MAC + FCS$$
$$= 1500 byte + 30 byte + 4 byte$$
$$= 1534\ byte$$

Dari data link, data dikirimkan ke layer *physical* dan mengalami penambahan PLCP Preamble sebanyak 18 byte dan PLCP Header sebanyak 6 byte (gambar 2.16) menjadi :

$$W_{total} = W_{frame} + \Pr eamble_{PLCP} + Header_{PLCP}$$
$$= 1534 byte + 18 byte + 6 byte$$
$$= 1558\ byte$$

Maka besar delay enkapsulasi adalah :

$$t_e = \frac{W_{frame}}{C_{WLAN}} x 8 bit / byte$$

Sedangkan besar delay dekapsulasi adalah :

$$t_d = \frac{W_{frame}}{C_{WLAN}} x 8 bit / byte$$

Dengan demikian delay proses adalah :

$$t_{proses} = t_e + t_d \tag{2.3}$$

2.6.4 Delay transmisi

Delay transmisi adalah waktu yang dibutuhkan untuk meletakkan semua data pada medium, dipengaruhi oleh ukuran paket dan kapasitas media transmisi. Besar *delay* transmisi sesuai dengan persamaan adalah :

$$t_{trans} = \frac{W_{frametotal}}{V_{trans}} \tag{2.4}$$

dimana :

t_{trans} : Delay transmisi pada jaringan WLAN (*s*).

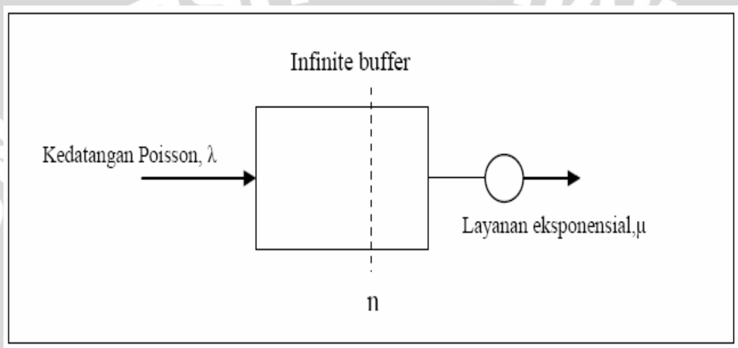
$W_{frametotal}$: Jumlah frame total pada jaringan WLAN (*bit*).

V : Kecepatan transmisi paket data antara *access point* dan *client* (*bit/s*).

2.6.5 Delay antrian

Delay antrian adalah waktu dimana paket data tersebut berada dalam antrian untuk ditransmisikan. Selama waktu itu paket data menunggu sampai selesainya paket lain ditransmisikan. Jika antrian kosong dan tidak ada paket data yang lain yang ditransmisikan, maka *delay* antrian tidak terjadi. Model antrian yang digunakan adalah model antrian *M/M/1*.

Delay antrian dapat dihitung dengan menggunakan model antrian M/M/1. M pertama menunjukkan distribusi kedatangan *Poisson,* M kedua berarti distribusi waktu pelayanan eksponensial, dan 1 menunjukkan bahwa jumlah *server* adalah tunggal. Disiplin antrian yang digunakan adalah FIFO (*First In First Out*).



Gambar 2.17 Model antrian M/M/1
[Sumber: Mischa Schwartz, 1987:31]

Besarnya *delay* antrian yang terjadi pada *node* yaitu:

$$t_w = t_{queue} + t_{serv} \tag{2.5}$$

dengan:

t_w = *delay* pada node (detik)

t_{queue} = waktu tunggu paket pada node (detik)

t_{serv} = waktu rata – rata pelayanan node (detik)

Waktu rata – rata pelayanan *node* diperoleh dari persamaan:

$$t_{serve} = \frac{1}{\mu} \tag{2.6}$$

dengan:

μ = kecepatan pelayanan node (paket/detik)

Sedangkan nilai kecepatan pelayanan node diperoleh dari persamaan [Mischa Schwartz, 1987:23]:

$$\mu = \frac{C}{L} \tag{2.7}$$

dengan:

C = kecepatan transmisi data pada node (bps)

L = panjang paket data (bit/paket)

Performansi sistem antrian ditunjukkan dalam bentuk utilisasi

$$\rho = \frac{\lambda}{\mu} \Rightarrow \lambda = \mu\rho \tag{2.8}$$

dengan:

ρ = utilisasi (0< ρ<1)

λ = kecepatan kedatangan paket pada node (paket/detik)

Faktor utilisasi bernilai lebih besar dari 0 dan lebih kecil dari 1 dengan kenaikan sebesar 0,1. Hal ini disebabkan karena jika ρ > 1 berarti rata – rata kedatangan melampaui rata – rata pelayanan atau server tidak dapat menjaga rata – rata kedatangan dan panjang antrian yang bertambah tanpa batas.

Dengan menggunakan teori Little diperoleh nilai *delay* antrian:

$$t_w = \frac{1}{\mu(1-\rho)} \tag{2.9}$$

Dari persamaan di atas maka waktu tunggu paket dirumuskan:

$$t_{queue} = t_w - t_{serv} = \frac{\lambda}{\mu(\mu-\lambda)} \tag{2.10}$$

Dari persamaan (2.6) dan (2.10) maka *delay* antrian dapat dirumuskan dengan:

$$t_w = \frac{\lambda}{\mu(\mu-\lambda)} + \frac{1}{\mu} \tag{2.11}$$

dengan:

t_w = *delay* antrian (detik)

λ = kecepatan kedatangan paket pada node (paket/detik)

μ = kecepatan pelayanan node (paket/detik)

2.6.6 Delay Total

Besar *delay* jaringan WLAN dari *access point* ke *client* adalah :

$$T_{total} = t_e + t_d + 3t_p + 2t_{prop} + 2t_t + t_w \tag{2.12}$$

2.7 *Throughput*

Throughput didefinisikan sebagai jumlah total *byte* yang diterima di sisi penerima dengan baik. Persamaan *throughput* adalah sebagai berikut :

$$\lambda = \frac{(1-\rho)}{t_i[1+(\alpha-1)\rho]}.(l+l') \qquad (2.13)$$

dengan :

λ = *throughput* (bps)

t_i = waktu total transmisi sebuah paket data (*s*)

α = konstanta propagasi

$$\alpha = \left[1+\frac{t_{prop}}{t_i}\right]$$

(l + l') = ukuran paket (bit)

ρ = probabilitas paket yang salah pada jaringan WLAN.

Panjang paket data ditambah panjang *header* yang digunakan sebagai pengontrol ditransmisikan dari pengirim ke penerima, sehingga probabilitas paket salah menjadi :

$$p = (L+L')\ x\ p_b \qquad (2.14)$$

dengan :

L = panjang paket data (*bit*).

L' = panjang header paket data (*bit*).

p_b = probabilitas *bit* salah dalam proses pengiriman data dari pengirim ke penerima, dan besarnya p_b dapat dirumuskan sebagai berikut :

$$p_b = 1/2\ erfc\sqrt{\frac{E_b}{N_o}} \qquad (2.15)$$

p_b = *bit error rate* (BER)

Untuk mendapatkan nilai BER, maka dicari nilai Eb/No.

Nilai perbandingan energi *bit* terhadap *noise* (Eb/No) dapat dicari dengan persamaan :

$$\left(\frac{E_b}{N_o}\right) = (RSL)_{dBW} - 10\log(Br) + 228.6dBW - 10\log T_e] \qquad (2.16)$$

dengan :

E_b / N_o = Energi *bit* terhadap *noise* (dB)

RSL = *Receive Signal Level* (dBW)

Br = *bit rate* (bps).

T_e = *effective noise temperature* (K).

