BAB II

LANDASAN TEORI

2.1 Jaringan Telekomunikasi

Komunikasi sebagai proses menampilkan, mengubah, menginterpretasikan, atau mengolah informasi antara manusia atau mesin. Proses ini melibatkan suatu pengiriman (*transmitter*), penerima (*receiver*), dan sebuah medium transmisi untuk tempat mengalirnya informasi. Sehingga jaringan telekomunikasi diartikan sebagai suatu sistem yang terbentuk dari interkoneksi fasilitas-fasilitas yang dirancang untuk membawa trafik dari beragam sumber telekomunikasi.

Perkembangan teknologi telekomunikasi terasa semakin cepat, terutama dengan pesatnya kemajuan teknologi komputer dan informatika. Dan seiring dengan bertambahnya tahun, komunikasi tanpa kabel (*wireless*) cukup diminati di berbagai negara sebagai salah satu solusi untuk mencukupi kebutuhan sarana telekomunikasi. Teknologi informasi dan komunikasi (infokom) berkembang semakin pesat didorong oleh *Internet protocol* (IP) dengan berbagai aplikasi baru dan beragam layanan multimedia. Infrastruktur infokom terdiri dari *public switched data network* (PSDN) dan *public switched telephone network* (PSTN), namun hingga kini tulang punggung infokom masih banyak berpijak pada jaringan PSTN. **PSTN** adalah singkatan dari ***Public Switched Telephone Network*** atau yang biasa disebut jaringan / saluran telepon konvensional yang menggunakan kabel. PSTN secara umum diatur oleh standar-standar teknis yang dibuat oleh ITU-T, dan menggunakan pengalamatan

E.163/E.164 (secara umum dikenal dengan nomor telepon). PSTN dilengkapi dengan telekomunikasi kabel interlokal dan lokal.

Pada tahun ini implementasi sistem komunikasi *wireless* sudah memasuki teknologi PCS(*Personal Communication System*)**[1].** Sistem ini dapat dimplementasikan atau diterapkan dengan berbagai teknologi. Adapun teknologi yang dimaksud adalah CDMA (*Code Division Multiple Access*). CDMA sebuah teknologi militer yang digunakan pertama kali pada Perang Dunia II oleh sekutu Inggris untuk menggagalkan usaha Jerman mengganggu transmisi mereka. Sekutu memutuskan untuk mentransmisikan tidak hanya pada satu frekuensi, namun pada beberapa frekuensi, sehingga menyulitkan Jerman untuk menangkap sinyal yang lengkap. Sehingga dapat dikatakan bahwa CDMA suatu sistem komunikasi *wireless* yang dipakai oleh para *mobile* operator, sistem ini menggunakan teknologi "*spread spectrum*" yang memberikan *access* pemakaian pada banyak pengguna pada frekuensi dan waktu yang sama, hal ini dapat dilakukan dengan pemberian kode unik untuk setiap komunikasi. CDMA juga menyediakan / memperbolehkan lebih banyak pengguna daripada sistem teknologi lainnya. Sejak itu CDMA digunakan dalam banyak sistem komunikasi, termasuk pada *Global Positioning System* (GPS) dan pada sistem satelit *OmniTRACS* untuk logistik transportasi. Dan CDMA juga menjanjikan solusi teknologi yang ekonomis untuk mempercepat penambahan PSTN.

2.2 Jaringan Komputer

Komputer yang tidak dihubungkan dengan komputer lain disebut *stand-alone*. Komputer yang berhubungan dengan komputer dan peralatan lain sehingga

membentuk suatu group disebut sebagai *network* (jaringan), sedangkan bagaimana komputer tersebut bisa saling berhubungan serta mengatur sumber yang ada disebut sebagai *networking* (sistem jaringan).

2.2.1 Protokol

Agar komputer dalam suatu jaringan dapat berkomunikasi, maka dibutuhkan suatu protokol atau suatu aturan standar komunikasi baik antar komputer maupun antar jaringan komputer. Protokol yang dibahas yaitu protokol TCP/IP (*Transmission Control Protocol / Internet Protocol*), karena TCP/IP dikembangkan untuk dapat diterapkan di segala jenis *platform* komputer, biasa dikenal dengan *open system.* Protokol untuk sistem jaringan dibagi menjadi dua bagian, yaitu:

1. Protokol komunikasi antara peralatan jaringan (*network interface card*) yang mengatur bentuk dan jenis data yang dikirim, apakah yang dikirim merupakan data atau sinyal untuk proses interup komunikasi; serta menentukan besaran listrik yang digunakan, jenis, dan banyaknya kabel yang dipakai untuk proses transmisi data jika menggunakan kabel sebagai media penghubung.
2. Protokol dari sistem operasi yang digunakan seperti *Netware* menggunakan protokol utamanya IPX/SPX, *Microsoft* menggunakan protokol *NetBIOS*, dan sekarang yang banyak digunakan dan menjadi protokol standar adalah protokol TCP/IP.

TCP/IP melakukan transmisi data per segmen, artinya paket data dipecah dalam jumlah yang sesuai dengan besaran paket, kemudian dikirim satu persatu hingga selesai. Agar pengiriman data sampai dengan baik, maka pada setiap paket

pengiriman, TCP menyertakan nomor seri (*sequence number*). Model protokol TCP disebut *connection oriented protocol*.

Internet Protokol menggunakan IP-Address sebagai identitas. Pengiriman data akan dibungkus dalam paket dengan label berupa IP-Address si pengirim dan si penerima. *IP-Address* terdiri atas 2 bagian, yaitu :

1. *Network* ID (Identitas Jaringan)
2. *Host* ID (Identitas Komputer)

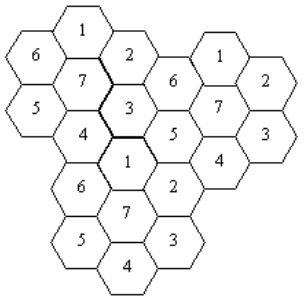
2.3 *Global System For Mobile Communication* (GSM)

2.3.1 Teknik Modulasi dan *Bandwidth* GSM

Teknik modulasi yang digunakan pada GSM adalah *Gaussian Minimum Shift Keying* (GMSK). Teknik ini bekerja dengan melewatkan data yang akan dimodulasikan melalui Filter Gaussian. Filter ini menghilangkan sinyal-sinyal harmonik dari gelombang pulsa data dan menghasilkan bentuk yang lebih bulat pada ujung-ujungnya. *Bandwidth* yang dialokasikan untuk tiap frekuensi pembawa pada GSM adalah sebesar 200 kHz.

2.3.2 Struktur Sistem Seluler

Pembagian area dalam kumpulan sel-sel merupakan suatu prinsip penting pada GSM sebagai sistem telekomunikasi selular. Sel-sel tersebut dimodelkan sebagai bentuk heksagonal seperti pada Gambar 2.1 yang terdapat pada halaman berikut :



Gambar 2. 1 Pembagian Area Sel Frekuensi GSM

Tiap sel tersebut mengacu pada satu frekuensi pembawa atau kanal tertentu. Pada kenyataannya jumlah kanal yang dialokasikan terbatas, sementara jumlah sel bisa saja berjumlah sangat banyak. Untuk memenuhi hal ini, dilakukan teknik pengulangan frekuensi (*frequency re-use*).

Jelas sekali bahwa semakin besar jumlah himpunan kanal, semakin sedikit jumlah kanal tersedia per-sel dan oleh karenanya kapasitas sistem menurun. Namun, peningkatan jumlah himpunan kanal menyebabkan jarak antara sel yang berdekatan kanal semakin jauh, dan ini mengurangi resiko terjadi interferensi sehingga desain sistem GSM memerlukan kompromi antara kualitas dan kapasitas nya.

Bagian paling rendah dari sistem GSM adalah *Mobile Station* (MS). Bagian ini berada pada tingkat pelanggan dan *portable*. Pada tiap sel terdapat *Base Transceiver Station* (BTS). BTS ini berfungsi sebagai *station* penghubung dengan MS dan merupakan sistem yang langsung berhubungan dengan *handphone*. BTS pada dasarnya hanya merupakan "pesuruh" saja. Otak yang mengatur lalu-lintas trafik di BTS adalah *Base Station Controller* (BSC). *Location Updating*, penentuan BTS dan proses *handover* pada percakapan ditentukan oleh BSC ini. Beberapa BTS pada satu region diatur oleh sebuah BSC. Seluruh BSC ini dihubungkan dengan *Mobile*

Switching Center (MSC). MSC merupakan pusat penyambungan yang mengatur jalur hubungan antar BSC maupun antara BSC dan jenis layanan telekomunikasi lain (PSTN, operator GSM lain, AMPS, dll). Saat ini teknik *switching* terus berkembang, dan begitu pula pada layanan GSM. Beberapa operator GSM di Indonesia telah menerapkan *Intelegent Network* lanjutan dalam teknik *switching*nya.

2.4 *Short Message Service* (SMS)

Short Message Service (SMS) merupakan sebuah layanan yang banyak diaplikasikan pada sistem komunikasi tanpa kabel, memungkinkan dilakukannya pengiriman pesan-pesan dalam bentuk *alphanumeric* antara terminal pelanggan dengan sistem eksternal seperti email, *paging, voice mail,* dan lain-lain. Isu pertama SMS pertama kali muncul dibelahan eropa pada sekitar tahun 1991 bersama sebuah teknologi komunikasi *wireless* yang saat ini cukup banyak penggunaannya, yaitu GSM.

