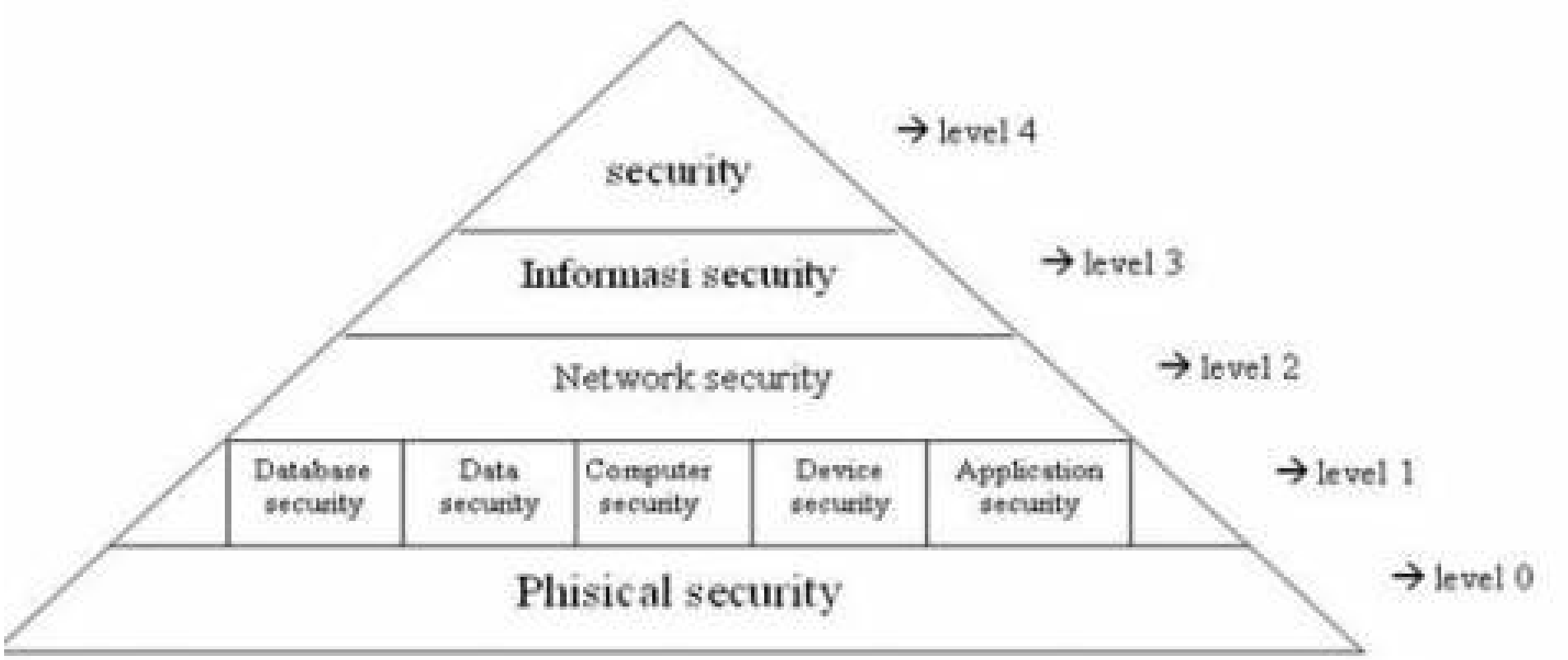
Metode Keamanan



Level 0

Keamanan Level 0 (Psychical Security)
Keamanan fisik yang merupakan tahap awal dari keamanan komputer.

Level 0

- Infrastuktur ?
- Device Location ?
- Power Saver ? (Backup)
- Hardware Safety ?
- Human Access ?
- Monitoring ?