Dimana *Receive Signal Level* (RSL) dapat dicari dengan persamaan :

$$RSL_{dBW} = EIRP_{dBW} - FSL + G_R \quad (2.17)$$

dengan :

EIRP = *Effective Isotropically Radiated Power* (dBW).

FSL = *Free Space Loss* (dB).

Sedangkan *effective isotropically radiated power* dapat dicari dengan persamaan :

$$EIRP_{dBW} = P_t + G_t \quad (2.18)$$

dengan :

P_t = daya pancar (dBW).

G_t = antena *gain* (dB).

dan *Free Space Loss* (FSL) dapat dihitung dengan persamaan :

$$FSL = 32{,}4 + 20 \log D + 20 \log F \quad (2.19)$$

dengan :

FSL = *Free Space Loss* (dB).

D = jarak antara *access point* ke *client* (km).

F = frekuensi yang digunakan (KHz).

2.8 *Wi-Fi Protected Access (WPA)*

Wi-Fi Protected Access adalah sebuah spesifikasi keamanan Wi-Fi (*Wireless Fidelity*) yang dibuat oleh *Wi-Fi Alliance* dan IEEE (*Institute of Electrical and Electronics Engineers*) untuk meningkatkan keamanan data dan kontrol akses pada jaringan WLAN yang sudah ada.

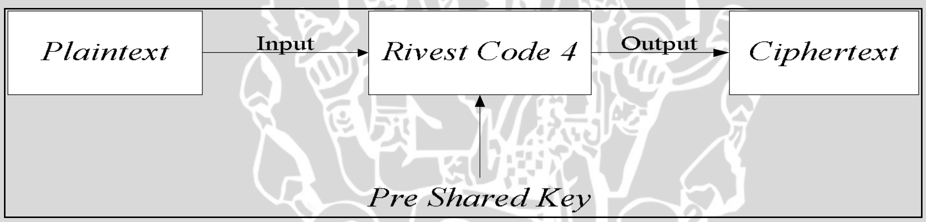
Pada WPA proses pengamanan dilakukan dengan cara memberikan *IV (Initialization Vector)*. Kemudian *Pre-Shared Key (PSK)* selanjutnya akan melalui proses RC4 menjadi *keystream* yang selanjutnya di-*XOR*-kan dengan *plaintext* dan kemudian ditambahkan dengan *message integrity* menjadi pesan terenkripsi (*ciphertext*).

Algoritma yang digunakan pada WPA adalah algoritma *hashing* dan algoritma RC4. Algoritma *hashing* berfungsi mengacak kunci, dan algoritma RC4 berfungsi untuk memproses unit atau input. Algoritma hashing yang dipakai adalah tipe MD5.

WPA bekerja pada semua versi piranti yang mendukung standar 802.11. WPA merupakan pengembangan dari WEP (*Wired Equivalent Privacy*). Perbedaannya dengan WPA adalah pada WEP kunci yang digunakan masih bersifat statik.

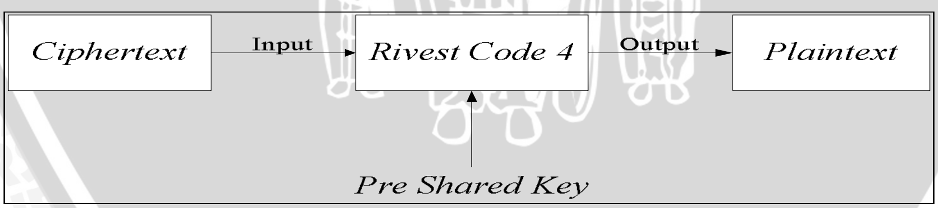
Kunci keamanan dinamik yang digunakan pada WPA adalah TKIP (*Temporal Key Integrity Protocol*) yang mampu berubah secara dinamis selama data ditransmisikan. Protokol TKIP akan mengambil kunci utama sebagai *starting point* yang kemudian secara reguler berubah sehingga tidak ada kunci enkripsi yang digunakan dua kali.

Selain itu, pada WPA juga disediakan authentikasi *user* yang belum diterapkan pada WEP. Authentikasi user yang digunakan pada WPA adalah PSK (*Pre Shared Key*). Blok diagram proses enkripsi dan dekripsi WPA-PSK ditunjukkan pada gambar 2.18 dan 2.19 di bawah ini.



Gambar 2.18 Proses enkripsi pada WPA-*PSK*

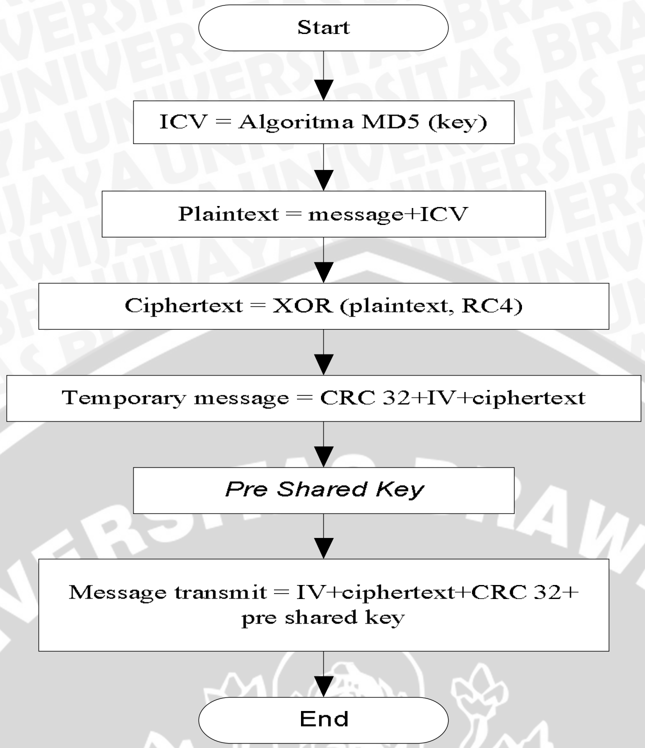
Sumber : Pemodelan



Gambar 2.19 Proses dekripsi pada WPA-*PSK*

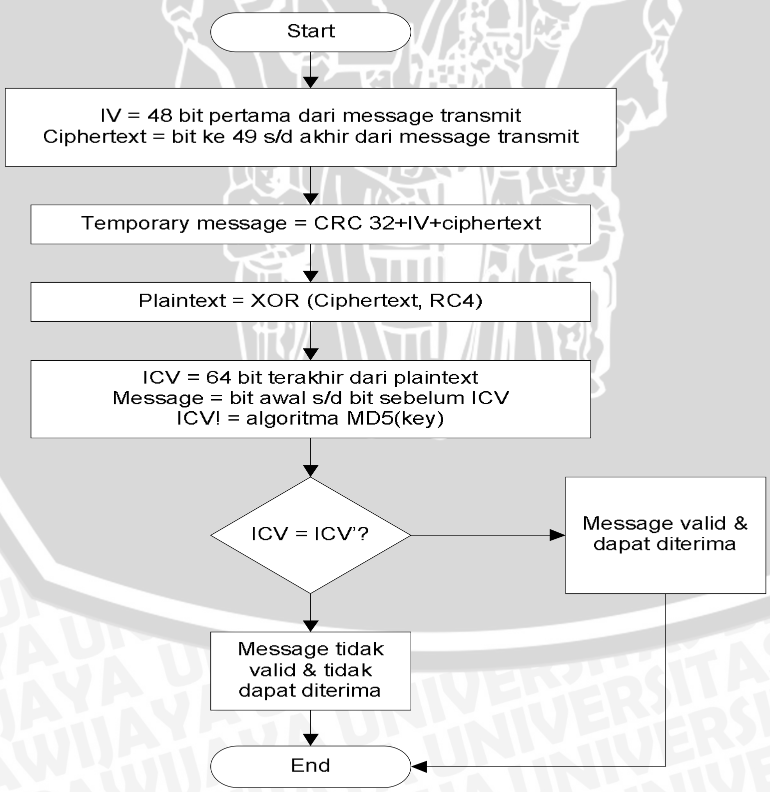
Sumber : Pemodelan

Sedangkan diagram alir proses enkripsi dan dekripsi pada WPA-PSK ditunjukkan pada gambar 2.20 dan 2.21