Layanan SMS merupakan sebuah layanan yang bersifat *nonreal time* dimana sebuah *short message* dapat di *submit* ke suatu tujuan, tidak peduli apakah tujuan tersebut aktif atau tidak. Pada dasarnya sistem SMS akan menjamin *delivery* dari suatu *short message* hingga sampai ke tujuan. Kegagalan pengiriman yang bersifat sementara seperti tujuan tidak aktif akan selalu teridentifikasi sehingga pengiriman ulang *short message* akan selalu dilakukan, kecuali *short message* yang telah melampaui batas waktu tertentu dinyatakan gagal terkirim.

2.4.1 Karakteristik SMS

Selain sebagai media mengirim dan menerima pesan *alphanumeric*, SMS juga dapat digunakan sebagai pengangkat muatan biner (*binary payload*) dan mengimplementasikan tumpukan (*stack*) *wap* lewat *Short Message Service Center* (SMSC). Ada beberapa karakteristik pesan SMS yang penting Yaitu :

a. Prinsip kerja dari SMS ini adalah bahwa setiap jaringan mempunyai suatu *Service Center (SC)*. Pesan tidak langsung dikirimkan ke tempat tujuan, melainkan disimpan terlebih dahulu di SC. SC juga dijadikan sebagai *interface* antara *Public Land Mobile Network* (PLMN).
b. Tranmisi SMS dapat terjadi meskipun *Mobile Station* (MS) sedang melakukan komunikasi dengan MS yang lain. Hal ini dimungkinkan karena kanal radio untuk tranmisi *voice* telah ditentukan selama durasi pemanggilan sedangkan pesan SMS merambat pada kanal radio dengan memanfaatkan jalur *signaling*.
c. Pengiriman pesan yang menggunakan kanal *signaling* memiliki dua tipe yaitu :
    1. SMS *point to point* : menyediakan mekanisme untuk mengirimkan pesan hanya dari satu MS ke MS tertentu.
    2. SMS *Broadcast* (*point to multipoint*) : pengiriman SMS ke beberapa MS sekaligus.
d. Pesan dijamin sampai atau tidak sampai sama sekali, selayaknya *email*, sehingga apabila terjadi kegagalan sistem, *time-out*, atau hal lain yang menyebabkan pesan tidak diterima, akan diberikan informasi (*report*) yang menyatakan pesan gagal dikirim.

e. Berbeda dengan fungsi *call* (pemanggilan), sekalipun saat mengirimkan pesan MS tidak aktif atau diluar jangkauan *service area*, bukan berarti pengiriman pesan akan gagal, namum pesan akan masuk ke antrian dulu selama belum *time-out*, pesan akan segera dikirimkan jika MS sudah aktif atau sudah berada di *service area*.

2.4.2 Mekanisme Distribusi Pesan

Terdapat empat macam mekanisme distribusi pesan SMS oleh aplikasi SMS, yaitu:

a. *Pull*, yaitu pesan yang dikirimkan ke pengguna berdasarkan permintaan pengguna.
b. *Push – Event based*, yaitu pesan yang diaktivasi oleh aplikasi berdasarkan kejadian yang berlangsung
c. *Push - Schedule*, yaitu pesan yang diaktivasi oleh aplikasi berdasarkan waktu yang telah terjadwal.
d. *Push – Personal Profile*, yaitu pesan yang diaktivasi oleh aplikasi berdasarkan *profile* dan *preference* dari pengguna.

2.4.3 Elemen Dasar Jaringan SMS

Elemen dasar dari suatu jaringan SMS seperti berikut ini :

1. *Short Messaging Entities* (SME) disebut juga ESME, suatu piranti yang dapat menerima dan mengirim pesan pendek, entitas dalam sistem SMS yang dapat

berada pada jaringan, berupa perangkat bergerak, dan merupakan *service center* yang berada di luar jaringan.

2. *Short Message Service Center* (SMSC), entitas yang bertanggung jawab untuk menyimpan, *routing*, dan meneruskan *short message* antar SME dan piranti bergerak (*mobile phone).* Terminologi SMSC mengacu pada sesuatu yang berupa *hardware* dan *software*.
3. *Signaling System 7* (SS7), protokol *signalling* yang umum di gunakan dalam jaringan telepon seluler.
4. *Base Station System* (BSS), kesatuan sistem yang bertanggung jawab mengatur transmisi sinyal elektromagnetik untuk membawa data dari MSC ke perangkat telepon bergerak. *Base station* terdiri dari *Base Station Controller (*BSC) dan *Base Transceiver Station* (BTS).
5. MSC, sebuah sistem yang melakukan fungsi *switching* dan mengontrol panggilan telepon dalam suatu jaringan komunikasi bergerak. Berfungsi mengirimkan sebuah *short message* ke suatu tujuan tertentu melalui *base station* yang sesuai.
6. *Home Location Register* (HLR), *database* yang digunakan sebagai tempat penyimpanan permanen data, pengelolaan dan profil layanan pelanggan.
7. *Visitor Location Register* (VLR), *database* tempat menyimpan informasi temporal berisi data pelanggan yang berasal dari suatu HLR yang roaming ke HLR lainnya.

2.4.4 Elemen Layanan

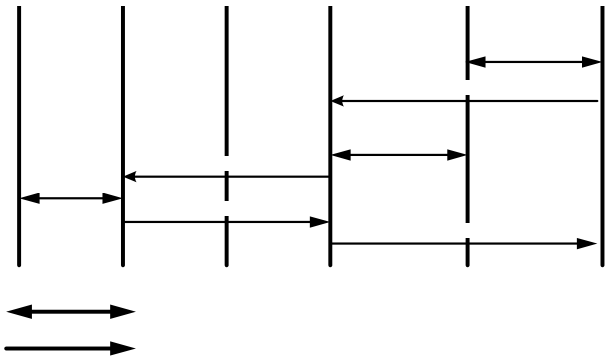
SMS terdiri dari beberapa elemen layanan yang relevan terhadap penerimaan dan pengiriman pesan pendek yaitu:

1. *Message Expiration*, SMSC akan menyimpan dan mencoba mengirimkan kembali pesan yang mengalami kegagalan sampai pengiriman tersebut berhasil.
2. *Priority*, Untuk memberi tanda pesan-pesan yang penting dan membedakannya dari pesan biasa.

Sistem SMS memiliki dua layanan dasar *point-to-point* bagi pelanggan yaitu:

a. *Mobile-Oriented* (MO) *Short Message*, dikirimkan dari *mobile phone* yang MO-*Capable* ke SMSC dan dapat ditujukan ke *mobile phone* lainnya. Pada layanan ini selalu ada laporan yang dikirimkan ke *mobile phone*, baik yang mengkonfirmasikan pengiriman pesan pendek ke SMSC ataupun mengkonfirmasikan kegagalan pengiriman dan mengidentifikasikan penyebabnya.

Gambar 2.2 dibawah ini merupakan skenario pengiriman *mobile oriented short message*:

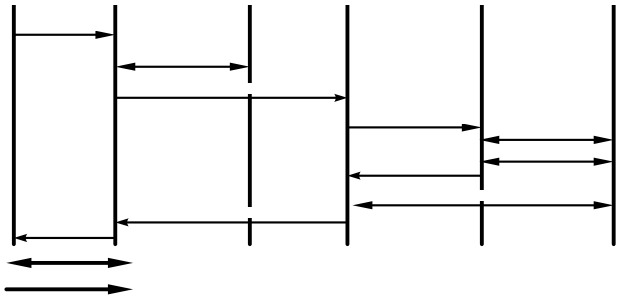


Gambar 2.2 Skenario Pengiriman MO-SM

Penjelasan dari Gambar 2.2 yaitu sebagai berikut :

1. MS mengirimkan SM ke MSC
2. MSC menginterogasi VLR untuk membuktikan bahwa pengiriman pesan tersebut tidak melanggar permintaan layanan pembatasan yang telah ditetapkan.
3. MSC mengirimkan pesan pendek ke SMSC dengan menggunakan operasi *Forward Short Message.*
4. SMSC mengirimkan pesan pendek ke SME
5. SMSC memberitahu MSC mengenai keberhasilan operasi *Forward Short Message.*
6. MSC mengembalikan hasil dari operasi MO-SM ke MS.

b. *Mobile Terminated* (MT) *Short Message*, dikirimkan dari SMSC ke *mobile phone* dan dapat sampai ke SMSC dari *mobile phone* lainnnya melalui MO-SM, pada layanan ini juga terdapat laporan yang diberikan kepada SMSC yang isinya bisa berupa konfirmasi pengiriman pesan pendek ke *mobile phone* maupun informasi kegagalan pengiriman pesan. Untuk lebih jelas, perhatikan Gambar 2.3 yaitu skenario pengiriman MT-SM :



Gambar 2.3 Skenario Pengiriman MT-SM

Penjelasan dari Gambar 2.3 yaitu sebagai berikut :

a. Pesan pendek dikirimkan dari SME ke SMSC.
b. Setelah menyelesaikan pengolahan internalnya, SMSC menginterogasi HLR dan menerima informasi *routing* untuk pelanggan *mobile*.
c. SMSC mengirimkan pesan pendek ke MSC dengan menggunakan operasi *Forward Short Message.*.
d. MSC mengambil informasi pelanggan dari VLR. Operasi ini dapat melibatkan prosedur autentifikasi.
e. MSC mengirimkan pesan pendek ke MS.
f. MSC mengembalikan hasil dari operasi *Forward Short Message* ke SMSC.
g. Jika diminta oleh SME, SMSC akan mengembalikan laporan status yang mengindikasikan pengiriman pesan pendek.

2.4.5 Jenis Aplikasi SMS

1. Aplikasi SMS untuk Konsumen Personal

Aplikasi untuk konsumen personal hingga saat ini masih mendominasi hingga 90% pengguna yang memakai aplikasi ini **[1]**, aplikasi ini antara lain yaitu:

a. Pesan SMS antar pengguna (*person to person messaging*)
b. Notifikasi *Voice* dan *Fax-Mail*
c. Notifikasi *e-mail* internet
d. *Unified Messaging,* merupakan penggabungkan tiga macam *messaging* yaitu *voicemail, faxmail*, dan *e-mail*, dalam satu *accoun*t *unified messaging box*.