Level 1

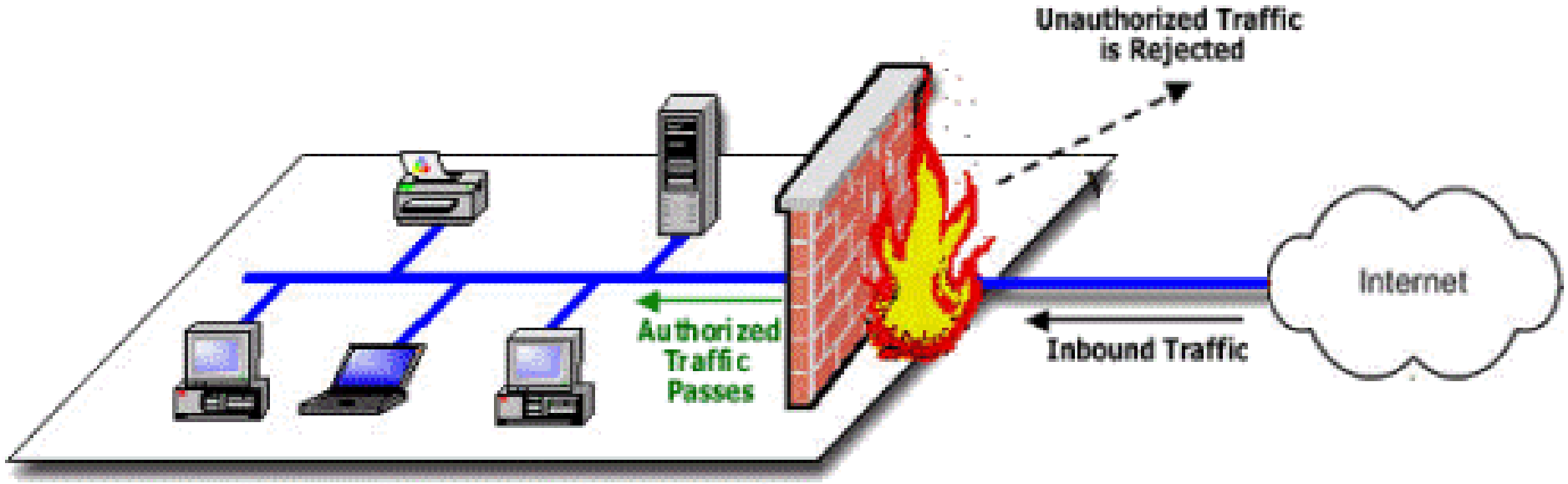
Software Security

- Database Security
- Computer Security (Operating System)
- Application Security
- Implementation & Testing
- Maintenance

Level 2

Network Security

Level 2


Unauthorized Traffic
is Rejected
Internet
Authorized
Traffic
Passes
Inbound Traffic

Level 2

Network Security

- Firewall
- IDS

Firewall

Sebuah sistem atau perangkat yang mengizinkan lalu lintas jaringan yang dianggap aman untuk melaluinya dan mencegah lalu lintas jaringan yang tidak aman. Umumnya, sebuah firewall diimplementasikan dalam sebuah mesin terdedikasi, yang berjalan pada pintu gerbang (gateway) antara jaringan lokal dan jaringan lainnya.

Jenis Firewall

Personal Firewall didesain untuk melindungi sebuah komputer yang terhubung ke jaringan dari akses yang tidak dikehendaki.

Contoh dari firewall jenis ini adalah Microsoft Windows Firewall (yang telah terintegrasi dalam sistem operasi Windows XP Service Pack 2, Windows Vista dan Windows Server 2003 Service Pack 1), Symantec Norton Personal Firewall, Kerio Personal Firewall, dan lain-lain.

Jenis Firewall

Network ’Firewall didesain untuk melindungi jaringan secara keseluruhan dari berbagai serangan. Umumnya dijumpai dalam dua bentuk, yakni sebuah perangkat terdedikasi atau sebagai sebuah perangkat lunak yang diinstalasikan dalam sebuah server.