Gambar 2.20 Diagram alir enkripsi pada WPA-*PSK*

Sumber : Pemodelan



Gambar 2.21 Diagram alir dekripsi pada WPA-*PSK*

Sumber : Pemodelan

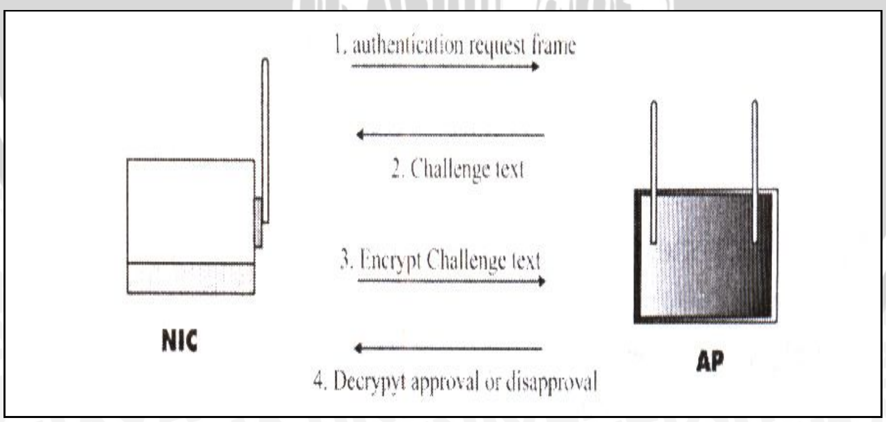
2.9 *Pre Shared Key (PSK)*

Pre Shared Key adalah sebuah metode autentikasi atau pencocokan identitas yang menggunakan kunci yang sama antara *Access Point* dan *client*. Pada PSK, sebuah identitas dianggap cocok apabila *challenge text* yang dikirim oleh *access point* ke NIC (*Network Interface Card*) sama dengan *challenge text* terenkripsi yang dikirim balik dari NIC ke *access point*.

Authentikasi yang digunakan pada PSK didasarkan pada WEP (*Wired Equivalent Privacy*). Pada PSK (*Pre Shared Key*) terdapat empat proses authentikasi, yaitu :

1. NIC (*Network Interface Card*) akan memulai dengan mengirimkan *authentication request frame* ke *access point.*
2. *Access point* akan menempatkan *challenge text* ke *body frame* sebagai respons dan mengirimkannya ke NIC.
3. NIC menggunakan kunci WEP untuk mengenkripsi *challenge text*, kemudian mengirimkannya kembali ke *access point* dalam frame yang lain.
4. *Access point* kemudian melakukan pembukaan enkripsi (*decrypt*) *challenge text* dan membandingkan dengan teks awal. Jika teks ini sama persis, maka access point akan menganggap NIC tersebut mempunyai kunci yang benar. *Access point* akan mengakhiri proses ini dengan mengirimkan frame authentikasi ke NIC dengan isi persetujuan atau penolakan.

Proses authentikasi dengan menggunakan metode *Pre-Shared Key* ditunjukkan pada gambar 2.22



Gambar 2.22 Proses *Pre-Shared Key Authentication*

[*Sumber Mulyanta, Edi. 2005.“Pengenalan Protokol Jaringan Wireless Komputer”*]

2.10 *TKIP (Temporal Key Integrity Protocol)*

TKIP adalah sebuah protokol yang didefinisikan oleh IEEE 802.11i. TKIP didesain untuk menggantikan WEP tanpa mengganti perangkat keras. TKIP menggunakan skema kunci berdasarkan RC4, tetapi tidak seperti WEP, TKIP mengenkripsi semua paket data yang dikirimkan dengan kunci enkripsi yang unik. TKIP menghasilkan "*per-packet key mixing*", sebuah pesan yang ter-*integrity* dan sebuah mekanisme "*re-keying*" sehingga pengalamatan menjadi pengamanan. TKIP mengacak kata kunci menggunakan algoritma *hashing*.

Proses enkripsi TKIP berawal dari sebuah paket yang terdiri kunci *pre shared key* dan sebuah *Initialization Vector* (*IV*). Oleh *IV*, *pre shared key* diacak menggunakan algoritma *hashing* menghasilkan sebuah *temporal key*.

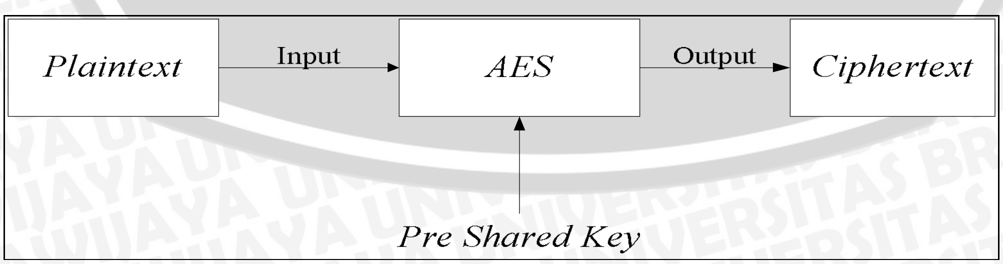
Hasil pengacakan berupa *temporal key* bersama IV dienkripsi menggunakan algoritma RC4 menghasilkan *stream cipher* (aliran bit kunci yang teracak). Selanjutnya bersama *plaintext*, *stream cipher* di-*XOR*-kan untuk menghasilkan data yang terenkripsi.

2.11 *Wi-Fi Protected Access2* (WPA2)

WPA2 adalah nama lain dari standar IEEE 802.11i, yang dibuat untuk mengatasi enkripsi data pada metode WEP yang sudah tidak aman. Enkripsi data yang digunakan pada WPA2 adalah *Advanced Encryption Standard* (AES).

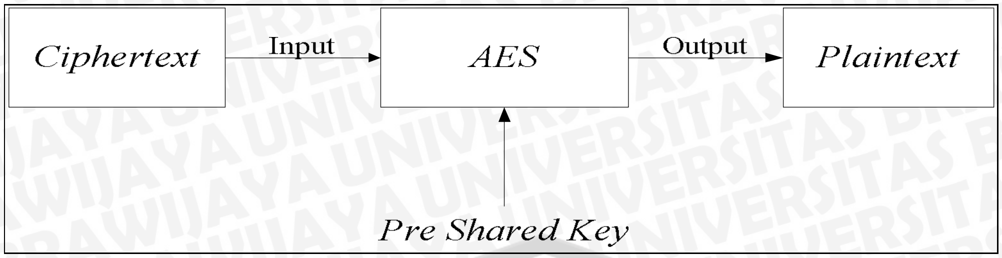
WPA2 menggunakan *Temporal Key Integrity Protokol* (TKIP) untuk mengacak kunci. Masukan pada WPA2 berupa data *plaintext* dan keluarannya berupa data *ciphertext*.

Pada WPA2 terdapat *authentikasi user* yang disebut *Pre Shared Key* (PSK), selanjutnya proses enkripsi data dan *authentikasi user* ini disebut WPA2-PSK. Blok diagram proses enkripsi dan dekripsi pada WPA2-PSK seperti pada gambar 2.23 dan gambar 2.24.