Pusat informasi merupakan layanan yang menyediakan informasi umum dan penting bagi pengguna. Informasi disajikan melalui dua mekanisme, yaitu *push-based* dimana informasi diaktivasi oleh aplikasi dan *pull-based* yaitu informasi diminta (*request*) oleh pengguna.

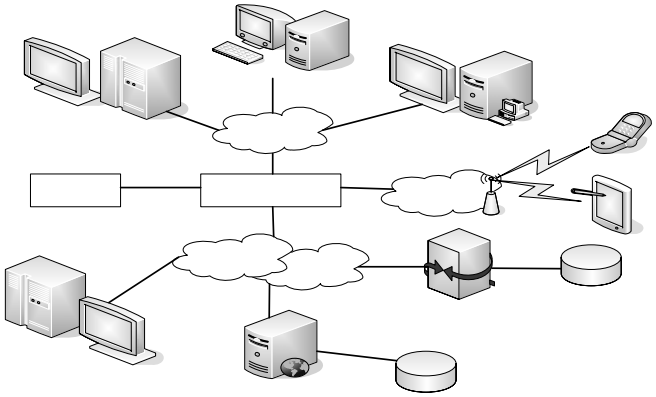
2. Aplikasi SMS untuk Korporat.

Aplikasi SMS untuk korporat adalah aplikasi SMS yang dimodifikasi berdasarkan kebutuhan terhadap pelayanan informasi dan komunikasi dalam sebuah perusahaan atau kelompok orang. Aplikasi yang dapat dikembangkan antara lain:

a. *E-mail* Korporat adalah layanan bagi karyawan perusahaan yang memiliki *account* di *e-mail server* perusahaan untuk dapat memantau datangnya *e-mail* melalui pesan SMS.
b. Program *Affinity,* merupakan jenis layanan yang pada awalnya merupakan kerja sama dari *operator network* dengan perusahaan-perusahaan yang memiliki pelanggan cukup besar, layanan ini pada dasarnya merupakan bagian dari pelayanan terhadap konsumen atau *customer service*.
c. *Mobile Banking*, merupakan salah satu proggram *affinity* untuk layanan perusahaan perbankan. Layanan ini memberikan kemudahan kepada pelanggan nasabah sebuah bank dalam bertransaksi melalui rekeningnya
d. *E-Commerce*, merupakan perdagangan elektronik dimana transaksi perdagangannya dapat dilakukan melalui pesan SMS.
e. Penentuan lokasi (*Positioning*), aplikasi ini mengintegrasikan aplikasi G*lobal Positioning System* (GPS) yang berbasis satelit dengan pesan melalui SMS yang dapat memberitahukan kepada orang lain mengenai keberadaan seseorang.

f. *Remote Monitoring*, layanan dibangun dengan aplikasi yang dapat secara otomatis melaporkan kejadian dimana kinerja suatu alat mencapai titik kritis tertentu, maka pada saat itu juga aplikasi akan secara elektronis segera mengirim pesan pemberitahuan melalui SMS ke *handset administrator* atau penanggung jawab alat tersebut.

Dari aplikasi SMS yang diuraikan diatas, Gambar 2.4 berikut merupakan infrastruktur jaringan inovatif korporat.



Gambar 2. 4 Infrastruktur Jaringan Inovatif

2.5 Pengiriman Paket Data SMS

2.5.1 Arsitektur Jaringan SMS

Untuk implementasi layanan SMS, operator menyediakan apa yang disebut sebagai *SMS Center* (SMSC). Secara fisik SMSC dapat berwujud PC biasa yang mempunyai interkonektivitas dengan jaringan GSM, salah satu implementasi SMSC *Open Source* adalah Kannel, yang digunakan untuk membangun WAP dan SMS *Gateway*. Perhatikan Gambar 2.5 pada halaman selanjutnya, merupakan arsitektur dasar dari jaringan SMS :

PC

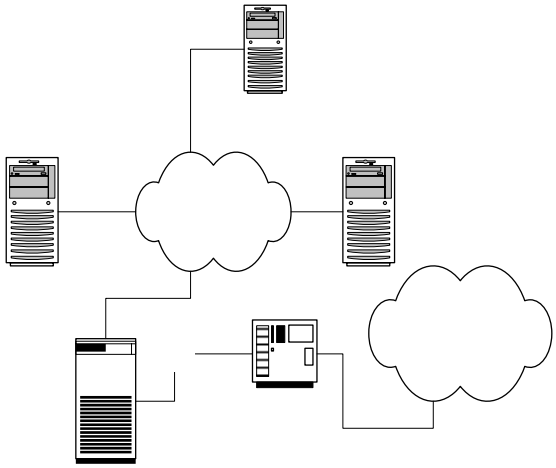
Operator

Wireli
Netwo

CCBS

Short Mes
Service C

Corporate
Intranet



Gambar 2.5 Arsitektur Dasar Jaringan SMS

2.5.2 *Short Message Peer – To – Peer Protocol* (SMPP)

SMPP, merupakan sebuah protokol standar industri yang digunakan dalam pertukaran *short message* antara *External Short Messaging Entity* (ESME), *Routing Entity* (RE), dan *Message Center* (MC). *Message center* merupakan terminologi generik untuk menyebutkan beberapa entitas seperti SMSC, GSM *Unstructured Supplementary Services Data* (USSD) *server*. ESME, entitas yang berada di luar jaringan komunikasi *wireless* seperti WAP *Proxy Server*, Email *Gateway*, atau *Voice Mail Server*. *Routing Entity* bertindak sebagai emulator entitas dalam komunikasi antara *message center* dan ESME, *routing entity* bagi ESME terlihat sebagai MC dan sebaliknya.

Protokol SMPP merupakan sebuah protokol yang berjalan pada lapisan aplikasi, seperti halnya protokol-protokol lain dalam konteks komunikasi data dalam jaringan komputer. Satuan paket data yang dipertukarkan pada lapisan aplikasi dalam protokol SMPP disebut PDU (*Protokol Data Unit*).

2.5.3 *Protocol Data Unit* (PDU)

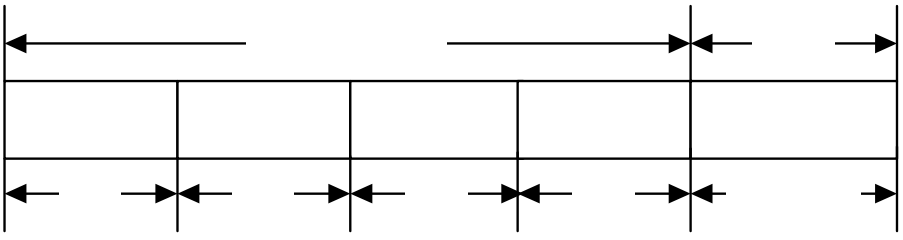
Satuan paket data yang dipertukarkan pada lapisan aplikasi dalam protokol SMPP disebut *Protocol Data Unit* (PDU). Dalam protokol tersebut terdapat beberapa macam format PDU dimana penggunaan masing-masing PDU tersebut harus sesuai dengan fungsinya. Sebagai contoh untuk mengirim *short message*, harus digunakan PDU dengan format ***submit_sm, deliver_sm,*** atau ***data_sm.***

Umumnya cara pengiriman paket data dari satu titik ke titik lain, salah satu titik harus bertindak sebagai *server* dan titik lainnya sebagai *client*, Inisiatif dan pembentukan sebuah *session* (jenis permintaan atau perintah) dilakukan oleh *client*. Jenis session yang dipilih sepenuhnya diserahkan kepada *client* (otorisasi diterima atau tidak tetap dipegang oleh *server*), terdapat tiga buah *session* yang dapat dipilih yaitu:

1. *Receiver* (RX), bila *client* ingin dapat menerima paket data.
2. *Transmitter* (TX), bila *client* ingin dapat mengirimkan paket data.
3. *Transceiver* (TRX), bila *client* ingin dapat mengirim dan menerima paket data.

2.5.4 Format Umum PDU

Secara umum format PDU dalam protokol SMPP adalah sebagai berikut:



Gambar 2.6 Format Umum PDU

Tabel 2.1 Format PDU

	SMPP PDU Field	Size (Octets)	Type	Description
PDU HEADER	*Command_length*	4	Integer	Overall size of PDU Including header and body
	Command_id	4	Integer	Identifies the PDU
	Command_status	4	Integer	Use to carry an error code
	Sequence_number	4	Integer	Use to uniquely identified PDU session
BODY	Standard Parameters	Var.	Mixed	The body part of PDU
	TLV Parameter	Var.	mixed	

Perhatikan Gambar 2.6, Enambelas oktet pertama disebut PDU *header*, merupakan bagian yang bersifat mandatori atau harus selalu ada dalam setiap PDU. Sisanya disebut PDU *Body*, merupakan bagian yang bersifat opsional (tergantung jenis PDU). Body PDU terdiri dari parameter standar dan parameter tambahan yang disebut parameter *Tag-Length_Value* (TLV), berikut penjelasan masing-masing bagian tersebut :

1) *command_length*

Command_length menyatakan panjang yang sesungguhnya dari PDU meliputi PDU Header dan PDU Body, termasuk didalamnya oktet dari *command_length* sendiri. Posisi nya terletak pada awal atau field pertama dari setiap PDU.