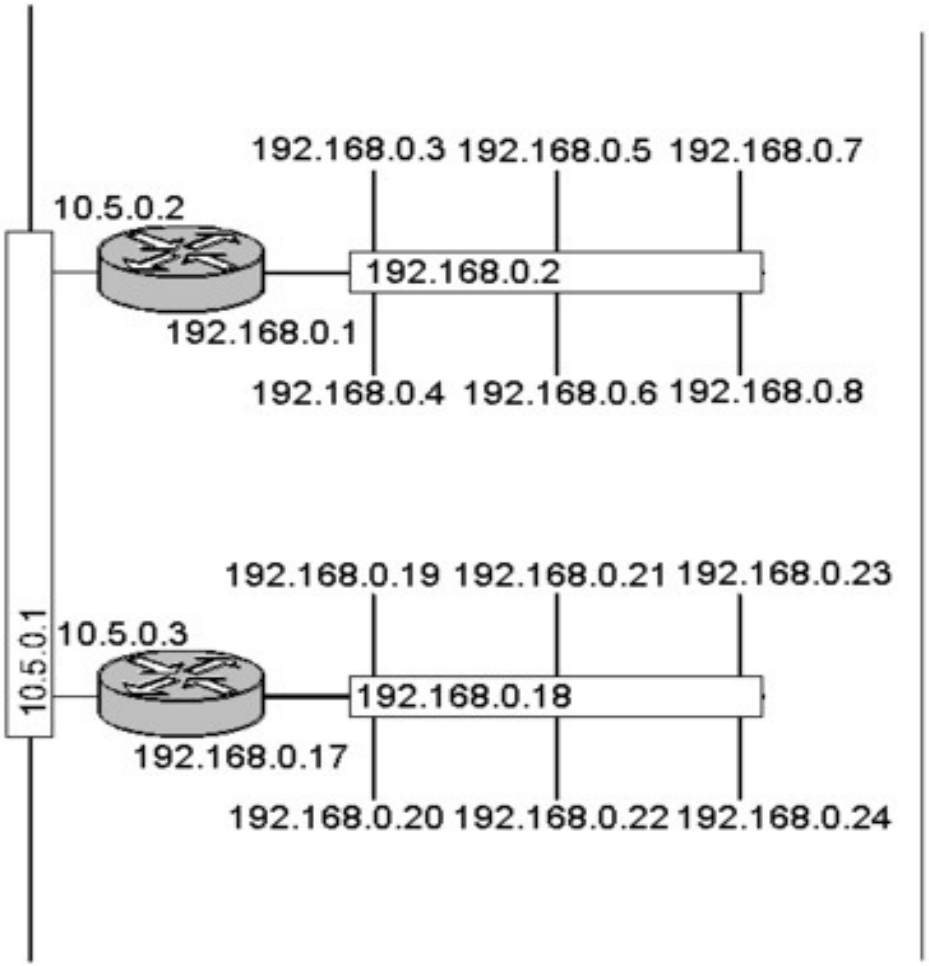
Contoh dari firewall ini adalah Microsoft Internet Security and Acceleration Server (ISA Server), Cisco PIX, Cisco ASA, IPTables dalam sistem operasi GNU/Linux, pf dalam keluarga sistem operasi Unix BSD, serta SunScreen dari Sun Microsystems, Inc. yang dibundel dalam sistem operasi Solaris.

Fungsi Firewall

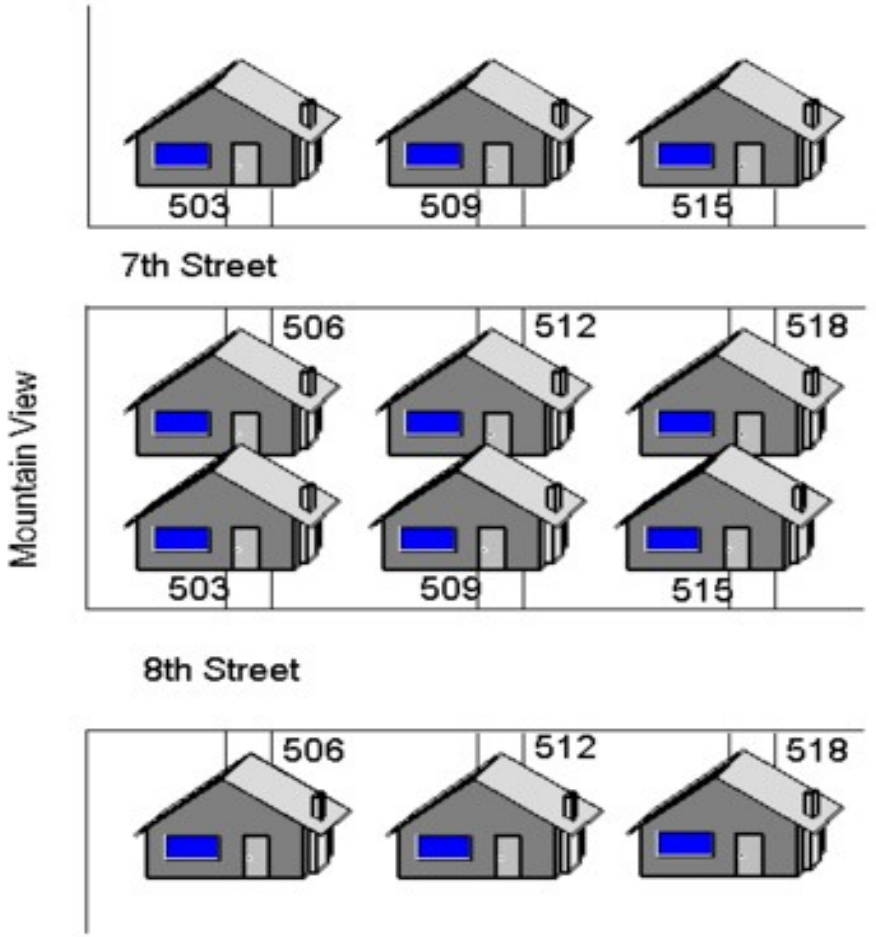
Pada umumnya fungsi firewall :