Gambar 2.23 Proses enkripsi pada WPA2-*PSK*

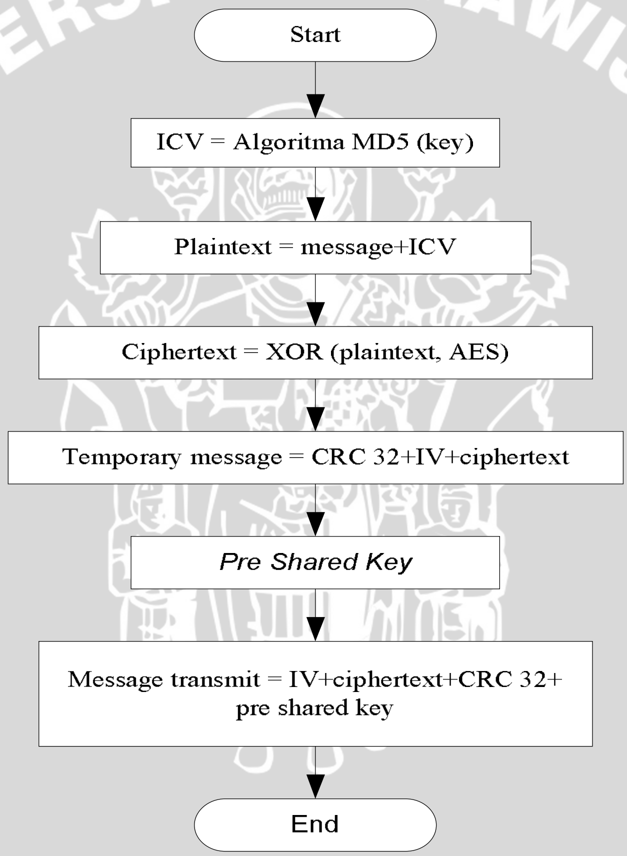
Sumber : Pemodelan



Gambar 2.24 Proses dekripsi pada WPA2-*PSK*

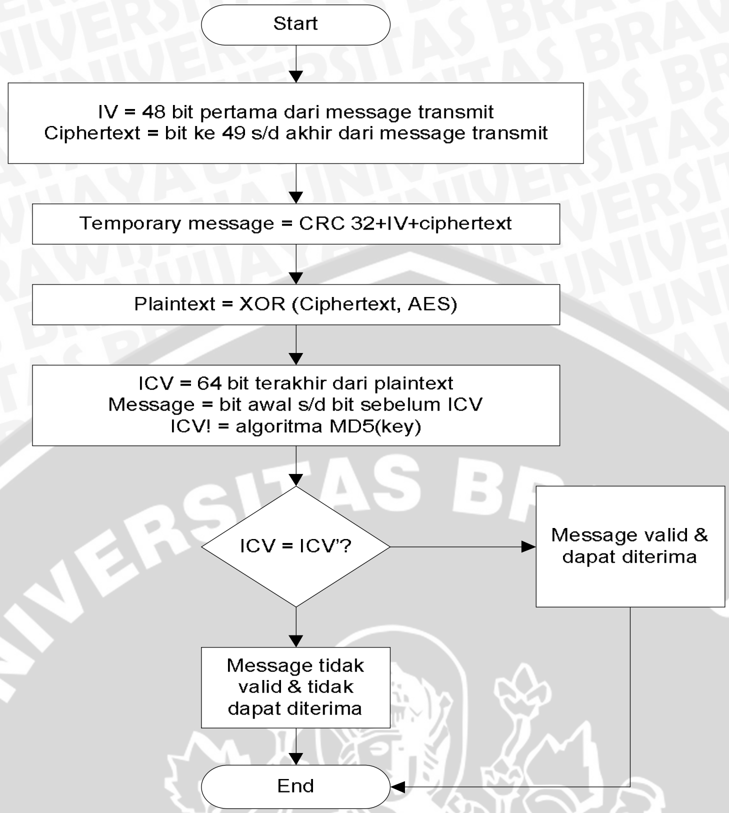
Sumber : Pemodelan

Sedangkan diagram alir proses enkripsi dan dekripsi pada WPA2-PSK ditunjukkan pada gambar 2.25 dan 2.26



Gambar 2.25 Diagram alir enkripsi pada WPA2-*PSK*

Sumber : Pemodelan



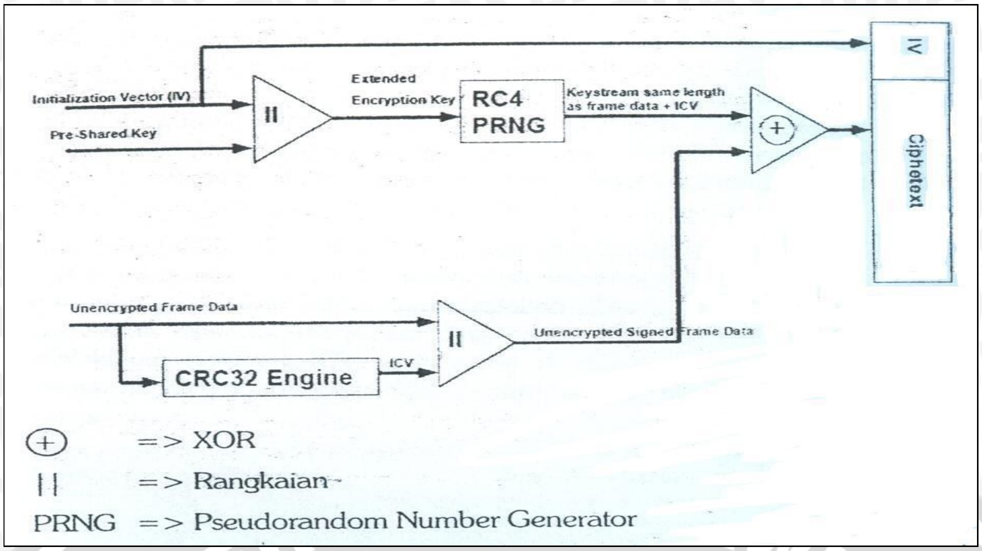
Gambar 2.26 Diagram alir dekripsi pada WPA2-*PSK*

Sumber : Pemodelan

2.12 *WEP (Wired Equivalent Privacy)*

WEP (*Wired Equivalent Privacy*) adalah salah satu metode enkripsi dan authentikasi pada standar 802.11. Algoritma yang digunakan pada WEP adalah algoritma RC4. Saat diaktifkan, WEP melakukan enkripsi pesan yang saling ditukarkan antara *mobile station* dengan *access point* melalui jaringan *wireless*.

Pada WEP masukannya berupa kunci *Pre Shared Key* 104 *bit* dan *Initialization Vector* (IV) 24 bit. Sedangkan *output*nya berupa *ciphertext* sebesar 128 bit. Rangkaian enkripsi WEP pada PSK ditunjukkan pada gambar 2.27.



Gambar 2.27 Rangkaian enkripsi *Wired Equivalent Privacy (*WEP*)*
[*Sumber : Mulyanta, Edi. 2005. "Pengenalan Protokol Jaringan Wireless Komputer". Hal 192*]

Saat WEP diaktifkan, WEP akan melakukan enkripsi pesan yang saling ditukarkan antara *access point* dan *client*. Proses enkripsi WEP pada PSK seperti ditunjukkan gambar 2.27 adalah sebagai berikut :

1. WEP menyiapkan sebuah *key schedule* (*seed*) untuk menghubungkan kunci yang di-*share* antara *access point* dan *client*, yang disebut *Pre Shared Key* (PSK). Kunci ini dikirimkan kepada *client* secara random yang di-*generate* menggunakan 24 bit *Initialization Vector* (IV).
2. IV digunakan bersama dengan kunci enkripsi WEP 104 bit yang disebut *Extended Encryption Key*. Kunci WEP kemudian akan ditempatkan bersama penggunaan RC4 PRNG (*Rivest Code 4 Pseudo Random Number Generator*) yang digunakan untuk melakukan *generate keystream* enkripsi.
3. RC4 PRNG akan menghasilkan keystream yang sama dengan panjang *payload frame* ditambah dengan 32 bit *Integrity Check Value* (ICV).
4. *Keystream* kemudian di-*XOR*-kan (melakukan proses XOR) dengan frame body (tanpa *frame header*) yang akan menghasilkan data terenkripsi (*ciphertext*).
5. Pada WEP terdapat bagian frame yang tidak terenkripsi. Bagian ini digunakan oleh CRC (*Cyclical Redundancy Checking*) untuk memastikan integritas data yang ditransmisikan.