2) *Command_id*

command_id merupakan parameter yang mengindikasikan jenis operasi dari protokol SMPP yang sedang dilakukan. Parameter ini dikodekan dalam 4 oktet dengan tipe data integer. Nilai parameter ini berkisar antara 0x00000000 hingga 0x00000001FF untuk parameter yang termasuk kategori *request*, kategori respons nilainya berkisar antara 0x80000000 hingga 0x800001FF. Berikut nilai dari beberapa command_id :

Tabel 2.2 Nilai command_id

Command_id	**Nilai**	**Command_id**	**Nilai**
Bind_receiver	0x00000001	*Broadcast_sm*	0x00000111
Bind_transmitter	0x00000002	*Bind_receiver_resp*	0x80000001
Query_sm	0x00000003	*Query_sm_resp*	0x80000003
Submit_sm	0x00000004	*Submit_sm_resp*	0x80000004
Deliver_sm	0x00000005	*Deliver_sm_resp*	0x80000005
Unbind	0x00000006	*Unbind_resp*	0x80000006
Replace_sm	0x00000007	*replace_sm_resp*	0x80000007
Cancel_sm	0x00000008	*cancel_sm_resp*	0x80000008
Bind_transceiver	0x00000009	*Data_sm_resp*	0x80000103
Outbind	0x0000000B	*Broadcast_sm_resp*	0x80000111
Data_sm	0x00000103	*Query_broadcast_sm_resp*	0x80000112

3) *command_status*

command_satus merupakan paramater yang menunjukkan status operasi dalam protokol dan hanya relevan untuk PDU-PDU kategori *respons*. Untuk PDU-PDU kategori *request*, parameter ini diabaikan.

4) *sequence_number*

sequence_number merupakan parameter yang digunakan untuk menandai sebuah PDU secara unik agar dapat dibedakan dengan PDU lain. Mekanisme pembangkitannya direkomendasikan sesuai dengan namanya, berupa bilangan bulat yang *monotonically increasing* dan dimulai dari angka 1 untuk setiap session yang ada.

5) Parameter standar

Parameter standar merupakan parameter yang terdapat pada PDU *Body* pada PDU-PDU tertentu (PDU yang *non-header only*, yaitu PDU *submission* dan *delivery*). Formatnya sendiri bervariasi tergantung PDU-nya dan merupakan kombinasi data dengan tipe integer, C-Octet String, atau Octet String.

6) Parameter TLV

Tag-Length-Value, merupakan parameter dalam protokol yang dapat dibongkar-pasang sesuai dengan kebutuhan. Satu-satunya syarat hanyalah parameter ini, bila disertakan, harus diletakkan setelah paramater standar.

2.5.5 Penggunaan Kode PDU

Langkah-langkah untuk menentukan kode PDU yang dibutuhkan untuk mengirimkan *(send)* SMS ke SMS *Center* :

a. Nomor SMS Center

Terdiri dari tiga *subheader*, yaitu:

1. Jumlah pasangan heksa desimal SMS *Center* dalam bilangan heksa.

2. Kode nasional dan kode internasional, nomor kode nasional yang digunakan adalah 81 sedangkan nomor kode internasional adalah 91.
3. Nomor SMS *Center*, dalam pasangan bilangan heksa yang saling dipertukarkan dengan aturan tertentu, jika tersisa satu angka heksa yang tak memiliki pasangan maka angka tersebut dipasangkan dengan huruf F didepannya.

Contoh konversi nomor ponsel kedalam kode PDU dengan menggunakan :

1. Kode Nasional

   SMS Center menggunakan nomor 0856000000 maka :

   a. Terdapat 6 pasang angka heksa desimal.

   b. Kode nasional 81, ada 1 pasang

   c. 80-56-00-00-00

   Maka kode PDU yang didapat : 06818056000000

2. Kode Internasional

   SMS Center menggunakan nomor 62811000000, maka:

   a. Terdapat 7 pasang angka heksa desimal

   b. Kode internasional 91, ada 1 pasang

   c. 26-18-01-00-00-F0

   Maka kode PDU yang didapat : 07912618010000F0

   Berikut ini tertera beberapa nomor SMS-*Center* operator selular di Indonesia :

Cara 1 :

No	Operator Selular	SMS-*Center* No	Kode PDU
1	Telkomsel	0811000000	06818011000000
2	Satelindo	0816125	0581806121F5
3	Excelcom	0818445009	06818081440590
4	Indosat-M3	0855000000	06818055000000

Cara 2 :

No	Operator Selular	SMS-*Center* No	Kode PDU
1	Telkomsel	6281000000	07912618010000F0
2	Satelindo	62816125	059126181652
3	Excelcom	62818445009	07912618485400F9
4	Indosat-M3	62855000000	07912658050000F0

b. Tipe SMS, untuk pengiriman atau *send* tipe SMS adalah 1 dalam heksa 01

c. Nomor referensi SMS, nomor ini dibiarkan dulu 0 atau dalam heksa 00, ponsel secara otomatis akan memberi nilai nomor referensinya.

d. Nomor ponsel penerima, terdiri atas tiga bagian *subheader* yaitu:

    1. Jumlah bilangan desimal ponsel yang dituju dalam bilangan heksa
    2. Kode nasional atau kode internasional, kode *subheader* nasional adalah 81 dan internasional adalah 91.
    3. Nomor ponsel yang dituju dalam pasangan heksa yang saling dipertukarkan menurut aturan tertentu.

Contoh untuk nomor ponsel yang dituju adalah : 085221960301, maka konversi kedalam heksa desimal yaitu dengan cara seperti yang dijabarkan berikut.

1. Kode Nasional:

   a. terdapat 12 angka, berarti dalam heksa adalah 0C

   b. kode nasional adalah 81

   c 80-25-12-69-03-01

   Maka kode *subheader* PDU yang didapat adalah : 0C81802512690301

2. Kode Internasional

   a 62 81 32 12 17 32 6

   b. Terdapat 13 angka, berarti dalam heksa adalah 0D

   c. Kode internasional adalah 91

   d. 261823212732F6

   Maka kode *subheader* PDU yang didapat adalah : 0D91261823212732F6

e. Bentuk SMS

   00 : dikirim sebagai SMS

   01 : dikirim sebagai Telekomunikasi

f. Skema *encoding* data *Input* dan *Output* (I/O)

   Terdapat dua skema yaitu ;

   1. Skema 7 bit, ditandai dengan angka 00
   2. Skema 8 bit, ditandai lebih besar dari nol (dalam heksa)

g. Jangka Waktu atau validasi sebelum SMS *expired* atau kadaluarsa, jika bagian ini diloncat itu berarti berlakunya SMS tidak dibatasi, sedangkan jika diisi dengan suatu bilangan integer yang kemudian diubah ke dalam bilangan heksa, maka bilangan tersebut mewakili jumlah waktu validasi SMS tersebut.

Berikut Tabel 2.3 merupakan validitas waktu SMS

Tabel 2.3 Tabel Validitas Waktu SMS

Integer (INT)	**Jangka Waktu Validasi**
0-143	(INT+1)x 5 menit (berarti 5 sampai dengan 12 jam)
144-167	12 jam + (INT-143) x 30 menit
168-196	(INT-166) x 1 hari
197-255	(INT-192) x 1 minggu

h. Isi SMS

Terdiri dari dua subheader yaitu:

1. Panjang Isi (Jumlah huruf dalam SMS), misal untuk kata “hello” terdiri dari 5 huruf.
2. Isi berupa pasangan bilangan heksa desimal, skema 7 bit dapat dilihat pada Tabel 2.4 dibawah ini.

i. Tanggal dan waktu SMS di-*stamp* di SMS *Center* diwakili oleh 12 bilangan heksa (6 pasang) yang berarti YY/MM/DD hh:mm:ss

Contoh:

207022512308 02/07/22 12:32:08 22 Juli2002 15:23:08 WIB

Perhatikan Tabel 2.4 yang terdapat pada halaman selanjutnya, dimana merupakan tabel konversi dari heksadesimal :

Tabel 2.4 Tabel konversi heksa desimal

				B7	0	0	0	0	1	1	1	1
				B6	0	0	1	1	0	0	1	1
				B5	0	1	0	1	0	1	0	1
B4	**B3**	**B2**	**B1**		**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**
0	0	0	0	**0**	@	Δ	SP	0	-	P		p
0	0	0	1	**1**			!	1	A	Q	a	q
0	0	1	0	**2**	$	Φ	“	2	B	R	b	r
0	0	1	1	**3**		г	#	3	C	S	c	s
0	1	0	0	**4**				4	D	T	d	t
0	1	0	1	**5**			%	5	E	U	e	u
0	1	1	0	**6**			&	6	F	V	f	v
0	1	1	1	**7**			.	7	G	W	g	w
1	0	0	0	**8**			(	8	H	X	h	x
1	0	0	1	**9**			)	9	I	Y	i	y
1	0	1	0	**10**	LF		*	:	J	Z	j	z
1	0	1	1	**11**			+	;	K		k	
1	1	0	0	**12**			‘	<	L		l	
1	1	0	1	**13**	CR		_	=	M		m	
1	1	1	0	**14**				>	N		n	
1	1	1	1	**15**			/	?	O		o	

Ada 2 langkah yang harus kita lakukan untuk mengkonversikan isi SMS , yaitu :

Langkah pertama : mengubahnya menjadi kode 7 bit

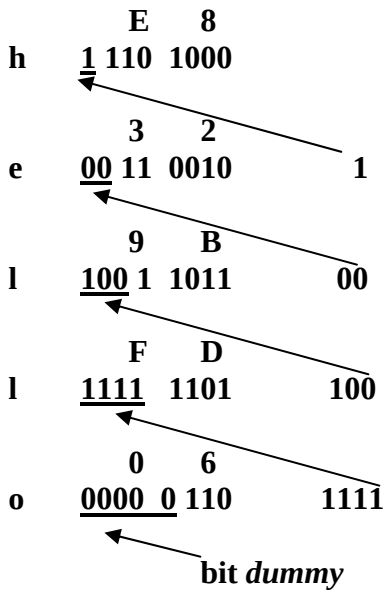
Langkah kedua : mengubah kode 7 bit menjadi 8 bit yang diwakili oleh pasangan heksa.