1. Mengontrol dan mengawasi lalu lintas data dalam jaringan
2. Authentikasi Akses
3. Mencatat setiap aktivitas (log)

Computer Networking

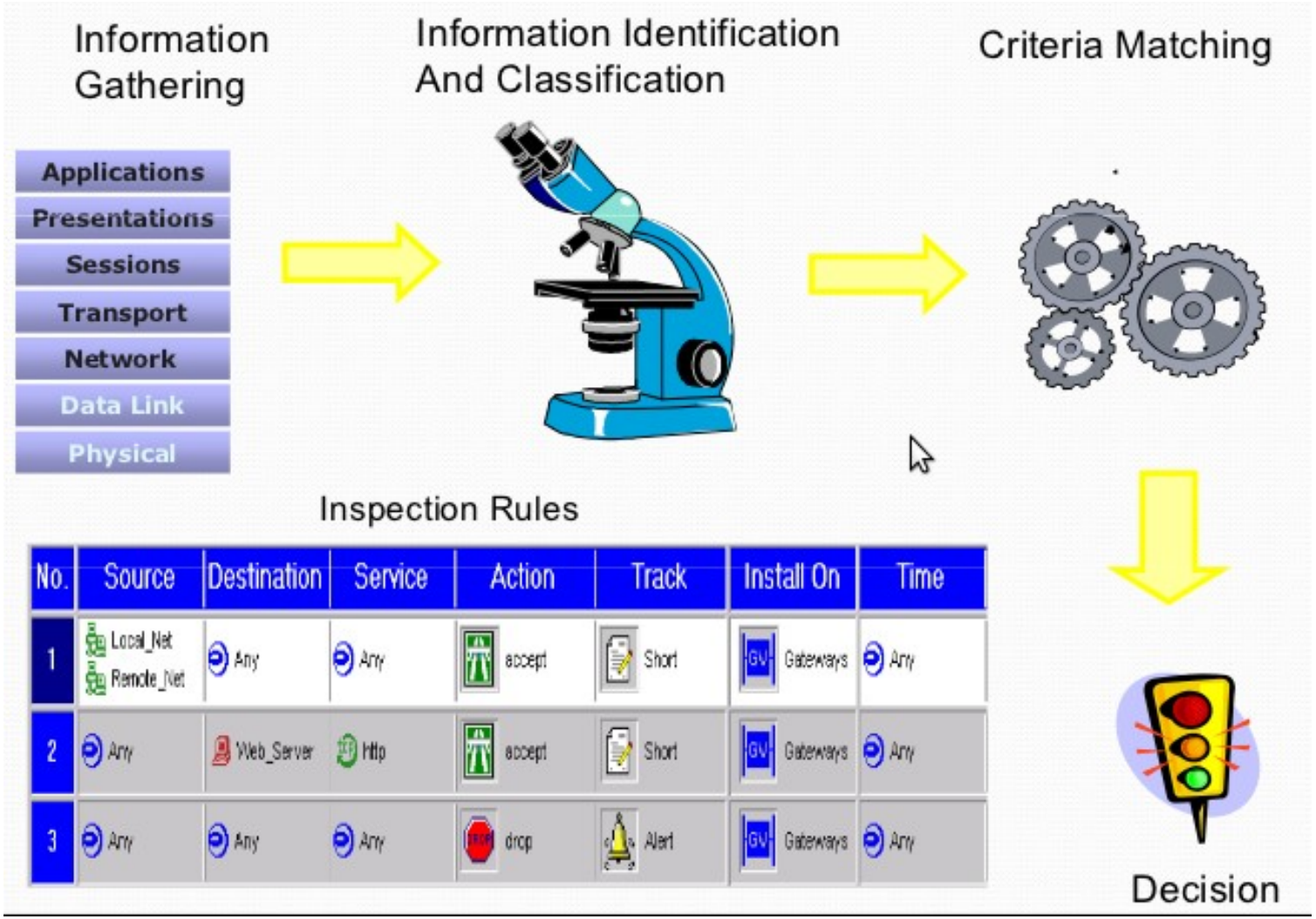


Network



Neighborhood

How it works ?