6. Pada CRC terdapat ICV (*Integrity Check Value*) yang bertugas menentukan apakah data yang terkirim mengalami kerusakan saat ditransmisikan atau tidak. Jika station penerima dalam melakukan kalkulasi ICV tidak sama, station penerima akan menolak frame yang terkirim.

WEP digunakan untuk menentukan kunci rahasia yang di-*share* dalam melakukan enkripsi dan dekripsi data. Dengan WEP, *station* penerima harus mempunyai kunci yang sama untuk melakukan dekripsi. Setiap NIC radio dan *access point* harus dikonfigurasikan secara manual untuk menyamakan kunci.

2.13 *Rivest Code 4* (RC4)

RC4 adalah algoritma yang digunakan pada metode keamanan WPA-PSK. RC4 merupakan jenis *stream cipher,* yaitu algoritma yang memproses enkripsi per karakter untuk setiap *byte*.

Kunci yang digunakan pada RC4 mempunyai panjang 1 sampai 256 *bit*. Kunci tersebut digunakan untuk menginialisasi tabel sepanjang 256 *bit*. Tabel tersebut digunakan untuk menghasilkan *pseudo random bit*. Kemudian aliran *pseudo random bit* yang memproses *XOR* dengan *plaintext* untuk menghasilkan *ciphertext*. Masing-masing elemen dalam tabel saling ditukarkan minimal sekali.

RC4 mempunyai sebuah S-Box, S0,S1,...,S255, yang berisi permutasi dari bilangan 0 sampai 255, dan permutasi merupakan fungsi dari kunci dengan panjang yang variabel. Terdapat dua indeks yaitu *i* dan *j*, yang diinisialisasi dengan bilangan nol. Langkah-langkah enkripsi pada RC4 :

1. Inisialisasi S-Box.

   Pada tahapan ini, S-Box akan diisi dengan nilai sesuai indeksnya untuk mendapatkan S-Box awal. Algoritmanya adalah sebagai berikut :

   a) Untuk i = 0 sampai 255 isikan S ke i dengan nilai i
   b) Tambahkan i dengan 1.

   Dari algoritma diatas akan didapat urutan nilai S-Box sebagai berikut :

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47
48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63
64	65	66	67	68	69	70	71	72	73	74	75	76	77	78	79
80	81	82	83	84	85	86	87	88	89	90	91	92	93	94	95
96	97	98	99	100	101	102	103	104	105	106	107	108	109	110	111
112	113	114	115	116	117	118	119	120	121	122	123	124	125	126	127
128	129	130	131	132	133	134	135	136	137	138	139	140	141	142	143
144	145	146	147	148	149	150	151	152	153	154	155	156	157	158	159
160	161	162	163	164	165	166	167	168	169	170	171	172	173	174	175
176	177	178	179	180	181	182	183	184	185	186	187	188	189	190	191
192	193	194	195	196	197	198	199	200	201	202	203	204	205	206	207
208	209	210	211	212	213	214	215	216	217	218	219	220	221	222	223
224	225	226	227	228	229	230	231	232	233	234	235	236	237	238	239
240	241	242	243	244	245	246	247	248	249	250	251	252	253	254	255

2. Menyimpan *key* dalam *Key Byte Array*.

   Pada tahapan ini, kunci (*key*) yang akan digunakan untuk mengenkripsi atau dekripsi akan dimasukkan ke dalam *array* berukuran 256 *byte* secara berulang sampai seluruh *array* terisi. Algoritmanya adalah sebagai berikut:

   a) Isi j dengan 1
   b) Untuk *i* = 0 sampai *i* = 255 isikan :

      Jika j > panjang kunci maka

      j diisi dengan nilai 1
   c) Isi K ke i dengan nilai ascii karakter kunci ke j.
   d) Nilai j dinaikkan 1
   e) Tambahkan i dengan 1.

Dari algoritma diatas akan didapat urutan *array key* sebagai berikut :

109	97	104	97	98	98	97	104	109	97	104	97	98	98	97	104
109	97	104	97	98	98	97	104	109	97	104	97	98	98	97	104
109	97	104	97	98	98	97	104	109	97	104	97	98	98	97	104
109	97	104	97	98	98	97	104	109	97	104	97	98	98	97	104
109	97	104	97	98	98	97	104	109	97	104	97	98	98	97	104
109	97	104	97	98	98	97	104	109	97	104	97	98	98	97	104
109	97	104	97	98	98	97	104	109	97	104	97	98	98	97	104
109	97	104	97	98	98	97	104	109	97	104	97	98	98	97	104
109	97	104	97	98	98	97	104	109	97	104	97	98	98	97	104
109	97	104	97	98	98	97	104	109	97	104	97	98	98	97	104
109	97	104	97	98	98	97	104	109	97	104	97	98	98	97	104
109	97	104	97	98	98	97	104	109	97	104	97	98	98	97	104
109	97	104	97	98	98	97	104	109	97	104	97	98	98	97	104
109	97	104	97	98	98	97	104	109	97	104	97	98	98	97	104
109	97	104	97	98	98	97	104	109	97	104	97	98	98	97	104
109	97	104	97	98	98	97	104	109	97	104	97	98	98	97	104

3. Permutasi pada S-Box.

   Pada tahapan ini, akan dibangkitkan sebuah nilai yang akan dijadikan aturan untuk permutasi pada S-Box. Misalkan untuk nilai i = 2 dihasilkan nilai j = 26, maka nilai pada S(2) akan ditukar dengan nilai pada S(26). Algoritmanya sebagai berikut :

   a) Isi nilai j dengan 0
   b) Untuk i = 0 sampai i = 255 lakukan

      Isi nilai j dengan hasil operasi (j+S(i) + K(i)) mod 256

      Swap S(i) dan S(j)

   c) Tambahkan i dengan 1.

   Dari algoritma tersebut akan diperoleh nilai S-Box sebagai berikut :

109	26	57	76	157	245	52	49	181	31	45	103	84	240	73	192
61	235	28	98	3	205	160	128	130	59	22	38	92	122	137	30
247	121	4	135	156	148	231	170	228	16	68	208	159	53	210	20
176	168	220	214	136	19	87	42	120	219	27	169	183	116	200	96
204	110	64	216	89	222	44	126	105	213	164	188	23	47	194	33
209	65	162	142	107	195	119	80	166	238	237	72	246	102	243	241
35	40	77	215	141	100	74	115	146	56	189	163	113	55	67	229
236	185	83	46	18	140	118	50	233	248	99	8	172	203	54	132
13	124	152	252	151	153	147	139	179	190	82	154	224	161	86	0
34	149	29	225	78	14	48	158	25	104	150	184	218	187	95	193
79	43	155	223	143	232	177	251	66	114	202	10	9	88	6	226
239	250	178	71	106	51	11	60	125	242	17	90	197	91	249	173
94	15	201	101	108	234	227	41	75	117	165	174	230	138	207	62
70	244	129	145	182	131	112	7	171	253	111	198	134	180	167	211
39	255	2	1	32	85	254	21	63	217	212	175	12	93	123	191
36	186	37	133	144	24	69	81	206	5	196	199	97	221	58	127

4. *Generate Pseudorandom byte stream.*

Pada tahapan ini akan dihasilkan nilai *pseudorandom* yang akan dikenakan operasi XOR untuk menghasilkan *ciphertext* ataupun sebaliknya yaitu untuk menghasilkan *plaintext*. Algoritmanya adalah sebagai berikut :

i = (i + 1) mod 256

j = (j + S (i)) mod 256

Swap S (i) dan *S (j)*

t = (S(I) + (S(j) mod 256)) mod 256

K = S(t), Nilai K akan di-XOR terhadap *plaintext* atau *ciphertext*.