Contoh untuk kata “hello”

Langkah pertama

Bit	**7**	**1**
h	110	1000
e	110	0101
l	110	1100
l	110	1100
o	110	1111

Langkah kedua



Sehingga hasil konversi kata "hello" ke bilangan heksa adalah **E8329BFD06**

Oleh karena total 7 bit x 5 huruf = 35 bit, sedangkan yang kita perlukan untuk mengubah ke 8 bit adalah 8 bit x 5 huruf = 40 bit, maka diperlukan 5 bit *dummy* yang diisi bilangan 0.

Setelah masing-masing *header* dan *subheader* untuk mengirim pesan pesan dipecahkan, maka *header-header* diatas digabung menjadi sebuah PDU lengkap. Seperti contoh untuk mengirim kata "Hello"ke MS nomor 628129573337 lewat SMS Center Exelcom tanpa membatasi jangka waktu valid, maka PDU lengkapnya: **07912618485400F901000C9126I892753373000005E8329BFD06**.

2.5.6 AT-*Command*

AT-*Command* atau *Attention Command* yaitu perintah AT (Hayes AT-*Command)* yang digunakan untuk berkomunikasi dengan terminal (modem) melalui

gerbang serial pada komputer. Dengan penggunaan perintah AT, dapat diketahui atau dibaca kondisi dari terminal, seperti mengetahui kondisi sinyal, kondisi baterai, mengirim pesan, membaca pesan, menambah item pada daftar telepon, dan sebagainya. Beberapa jenis ponsel memiliki *extended* AT *Command* yang bisa digunakan untuk mengambil informasi jenis, model hp, nomor *Internasional Mobile Station Equipment Identity* (IMEI) , SIM *Subscriber Identification Number* (IMSI), status baterai, kekuatan sinyal, nama operator, lokasi dan cell ID. Pada tabel 2.5 berikut diperlihatkan beberapa jenis perintah Hayes yang berhubungan dengan penanganan pesan-pesan AT-Command GSM versi 07.07.

Tabel 2.5 Perintah AT-Command pada GSM Versi 07.07

AT-Command	**Singkatan**	**Fungsi**
ATE1	*Activate Command*	Mengaktivasi At-Command 07.07
AT+C.....	*Attention + Command.....*	Awal perintah hayes untuk....
AT+COPS	*Operator Selection*	Memilih operator jaringan
AT+CLCK	*Lock*	Menampilkan penguncian telepon
AT+CBC	*Battery Charge*	Menampilkan level batere
AT+CSQ	*Signal Quality*	Menampilkan kualitas sinyal
AT+CCLK	*Clock Mode*	Pengaturan Jam
AT+CPBR	*Phone Book Read*	Membaca daftar buku telepon
AT+CPBS	*Phone Book Selection*	Menampilkan isi buku telepon
AT+CCSA	*Service Center Address*	Menampilkan Lokasi *Service Center*
AT+CMGS	*Message Get Send*	Mengirimkan SMS
AT+CMGL	*Message Get List*	Membaca isi *inbox* dan *outbox* SMS

Keterangan :

Perintah AT-Command selanjutnya dapat dilihat di **Lampiran I**.

2.6 Kriptografi

Kriptografi (*cryptography*) berasal dari bahasa yunani: "*cryptos"* artinya "*secret"* (rahasia), sedangkan "*graphein"* artinya *"writing"* (tulisan). Jadi kriptogarfi berarti "*secret writing"* (tulisan rahasia). Sehingga Kriptografi adalah ilmu dan seni untuk menjaga keamanan pesan *(Cryptography is the art and science of keeping messages secure)* atau ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan, integritas data, serta otentikasi.

Berikut istilah atau termonologi di dalam kriptografi, yaitu:

a. Pesan, *Plaintext,* dan *Ciphertext*

Pesan *(message)* adalah data atau informasi yang dapat dibaca dan dimengerti maknanya. Nama lain pesan yaitu *Plaintext* atau teks-jelas *(Cleartext).* Pesan yang dikirim dapat berupa data atau informasi. pesan yang tersimpan tidak hanya berupa teks, tetapi dapat berbentuk citra (*image),* suara/bunyi, video atau berkas biner.

Agar pesan tidak dapat dimengerti maknanya, pesan disandikan ke bentuk lain yang tidak dapat dipahami. Bentuk pesan yang tersandi disebut *Ciphertext* atau *Cryptogram.* Cipherteks harus dapat ditransformasikan kembali menjadi plainteks semula agar pesan yang diterima bisa dibaca.

b. Pengirim dan Penerima

Komunikasi data melibatkan pertukaran pesan antara dua entitas. **Pengirim** (*sender)* adalah entitas yang mengirim pesan kepada entitas lainnya.

Penerima (*receiver)* adalah entitas yang menerima pesan. Entitas dapat berupa orang, mesin (komputer), kartu kredit, dan lain-lain.

c. *Encryption* dan *Decryption*

Enkripsi (*encryption*) proses menyandikan plainteks menjadi Cipherteks. Sedangkan dekripsi (*Decryption*) proses mengembalikan Cipherteks menjadi plainteks semula. Enkripsi dan dekripsi dapat diterapkan pada pesan yang dikirim maupun yang tersimpan. Istilah *encryption of data in motion* mengacu pada enkripsi pesan yang ditransmisikan melalui saluran komunikasi, sedangkan istilah *encryption of data at-rest* mengacu pada enkripsi dokumen yang disimpan di dalam *storage.*

d. Cipher dan kunci

Algoritma kriptografi disebut *Cipher* yaitu aturan untuk *enciphering* dan *deciphering* atau fungsi matematika yang digunakan untuk enkripsi dan dekripsi. Berikut rumus matematis :

Fungsi enkripsi *E* memetakan *P* (plainteks) ke *C* (Cipherteks),

$E(P) = C$

Fungsi dekripsi *D* memetakan *C* ke *P*,

$D(C) = P$

Karena proses enkripsi kemudian dekripsi mengembalikan ke pesan asal, maka persamaannya seperti berikut :

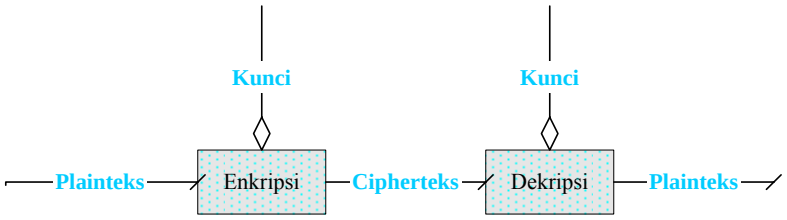
$D(E(P)) = P$

Keamanan kriptografi tidak ditentukan dengan menjaga kerahasiaan algoritmanya, tetapi dengan penggunaan kunci yang kerahasiaannya harus

dijaga. **Kunci** (*key)* adalah parameter yang digunakan untuk transformasi *enciphering* dan *deciphering.* Dengan menggunakan kunci *K,* maka fungsi enkripsi dan dekripsi :

$E_k(P) = C$ dan $D_k(C) = P$, dan memenuhi fungsi $D_k(E_k(P)) = P$.

Gambar 2.7 dibawah ini merupakan skema dari proses enkripsi dan dekripsi.



Gambar 2.7 Skema Enkripsi dan Dekripsi

e. Sistem Kriptografi

Sistem kriptografi (*cryptosystem)* merupakan kumpulan yang terdiri dari algoritma kriptografi, semua plainteks dan cipherteks yang mungkin, dan kunci. Dalam sistem kriptogarfi, *cipher* hanyalah salah satu komponen saja.

f. Penyadap

Penyadap (*eavesdropper*) adalah orang yang mencoba menangkap pesan selama ditransmisikan. Tujuan penyadap adalah mendapatkan informasi sebanyak-banyaknya mengenai sistem kriptografi yang digunakan untuk berkomunikasi dengan maksud memecahkan Cipherteks.

2.6.1 Tujuan Kriptografi

Kriptografi bertujuan untuk memberi layanan keamanan, ada empat macam kemanan yaitu :

a. Kerahasiaan (*Confidentiality)*, layanan yang ditujukan untuk menjaga agar pesan tidak dapat dibaca oleh pihak yang tidak berhak.
b. Integritas Data *(Data Integrity),* layanan yang menjamin bahwa pesan masih asli / utuh atau belum pernah dimanipulasi selama pengiriman
c. Otentikasi *(Authentication)*, layanan yang berhubungan dengan identifikasi, baik mengidentifikasi kebenaran pihak-pihak yang berkomunikasi (*User Authentication* atau *Entity Authentication*) maupun mengidentifikasi kebenaran sumber pesan (*Data origin authentication*).
d. Nirpenyangkalan (*Non-Repudiation*), layanan untuk mencegah entitas yang berkomunikasi melakukan penyangkalan, yaitu pengirim pesan menyangkal melakukan pengiriman atau penerima pesan menyangkal telah menerima pesan.