Operasi XOR pada *generate pseudorandom byte stream* :

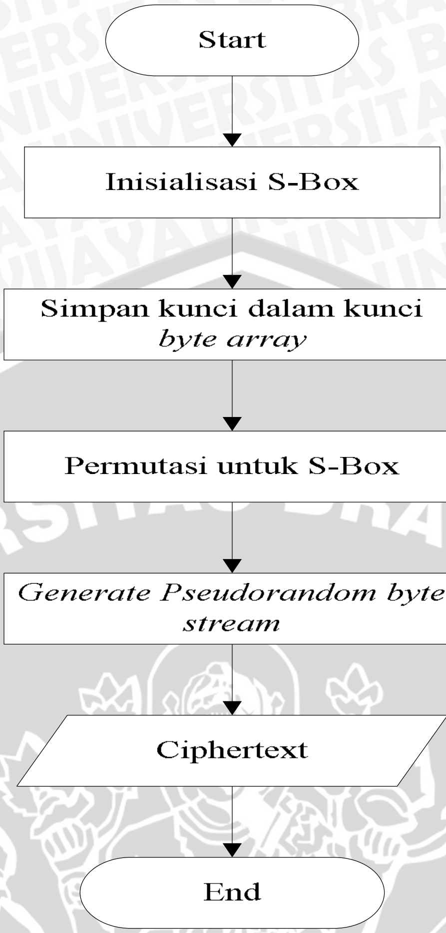
Exclusive OR (XOR) merupakan operator *Boolean* yang akan membandingkan dua angka untuk menentukan dua angka tersebut sama atau tidak. Jika nomor sama, nilai 0 akan diberikan. Jika nilai berubah, maka nilai 1 diberikan. Implementasi operasi XOR seperti berikut :

01100010 adalah huruf b dalam biner

01101110 adalah huruf n dalam biner

00001100 adalah nilai XOR

Proses algoritma RC4 ditunjukkan pada gambar 2.28 berikut ini:



Gambar 2.28 Rangkaian proses algoritma RC4
[Sumber : Nugroho, 2004 : 71]

2.14 *Advanced Encryption Standard* (AES)

Advanced Encryption Standard (AES) adalah algoritma yang digunakan pada metode keamanan WPA2-PSK. AES merupakan jenis blok *cipher*, yaitu algoritma yang memproses enkripsi per blok (8 byte atau 16 byte).

Masukan data pada AES berupa *plaintext* 128 *bit*. Masukan ini diberi *cipher key* menghasilkan keluaran berupa *ciphertext*.

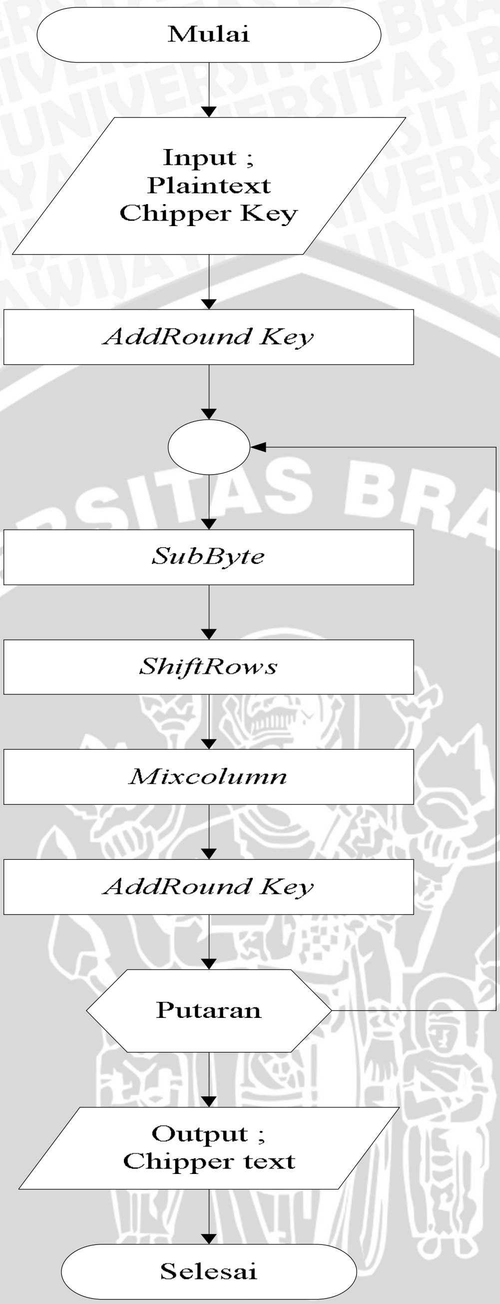
Pada algoritma AES, data input atau *plaintext* diproses melalui serangkaian transformasi, yang terdiri dari transformasi *SubBytes*, *ShiftRows*, *MixColumns* dan *AddRoundKey*, dengan menggunakan kunci rahasia yaitu *cipher key*.

Langkah-langkah enkripsi pada *Advanced Encryption Standard* (AES) adalah sebagai berikut :

1. *AddRoundKey* : melakukan XOR antara state awal (*plaintext*) dengan *cipher key*. Tahap ini disebut juga *initial round*.

2. Putaran sebanyak Nr – 1 kali. Proses yang dilakukan pada setiap putaran adalah :
   a. *SubByte* : Substitusi *byte* dengan menggunakan tabel substitusi (*S-box*)
   b. *ShiftRow* : Pergeseran baris-baris *array state.*
   c. *MixColumn* : Mengacak data di masing-masing kolom *array State*.
   d. *AddRoundKey* : Melakukan *XOR* antara *state* sekarang dengan *round key*.
3. *Final round* : Proses untuk putaran akhir.
   a. SubByte
   b. ShiftRow
   c. AddRoundKey

Diagram proses enkripsi AES ditunjukkan pada gambar 2.29.



Gambar 2.29 Diagram proses enkripsi AES

[Sumber : Sidiq, Ahmad Fajar. 2007. *Jenis-jenis enkripsi*, hal 7]

Proses yang dilakukan pada setiap putaran adalah sebagai berikut :

1. Transformasi *SubBytes*

   Transformasi *SubBytes* merupakan operasi substitusi yang beroperasi secara independen pada setiap *byte state* menggunakan tabel substitusi (kotak-S).