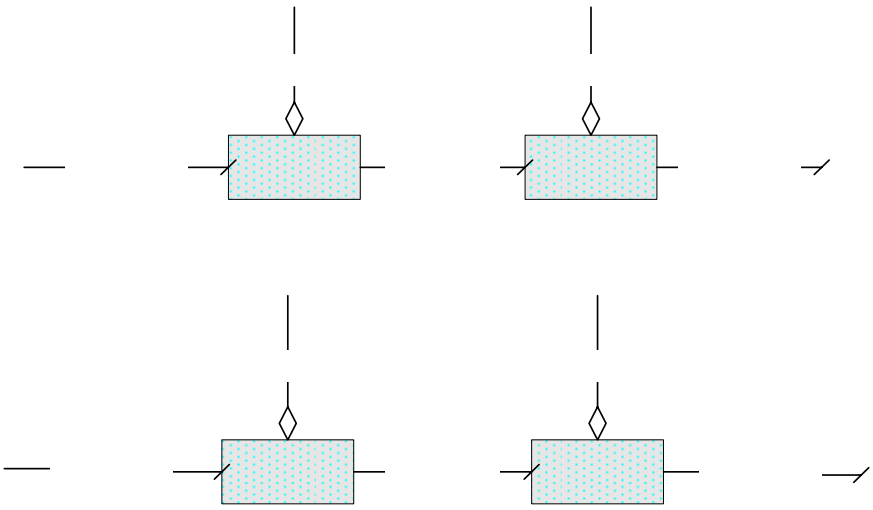
2.6.2 Kriptografi Kunci-Simetri dan Asimetri

Berdasarkan kunci yang digunakan untuk enkripsi dan dekripsi, kriptografi dibedakan menjadi Kriptografi Kunci-Simetri (*Symmetric-Key Cryptography*) dan Kriptografi kunci Asimetri (*Asymmetric-Key Cryptography).*

Kriptografi simetri mengasumsikan pengirim dan penerima pesan sudah berbagi kunci yang sama sebelum bertukar pesan, dan keamanannya terletak pada kerahasiaan kuncinya. Algoritma kriptografi modern yang termasuk kriptografi modern seperti *DES (Data Encryption Standard), Blowfish, Twofish, IDEA, AES (Advanced Encryption Standard).* Kelemahan dari kriptografi simetri baik pengirim

maupun penerima pesan harus memiliki kunci yang sama, sehingga pengirim pesan harus mencari cara yang aman untuk memberitahukan kunci kepada penerima pesan.

Kunci untuk enkripsi tidak sama dengan kunci untuk dekripsi disebut kriptografi Asimetri. Kunci untuk enkripsi tidak rahasia dan dapat diketahui oleh siapapun, dan kunci untuk dekripsi hanya diketahui oleh *receiver*. Pada kriptografi ini setiap yang berkomunikasi mempunyai sepasang kunci privat dan kunci publik. Pengirim mengenkripsi pesan dengan menggunakan kunci publik *receiver*. Hanya *receiver* yang dapat mendeskripsi pesan karena hanya *receiver* yang mengetahui kunci privatnya. Dari penjelasan diatas, perhatikan skema kriptografi simetri dan asimetri pada Gambar 2.8 dibawah ini :



Gambar 2.8 A: Skema Kriptografi Simetri

B: Skema Kriptografi Asimetri

2.6.3 Serangan Terhadap Kriptografi

Serangan (*attack*) adalah setiap usaha (*attempt*) atau percobaan yang dilakukan oleh kriptanalis untuk menemukan kunci atau menemukan plainteks dari Cipherteksnya dan disebut tujuan dari **kriptanalisis.**

1) Kriptanalisis

   Kriptanalisis berusaha menemukan kelemahan dari sistem kriptografi yang pada akhirnya mengarah untuk menemukan kunci dan mengungkap plainteks.

2) Keamanan Algoritma Kriptografi

   Lars Knudsen mengelompokkan hasil kriptanalisis ke dalam beberapa kategori berdasarkan jumlah dan kualitas informasi yang berhasil ditemukan, seperti berikut:

   a. Pemecahan total (*total break*). Kriptanalis menemukan kunci *K* sedemikian sehingga dekripsi $D_K\ (C) = P$.
   b. Deduksi (penarikan kesimpulan) global (*global deduction*). Kriptanalis menemukan algoritma alternatif, *A* yang ekivalen dengan $D_K\ (C)$ tetapi tidak mengetahui kunci *K*.
   c. Deduksi lokal (*instance / local deduction*). Kriptanalis menemukan plainteks dan cipherteks yang disadap.
   d. Deduksi informasi (*information deduction*). Kriptanalis menemukan beberapa informasi perihal kunci atau plainteks.

Sebuah algoritma kriptografi dikatakan **aman mutlak tanpa syarat** (*unconditionally secure*) bila cipherteks yang dihasilkan oleh algoritma tersebut tidak

mengandung cukup informasi untuk menentukan plainteksnya. Artinya, cipherteks sebanyak berapapun yang dimiliki kriptanalis tidak memberikan informasi yang cukup mendeduksi plainteks yang berkoresponden dengan cipherteks tersebut.

Sebaliknya sebuah algoritma kriptografi dikatakan **aman secara komputasi** (*computationally secure*) bila memenuhi kriteria sebagai berikut [STA98]**[2]**:

a) Biaya untuk memecahkan cipherteks melampaui nilai informasi yang terkandung di dalam cipherteks tersebut.
b) Waktu yang diperlukan untuk memecahkan cipherteks melampaui lamanya waktu informasi tersebut harus dijaga kerahasiaanya.

2.6.4 Kompleksitas Serangan

Kompleksitas serangan dapat diukur dengan beberapa cara seperti berikut:

a) Kompleksitas data (*data complexity*)

   Jumlah data (plainteks dan cipherteks) yang dibutuhkan sebagai masukan untuk serangan. Semakin banyak data yang dibutuhkan untuk melakukan serangan, semakin kompleks serangan tersebut, berarti semakin bagus sistem kriptografi tersebut.

b) Kompleksitas waktu (*time complexity*)

   Waktu yang dibutuhkan untuk melakukan serangan. Semakin lama waktu yang dibutuhkan untuk melakukan serangan, berarti semakin bagus sistem kriptografi tersebut.

c) Kompleksitas ruang memori (*space/storage complexity*)

Jumlah memori yang dibutuhkan untuk melakukan serangan. Semakin banyak memori yang dibutuhkan untuk melakukan serangan, berarti semakin bagus sistem kriptografi tersebut.

2.6.5 Jenis-jenis Serangan

Serangan atau "serangan kriptanalisis" terhadap sistem kriptografi dikelompokkan dengan beberapa cara:

a. Berdasarkan keterlibatan penyerang dalam komunikasi, serangan dapat dibagi 2 macam, yaitu:

1. Serangan pasif (*passive attack*)

   Jenis serangan ini, penyerang tidak terlibat dalam komunikasi antara pengirim dan penerima, tetapi penyerang menyadap semua pertukaran pesan antara kedua entitas. Tujuannya untuk mendapatkan sebanyak mungkin informasi yang digunakan kriptanalisis. Metode penyadapan data seperti [SCH96]**[2]**:

   a) *Wiretapping*: penyadap mencegat data yang ditransmisikan pada saluran kabel komunikasi dengan menggunakan sambungan perangkat keras.

   b) *Electromagnetic eavesdropping*: penyadap mencegat data yang ditransmisikan melalui saluran *wireless,* misal radio.

   c) *Acoustic eavesdropping*: menangkap gelombang suara yang dihasilkan suara manusia.

2. Serangan aktif (*active attack*)

   Penyerang mengintervensi komunikasi dan ikut mempengaruhi sistem untuk keuntungan dirinya. Misal penyerang mengubah aliran pesan seperti menghapus sebagian cipherteks, mengubah cipherteks, menyisipkan potongan cipherteks palsu, me-*reply* pesan lama, mengubah informasi yang tersimpan. Tujuannya untuk mendapatkan informasi berharga seperti kunci atau nilai rahasia lainnya. Caranya, penyerang memutuskan komunikasi antara dua pihak lalu menempatkan dirinya diantara keduanya.

b. Berdasarkan banyaknya informasi yang diketahui oleh kriptanalis, serangan dikelompokkan menjadi 5 jenis yaitu:

   1) *Ciphertext-olnly attack*

      Adalah jenis serangan yang paling umum namun paling sulit karena informasi yang tersedia hanyalah cipherteks saja. Kriptanalis memiliki beberapa cipherteks dari beberapa pesan, semuanya dienkripsi dengan algoritma yang sama. Tugas kriptanalisis menemukan plainteks sebanyak mungkin dari cipherteks atau menemukan kunci yang digunakan untuk mendekripsi. Diformulasikan seperti berikut:

      Diberikan: $C_1 = E_k(P_1), C_2 = E_k(P_2),\ldots, C_i = E_k(P_i)$

      Deduksi:$P_1, P_2,\ldots, P_i$ atau k untuk mendapatkan P_{i+1} *dari* $C_{i+1} = E_k(P_{i+1})$.

2) *Known-plaintext attack*

Adalah jenis serangan dimana kriptanalis memiliki pasangan plainteks dan cipherteks yang berkoresponden. Plainteks mungkin diperoleh dengan mempelajari karakteristik pesan. Diformulasikan seperti berikut:

Diberikan: $P_1, C_1 = E_k(P_1); P_2, C_2 = E_k(P_2);\ldots, Pi, C_i = E_k(P_i)$

Deduksi: *k* untuk mendapatkan P_i+_1 *dari* $C_i+_1 = E_k(P_i+_1)$.

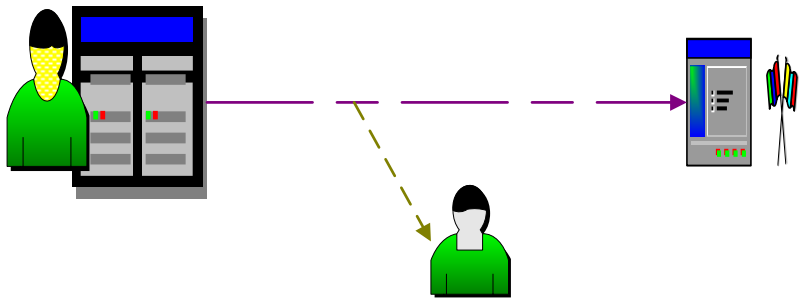
3) *Chosen-plaintext attack*

Adalah jenis serangan yang lebih hebat dari *Known-plaintext,* karena kriptanalis dapat memilih plainteks yang dimiliki untuk dienkripsikan, yaitu plainteks yang lebih mengarahkan penemuan kunci. Diformulasikan seperti berikut:

Diberikan: $P_1, C_1 = E_k(P_1); P_2, C_2 = E_k(P_2);\ldots, Pi, C_i = E_k(P_i)$ dimana kriptanalis dapat memilih diantara P1, P2,…, P_i

Deduksi: *k* untuk mendapatkan P_i+_1 *dari* $C_i+_1 = E_k(P_i+_1)$.

Agar lebih jelas, berikut contoh serangan dari *Chosen-plaintext attack* :



Gambar 2.9 *Chosen-plainteks attack*

4) *Chosen-ciphertext attack*

Adalah jenis serangan dimana kriptanalis memilih ciphertext untuk didekripsikan dan memiliki akses ke plainteks hasil dekripsi. Jenis serangan ini biasanya dipakai pada sistem kriptografi. Diformulasikan seperti berikut:

Diberikan: $C_1, P_1 = D_k(C_1); C_2, P_2 = D_k(P_2);\ldots, Ci, P_i = D_k(C_i)$

Deduksi: *k* (yang mungkin diperlukan untuk mendekripsi pesan pada waktu yang akan datang).

5) *Chosen-text attack*

Adalah jenis serangan yang merupakan kombinasi *Chosen-plaintext attack* dan *Chosen-ciphertext attack.*

c. Berdasarkan teknik yang digunakan dalam menemukan kunci, serangan dibagi menjadi *exhaustive attack* dan *analytical attack:*

1) *Exhaustive attack* atau *brute force attack*

Adalah serangan untuk mengungkapkan plainteks atau kunci dengan mencoba semua kemungkinan kunci. Diasumsikan kriptanalis mengetahui algoritma yang digunakan oleh pengirim pesan dan kriptanalis memiliki sejumlah cipherteks dan/atau plainteks yang bersesuaian.

Jika hanya cipherteks yang tersedia, cipherteks didekripsi dengan setiap kemungkinan kunci, dan plainteks hasil dekripsi diperiksa apakah mengandung arti. Jika ya, kunci yang sedang dites punya peluang paling besar sebagai kunci yang digunakan untuk menekripsi pesan. Jika plainteks yang dihasilkan tidak mempunyai arti, tes lagi dengan kunci lain.

Jika cipherteks dan plainteks yang berkoresponden tersedia (*known plaintext*) maka *exhaustic attack* menjadi lebih mudah.

2) *Analytical attack*

Jenis serangan ini, kriptanalis tidak mencoba-coba semua kemungkinan kunci tetapi menganalisis kelemahan algoritma kriptografi untuk mengurangi kemungkinan kunci yang tidak mungkin ada. Diasumsikan kriptanalis mengetahui algoritma kriptografi yang digunakan oleh pengirim pesan. Analisis dapat menggunakan pendekatan matematik dan statistik dalam rangka menemukan kunci, seperti *linear cryptanalysis, differential cryptanalysis*, dan *integral cryptanalysis.*

Untuk menghadapi serangan ini, kriptografer harus membuat algoritma kriptografi yang kompleks sehingga plainteks merupakan fungsi matematika dari cipherteks dan kunci yang cukup kompleks, dan tiap kunci merupakan fungsi matematika dari cipherteks dan plainteks yang cukup kompleks. Model *analytical* biasanya lebih cepat menemukan kunci dibandingkan *exhaustive attack.*

2.6.6 Algoritma Kriptografi *Caesar-Chipper*

Pada dasarnya, algoritma kriptografi klasik dapat dikelompokkan ke dalam dua macam *Cipher* :

a) *Cipher* Subtitusi (*Subtitution Ciphers)*

b) *Cipher* Transposisi (*Transpotition Ciphers)*

Di dalam *Cipher* subtitusi setiap unit plainteks diganti dengan satu unit Cipherteks. Satu unit bisa berarti satu huruf, pasangan huruf, atau kelompik lebih dari dua huruf. Algoritma subtitusi tertua adalah *Caesar- Cipher* yang digunakan oleh kaisar Romawi, Julius Caesar sehingga dinamakan *Caesar Cipher,* untuk menyandikan pesan kepada yang dikirim kepada gubernurnya.

Pada *Caesar Cipher,* tiap huruf disubtitusi dengan huruf ketiga berikutnya dari susunan alphabet yang sama. Dalam hal ini kuncinya adalah jumlah pergeseran huruf.

A. Jenis-jenis *Cipher* Subtitusi

Cipher subtitusi dikelompokkan kedalam empat jenis yaitu :

a) *Cipher* alphabet-tunggal (*monoalphabetic cipher)* :

Merupakan *Cipher* subtitusi sederhana, satu huruf di plainteks diganti dengan tepat satu huruf cipherteks.

b) *Cipher* alphabet-majemuk (*polyalphabetic cipher)* :

Merupakan *cipher* subtitusi-ganda yang melibatkan penggunaan kunci berbeda. Ditemukan pertama kali oleh Leon Battista Alberti tahun 1568. metode ini digunakan oleh tentara AS selama perang Sipil Amerika.

Misal : $P = p_1p_2...p_mp_{m+1}...p_{2m...}$ P= *Plaintext*

Maka Cipherteks hasil enkripsi yaitu :

$Ek(P)=f_{1(}p_{1)}\ f_{2(}p_{2)}..\ f_{m(}p_{m)}\ f_{m+1(}p_{m+1)}...f_{2m(}p_{2m)...}$

Dalam hal ini p_i adalah huruf-huruf dalam plainteks dan f_i adalah fungsi enkripsi untuk m=1, *cipher*-nya ekivalen dengan *cipher* alpfabet tunggal.

c) *Cipher* subtitusi homofonik (*homophonic substitution cipher)* :

Sama seperti *cipher* alphabet tunggal, kecuali bahwa setiap huruf didalam plainteks dapat dipetakan kedalam salah satu dari unit cipherteks yang mungkin. Maksudnya, setiap huruf plainteks dapat memiliki lebih dari satu kemungkinan unit cipherteks. Huruf yang paling sering muncul didalam teks mempunyai lebih banyak pilihan unit cipherteks.

d) *Cipher* subtitusi poligram (*polygram substitution cipher)* :

Setiap kelompok huruf disubtitusi dengan kelompok huruf Cipherteks, dalam artian bahwa tidak mensubtitusi setiap huruf seperti pada tipe *cipher* subtitusi sebelumnya. Jika unit huruf plainteks/cipherteks panjangnya 2 huruf, maka disebut *digram,* jika tiga huruf maka disebut *trigram.* Keuntungannya distribusi kemunculan poligraf menjadi *flat*(datar), dan ini menyulitkan analisis frekuensi.

B. *Cipher* Transposisi

Pada *cipher* transposisi, huruf-huruf didalam plainteks tetap sama, hanya saja urutannya diubah. Dengan kata lain algoritma ini melakukan *transpose* terhadap rangkaian karakter didalam teks. Atau disebut juga dengan **permutasi** atau **pengacakan** (*scrambling)* karena *transpose* setiap karakter didalam teks sama dengan mempermutasikan karakter-karakter tersebut.

2.7 Pemilihan Bahasa Pemrograman

Pemrograman (*programming)* merupakan kegiatan menulis kode program yang akan di *compiler* oleh bahasa pemrograman. Penulisan kode program

merupakan kegiatan yang paling utama dalam tahap implementasi sistem. Untuk mengimplementasikan sistem yang telah dirancang, akan dimplementasikan dalam versi windows. Versi windows akan menggunakan bahasa pemrograman berorientasi objek yaitu Borland Delphi 7.0

2.8 Perbankan Secara Umum

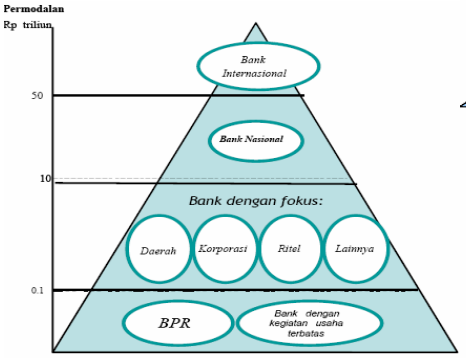
Industri perbankan nasional saat ini telah memiliki Arsitektur Perbankan Indonesia (API) yang merupakan suatu *blueprint* mengenai arah dan tatanan perbankan nasional kedepan. API tersebut merupakan *policy direction* dan *policy recommendations* untuk industri perbankan nasional dalam jangka panjang yaitu untuk jangka waktu sepuluh tahun ke depan. Jelas sekali bahwa API tersebut merupakan suatu *banking architecture* yang tidak hanya diperlukan bagi industri perbankan saja melainkan juga sektor keuangan keseluruhan untuk melihat gambaran atau peta perbankan di masa depan. Keberadaan API tersebut memiliki tujuan yang sangat fundamental yaitu terciptanya industri perbankan nasional yang sehat, kuat dan efisien guna menciptakan kestabilan sistem keuangan dalam rangka mendorong pertumbuhan ekonomi nasional**[3].**

Arah kedepan perbankan nasional tersebut telah tertuang di dalam Visi API ke Depan (lihat Tabel 2.6) sehingga setiap bank akan melihat kembali kemampuan dan sumber daya masing-masing apakah mempunyai tujuan jangka panjang untuk menjadi bank internasional, bank nasional atau menjadi bank spesialis yang memliki fokus kegiatan tertentu. Untuk mencapai visi tersebut diperlukan kerja keras dan berbagai program dan kegiatan pendukung. Oleh sebab itu tahap-tahap

pencapaiannya harus dilakukan secara bertahap dan dalam jangka waktu yang cukup panjang. Program kegiatan untuk mencapai Visi dimaksud dilakukan secara komprehensif dan menyeluruh, yang dikelompokkan menjadi enam pilar API (Tabel 2.7) **[3]**.