   Tabel substitusi ditunjukkan pada gambar 2.30 di bawah ini:

	y															
x	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
0	63	7c	77	7b	f2	6b	6f	c5	30	01	67	2b	fe	d7	ab	76
1	ca	82	c9	7d	fa	59	47	f0	ad	d4	a2	af	9c	a4	72	c0
2	b7	fd	93	26	36	3f	f7	cc	34	a5	e5	f1	71	d8	31	15
3	04	c7	23	c3	18	96	05	9a	07	12	80	e2	eb	27	b2	75
4	09	83	2c	1a	1b	6e	5a	a0	52	3b	d6	b3	29	e3	2f	84
5	53	d1	00	ed	20	fc	b1	5b	6a	cb	be	39	4a	4c	58	cf
6	d0	ef	aa	fb	43	4d	33	85	45	f9	02	7f	50	3c	9f	a8
7	51	a3	40	8f	92	9d	38	f5	bc	b6	da	21	10	ff	f3	d2
8	cd	0c	13	ec	5f	97	44	17	c4	a7	7e	3d	64	5d	19	73
9	60	81	4f	dc	22	2a	90	88	46	ee	b8	14	de	5e	0b	db
a	e0	32	3a	0a	49	06	24	5c	c2	d3	ac	62	91	95	e4	79
b	e7	c8	37	6d	8d	d5	4e	a9	6c	56	f4	ea	65	7a	ae	08
c	ba	78	25	2e	1c	a6	b4	c6	e8	dd	74	1f	4b	bd	8b	8a
d	70	3e	b5	66	48	03	f6	0e	61	35	57	b9	86	c1	1d	9e
e	e1	f8	98	11	69	d9	8e	94	9b	1e	87	e9	ce	55	28	df
f	8c	a1	89	0d	bf	e6	42	68	41	99	2d	0f	b0	54	bb	16

Gambar 2.30 Tabel substitusi AES
[Sumber : Kurniawan, Yusuf. 2004. *Kriptografi Keamanan Internet dan Jaringan Telekomunikasi*, Bandung]

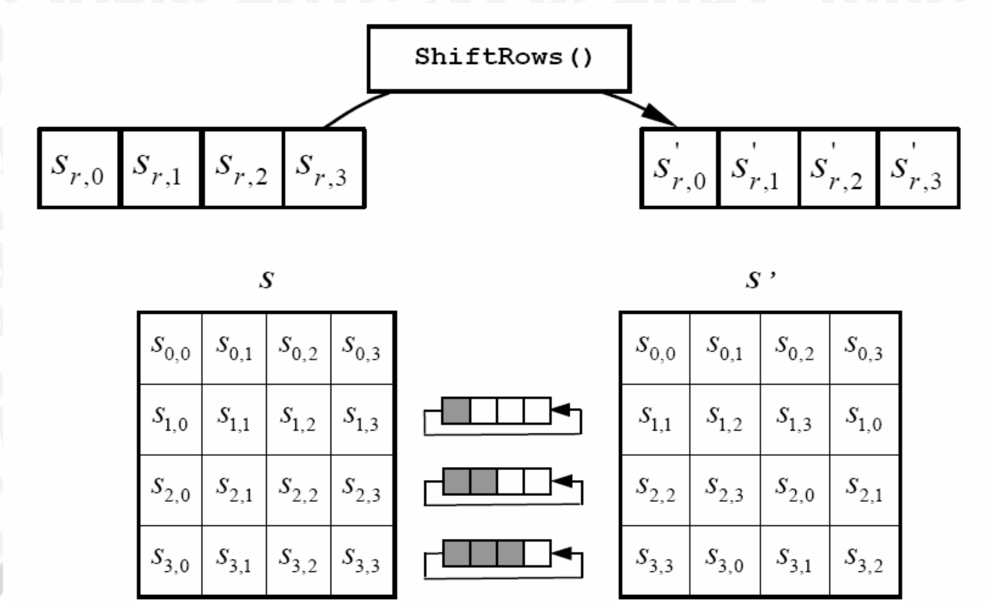
Tabel substitusi yang digunakan pada transformasi *SubByte* ditampilkan dalam bentuk heksadesimal seperti pada gambar 2.30. Misalnya, jika $s_{1,1}$ = {53}, maka nilai substitusinya akan ditentukan oleh perpotongan baris dengan indeks “5” dan kolom dengan indeks “3” seperti gambar 2.30. Ini akan menghasilkan $s'_{1,1}$ yang mempunyai nilai {ed}.

2. Transformasi *ShiftRows*

Pada transformasi *ShiftRow*, *byte-byte* pada 3 baris terakhir (baris 1, 2, dan 3) dari *state*, digeser secara memutar dengan jumlah pergeseran yang berbeda-beda.

Jumlah pergeseran bergantung pada nilai baris (r). Baris $r = 1$ digeser sejauh 1 *byte*, baris $r = 2$ digeser sejauh 2 *byte*, dan baris $r = 3$ digeser sejauh 3 *byte*. Baris pertama atau baris 0 tidak digeser.

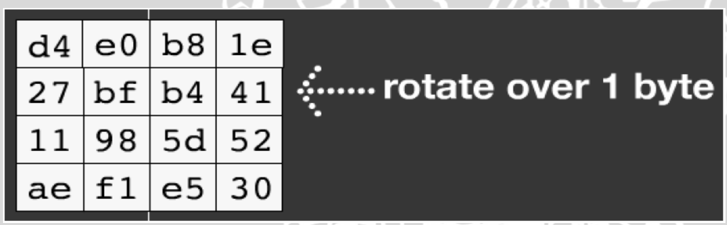
Gambar transformasi *ShiftRow* ditunjukkan pada gambar 2.31 berikut ini :



Gambar 2.31 Transformasi *ShiftRow* pada AES
[Sumber : Kurniawan, Yusuf. 2004. *Kriptografi Keamanan Internet dan Jaringan Telekomunikasi,* Bandung]

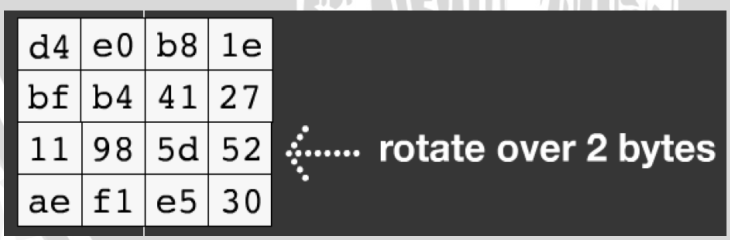
Penerapan pergeseran pada transformasi *ShiftRow* seperti di bawah ini :

1. Geser baris ke-1



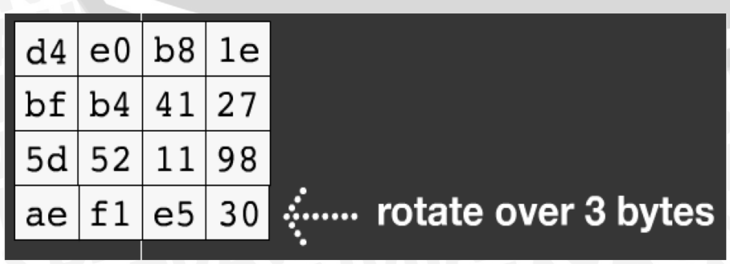
d4	e0	b8	1e
27	bf	b4	41
11	98	5d	52
ae	f1	e5	30

2. Hasil pergeseran baris ke-1 dan geser baris ke-2 :



d4	e0	b8	1e
bf	b4	41	27
11	98	5d	52
ae	f1	e5	30

3. Hasil pergeseran baris ke-2 dan geser baris ke-3 :



d4	e0	b8	1e
bf	b4	41	27
5d	52	11	98
ae	f1	e5	30

4. Hasil pergeseran akhir :

d4	e0	b8	1e
bf	b4	41	27
5d	52	11	98
30	ae	f1	e5

3. Transformasi *MixColumn*

Transformasi *MixColumn* mengalikan setiap kolom dari *array state* dengan polinom *a(x) mod* $(x^4 + 1)$.

a(x) yang ditetapkan adalah :

$$a(x) = \{03\}x^3 + \{01\}x^2 + \{01\}x + \{02\}$$

Transformasi ini dinyatakan sebagai perkalian matriks :

$$s'(x) = a(x) \otimes s(x)$$

$$\begin{bmatrix} s'_{0,c} \\ s'_{1,c} \\ s'_{2,c} \\ s'_{3,c} \end{bmatrix} = \begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \begin{bmatrix} s_{0,c} \\ s_{1,c} \\ s_{2,c} \\ s_{3,c} \end{bmatrix}$$

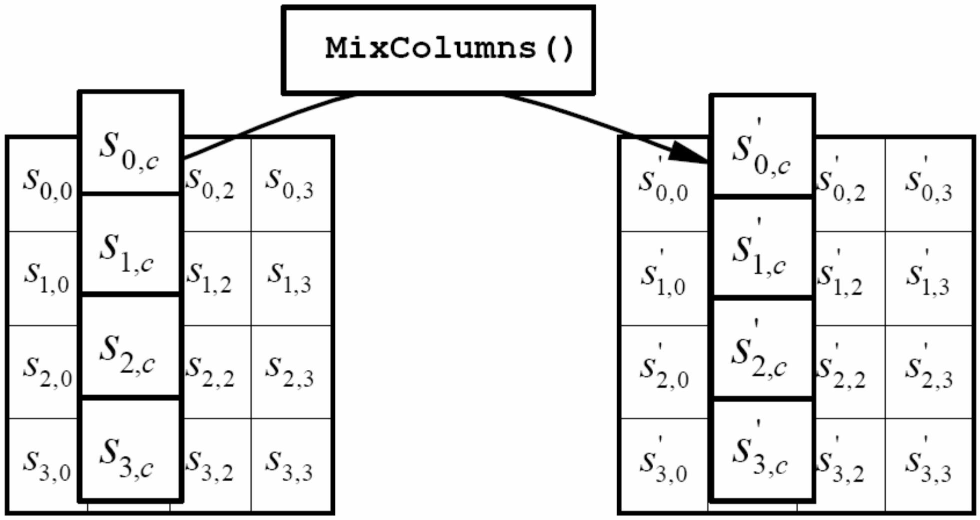
$$s'_{0,c} = (\{02\} \bullet s_{0,c}) \oplus (\{03\} \bullet s_{1,c}) \oplus s_{2,c} \oplus s_{3,c}$$

$$s'_{1,c} = s_{0,c} \oplus (\{02\} \bullet s_{1,c}) \oplus (\{03\} \bullet s_{2,c}) \oplus s_{3,c}$$

$$s'_{2,c} = s_{0,c} \oplus s_{1,c} \oplus (\{02\} \bullet s_{1,c}) \oplus (\{03\} \bullet s_{3,c})$$

$$s'_{3,c} = (\{03\} \bullet s_{0,c}) \oplus s_{0,c} \oplus s_{1,c} \oplus (\{02\} \bullet s_{3,c})$$

Gambar transformasi *ShiftRow* ditunjukkan pada gambar 2.32 berikut ini :



Gambar 2.32 Operasi *MixColomn* pada state per kolom
[Sumber : Kurniawan, Yusuf. 2004. *Kriptografi Keamanan Internet dan Jaringan Telekomunikasi*, Bandung]

Penerapan operasi transformasi *MixColomn* seperti di bawah ini:

1. Hasil transformasi *ShiftRows* sebelumnya :

d4	e0	b8	1e
bf	b4	41	27
5d	52	11	98
30	ae	f1	e5

2. Operasi *MixColumns* terhadap kolom pertama

$$\begin{bmatrix} d4 \\ bf \\ 5d \\ 30 \end{bmatrix} \bullet \begin{bmatrix} 02 & 01 & 01 & 03 \\ 03 & 02 & 01 & 01 \\ 01 & 03 & 02 & 01 \\ 01 & 01 & 02 & 03 \end{bmatrix} = \begin{bmatrix} 04 \\ 66 \\ 81 \\ e5 \end{bmatrix}$$

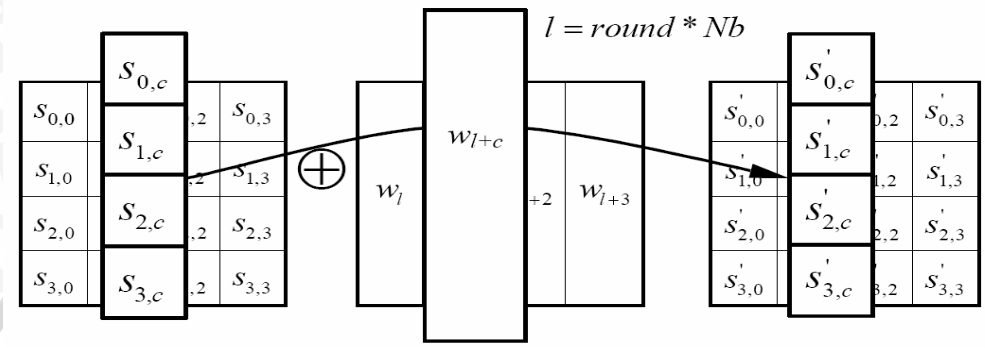
3. Hasil transformasi *MixColumns* seluruhnya :

04	e0	48	28
66	cb	f8	06
81	19	d3	26
e5	9a	7a	4c

4. Transformasi *AddRoundKey*

Transformasi ini melakukan operasi XOR terhadap sebuah *round key* dengan *array state*, dan hasilnya disimpan di *array state*.

Operasi *AddRoundKey* dengan meng-XOR kolom *state* dengan *subkey* ditunjukkan pada gambar 2.33 di bawah ini.



Gambar 2.33 Transformasi *AddRoundKey* kolom *state* dengan *subkey*
[Sumber : Kurniawan, Yusuf. 2004. *Kriptografi Keamanan Internet dan Jaringan Telekomunikasi*, Bandung]

Penerapan Transformasi *AddRoundKey* seperti di bawah ini :

1. Hasil transformasi *MixColumns* sebelumnya :

04	e0	48	28
66	cb	f8	06
81	19	d3	26
e5	9a	7a	4c

a0	88	23	2a
fa	54	a3	6c
fe	2c	39	76
17	b1	39	05

Round key

2. *XOR*-kan kolom pertama *state* dengan kolom pertama *round key* :

$$\begin{bmatrix} 04 \\ 66 \\ 81 \\ e5 \end{bmatrix} \oplus \begin{bmatrix} a0 \\ fa \\ fe \\ 17 \end{bmatrix} = \begin{bmatrix} a4 \\ 9c \\ 7f \\ f2 \end{bmatrix}$$

3. Hasil *AddRoundKey* terhadap seluruh kolom :

a4	68	6b	02
9c	9f	5b	6a
7f	35	ea	50
f2	2b	43	49

Proses XOR kolom *state* dengan *roundkey* :

1. Bilangan heksadesimal pada kolom pertama *state* dan kolom pertama *round key* diubah menjadi bilangan biner, kemudian dilakukan operasi XOR, sehingga menjadi :

   04 = 0000 0100

   A0 = 1010 0000

   ———————————— $\oplus$

   1010 0100

2. Hasil operasi XOR menghasilkan bilangan biner 1010 0100, dan bila diubah ke bilangan heksadesimal menjadi A4.

   Proses ini dilakukan mulai baris pertama sampai baris ke-4 pada kolom pertama. Selanjutnya hal yang sama dilakukan pada kolom kedua, kolom ketiga, dan kolom keempat.

Tabel kebenaran dan gerbang logika pada operasi XOR dapat dilihat pada Tabel 2.3 dan gambar 2.34 berikut ini.

Tabel 2.3 Tabel kebenaran XOR

Masukan		Keluaran
A	B	F
0	0	0
0	1	1
1	0	1
1	1	0

Gambar 2.34 Gerbang logika XOR

Sedangkan konversi bilangan heksadesimal ke bilangan biner dapat dilihat pada tabel 2.4 berikut ini.

Tabel 2.4 Tabel konversi bilangan heksadesimal ke bilangan biner

Heksadesimal	Biner
0	0000
1	0001
2	0010
3	0011
4	0100
5	0101
6	0110
7	0111
8	1000
9	1001
A	1010
B	1011
C	1100
D	1101
E	1110
F	1111