Berikut Visi Perbankan di masa yang akan datang dan enam pilar arsitektur perbankan indonesia :

Tabel 2.6 Visi Perbankan



Tabel 2.7 Enam Pilar Arsitektur Perbankan



2.8.1 Perusahaan Daerah Bank Perkreditan Rakyat Jawa Barat (PD BPR)

Terbentuknya PD.BPR-LPK Garut Kota yang semula bernama Lembaga Perkreditan Kecamatan di Jawa barat yang didirikan dengan peraturan daerah Propinsi Daerah Tingkat I Jawa Barat Nomor 3 Tahun 1987 diubah bentuknya menjadi PD BPR LPK

Kegiatan PD BPR LPK sehari-hari adalah melaksanakan kegiatan usaha dibidang perbankan, yaitu melakukan kegiatan menerima dana masyarakat dan menyalurkannya kembali kepada masyarakat dalam bentuk bantuan modal bagi yang memerlukan serta melayani jasa perbankan BPR lainnya. Usaha BPR meliputi :

1. Menghimpun simpanan berupa deposito berjangka, tabungan dan/atau bentuk lainnya yang dipersamakan dengan itu;
2. Memberikan kredit;
3. menyediakan pembiayaan bagi nasabah berdasarkan prinsip bagi hasil sesuai dengan ketentuan yang berlaku;
4. Menempatkan dana dalam bentuk Sertifikat Bank Indonesia (SBI), deposito berjangka, sertifikat deposito dan/atau tabungan pada bank lain.

Untuk menunjang kegiatan operasional tersebut, perlu didukung oleh suatu sistem akuntansi yang memadai, sehingga setiap langkah kegiatan operasionalnya dapat termonitor dengan baik, dan dalam pelaksanaannya diperlukan adanya pengaturan yang tegas antara petugas pelaksana (*maker*) dengan pengawas (*checker*), dan pejabat yang mengesahkan (*signer*) agar terselenggara kontrol intern yang baik.

2.8.1.1 Struktur Organisasi PD. BPR LPK Garut Kota

Struktur organisasi di PD.BPR LPK Garut Kota disesuaikan dengan ketentuan Keputusan Menteri Dalam Negeri No.82 Tahun 1997 tanggal 4 Juni 1997 tentang Pedoman Organisasi dan Tata Kerja Perusahaan Daerah Bank Perkreditan Rakyat.

2.8.1.2 Jenis – Jenis Transaksi Keuangan PD.BPR

1. Transaksi tunai adalah transaksi keuangan yang berhubungan dengan perubahan posisi kas secara tunai, yaitu terdiri dari:

1.1. Transaksi Penerima/Penarikan Tunai :

A. Setoran penyertaan modal dari pemilik/pemegang saham

B. Setoran tabungan

C. Setoran simpanan berjangka (Deposito)

D. Penerimaan pinjaman pihak ketiga

E. Penerimaan pinjaman antar bank

F. Pengambilan uang dari Bank dan Lembaga lainnya

G. Penerimaan angsuran pokok kredit, bunga, denda, dan biaya lain dari debitur

H. Penerimaan komisi dan provisi serta jasa lainnya

I. Hasil penjualan aktiva tetap dan inventaris lainnya

J. Penerimaan uang titipan dari lembaga lain

K. Transaksi penerimaan lainnya yang bersifat penerimaan tunai

1.2. Transaksi Pengeluaran/Pembayaran Tunai :

B. Pembayaran kewajiban yang harus dibayar

C. Pengambilan tabungan

D. Pengambilan deposito dan bunganya

E. Pengembalian dan pembayaran bunga pinjaman kepada pihak ke tiga

F. Pemberian pinjaman yang diberikan

G. Pengeluaran biaya-biaya

H. Penyimpanan uang di BI dan Lembaga Keuangan lain bukan Bank

I. Pemberian pinjaman antar bank

J. Pembelian aktiva tetap dan inventaris

K. Pembayaran pajak

L. Pembayaran pembagian laba

M. Pengembalian uang titipan

N. Transaksi pengeluaran lainnya yang bersifat tunai

2. Transaksi non tunai adalah transaksi keuangan yang tidak berhubungan dengan perubahan posisi kas secara tunai, yaitu :

A. Pemindahbukuan antar rekening

B. Penyisihan penghapusan aktiva produktif

C. Penyusutan aktiva tetap dan inventaris

D. Penghapusan rupa-rupa aktiva

E. Penghitungan bunga tagihan kredit

F. Pembiayaan bunga tabungan yang masih harus dibayar

G. Pembayaran bunga deposito yang masih harus dibayar

H. Pembayaran bunga pinjaman yang masih harus dibayar

I. Perhitungan pembagian laba

J. Cadangan pembayaran pajak

K. Perbaikan kesalahan

L. Transaksi lainnya yang bersifat pemindahbukuan

2.8.1.3 Produk di PD.BPR LPK Garut

1. Tabungan PD.BPR LPK. Terdiri dari ;

1.1 Tabungan Wajib ;

Tabungan yang diwajibkan kepada setiap nasabah pengambil kredit di PD.BPR masing-masing, yang mana tabungan tersebut baru boleh diambil apabila kreditnya telah lunas dan tidak memperoleh bunga tabungan.

1.2 Tabungan Sukarela ;

Diperuntukkan bagi perorangan atau lembaga termasuk para penabung wajib yang menabung uangnya (selain tabungan wajib) pada PD.BPR masing-masing, yang penyetoran dan penarikannya berdasarkan syarat yang telah ditentukan. terdiri dari :

a) Tabungan Umum : Tabungan Masyarakat Desa (TAMASA)

b) Tabungan Khusus :

Tabungan Kotak Masyarakat (Kotak Mas)

Tabungan Wajib Pajak (TAWAP)

Tabungan Anak Sekolah (TAS)

Tabungan Kesehatan Masyarakat

Tabungan Kerja Sama dengan Bank Lain

1.3 Tabungan Titipan ;

Tabungan yang diperuntukkan bagi penabung yang menyimpan uangnya pada PD.BPR masing-masing, secara sementara tergantung kepada waktu rencana penggunaan uang tersebut oleh penabung yang bersangkutan. Merupakan jenis tabungan sebagai produk kerjasama dengan Bank lain, baik PD.BPR maupun Bank umum.

2. Deposito ;

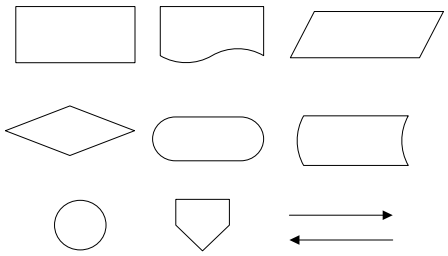
   Simpanan yang penarikannya hanya dapat dilakukan pada waktu tertentu berdasarkan perjanjian antara nasabah penyimpan dengan PD.BPR yang bersangkutan.

3. Perkreditan ;

   Kesepakatan pinjam meminjam antara pihak Bank dengan pihak lain yang mewajibkan pihak peminjam untuk melunasi utangnya setelah jangka waktu tertentu dengan pemberian bunga.

2.9 *FlowChart*

Flowchart adalah suatu alat yang cukup efisien untuk menggambarkan suatu algoritma agar dapat dengan mudah diimplementasikan pada suatu aplikasi. Tujuan utama penggunaan *flowchart* adalah untuk menggambarkan suatu tahapan penyelesaian masalah secara sederhana. Metode ini menggunakan simbol-simbol tertentu yang mudah dimengerti dan telah di standarisasi dalam menyelesaikan masalah yang dihadapi. Adapun simbol-simbol program *flowchart* dapat dilihat pada Gambar 2.11 berikut ini :



Gambar 2.10 Simbol-simbol *Flowchart*

Perhatikan keterangan berikut ini dari Gambar 2.11 :

a) Proses : Menyatakan kegiatan pengolahan data setelah menerima masukan dari simbol yang lain dan mendistribusikan hasilnya kepada proses berikutnya.
b) Pengujian : Simbol yang digunakan untuk menanyakan apakah suatu kondisi logika tertentu sudah terpenuhi. Jika sudah, proses dapat dilanjutkan ke tahap berikutnya dan jika tidak maka proses tidak dilanjutkan atau kembali ke proses sebelumnya.
c) Konektor : Untuk menandai dan mengatur perpindahan halaman jika diagram alur tidak cukup diterapkan dalam satu halaman saja.
d) Dokumen : Sebagai sebuah dokumen, dokumen input maupun dokumen report. Jika simbol merupakan data masukan, maka yang mengikutinya anak panah keluar dilanjutkan ke proses berikutnya. Jika simbol merupakan hasil suatu proses, maka ada simbol lain yang mengikuti atau mengarah pada simbol tersebut.
e) Terminator : Digunakan sebagai posisi yang menyatakan awal atau akhir suatu proses.
f) *Input / Output* : Simbol yang menandai adanya proses inputan (masukan) atau *output* (keluaran) suatu data.
g) Media Penyimpanan : Sebagai simbol penyimpanan data dalam suatu proses.
h) Arus : Simbol arah yang menunjukkan panah keluar atau masuk dalam suatu proses.