Information Gathering
Information Identification And Classification
Criteria Matching
Applications
Presentations
Sessions
Transport
Network
Data Link
Physical
Inspection Rules
No.
Source
Destination
Service
Action
Track
Install On
Time
1
Local_Net
Remote_Net
Any
Any
accept
Short
Gateways
Any
2
Any
Web_Server
Http
accept
Short
Gateways
Any
3
Any
Any
Any
drop
Alert
Gateways
Any
Decision

Contoh Firewall

;;; Web-Server											
48		accept	forward		192.168.31.1						8.3 KiB	74
;;; File-Server											
49		accept	forward		192.168.111.7						0 B	0
;;; Server-Proxy											
50		accept	forward		192.168.2.10						4152 B	13
;;; Server-Library											
51		accept	forward		192.168.20.37	6 (tcp)		80			0 B	0
;;; Allow-server-sisfo:80											
52		accept	forward		192.168.111.11	6 (tcp)		80			3944 B	71
;;; Allow-All-Out-toInternet											
53		accept	forward							ether1...	2968.3 KiB	54 532
;;; eth5-wireless-to-sisfo:80											
54		accept	forward		192.168.111.11	6 (tcp)		80	ether5...		0 B	0
;;; eth5-wireless-to-library:80											
55		accept	forward		192.168.20.37	6 (tcp)		80	ether5...		0 B	0
;;; eth5-wireless-to-internet											
56		accept	forward						ether5...	ether1...	0 B	0
;;; drop-from-wireless											
57		drop	forward						ether5...		0 B	0

Level 3

Information Security (Human Factor)

- Kertas bekas transaksi, topologi, broken print
- Tell me your password ?
- SOP
- Training

Level 4

Evaluasi, Monitoring & Maintenance

Policy Security

Sebuah sistem yang canggih dan mahal tanpa adanya standar kebijakan-kebijakan keamanan akan menjadi kurang optimal.

Security Policy

Policy penggunaan komputer

Tidak boleh meminjamkan account kepada orang lain
Tidak boleh mengambil/menaruh file dari komputer kantor, dll

Policy penggunaan Installasi program

Tidak boleh mengintsall program tanpa seijin staff IT
Tidak boleh mengintsall program ilegal, dll

Policy penggunaan Internet

Tidak boleh menggunakan internet untuk kegiatan carding, hacking dkk
Tidak boleh menggunakan internet untuk mengakses situs-situs yang berpotensi menyebarkan virus, dll

Policy penggunaan Email

Tidak boleh menggunakan email kantor untuk kegiatan milis, dll

ISO Policy Security

Standard ISO 17799 : 27002 Tahapan Mengatur tentang Keamanan Sistem Informasi

KRIPTOGRAFI

Seni atau ilmu untuk menjaga kerahasiaan berita / data.

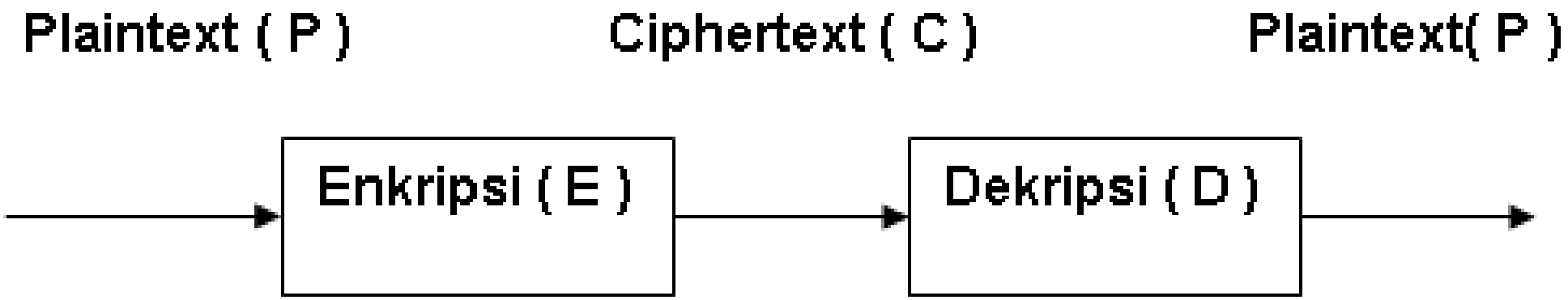
Tujuan dari Ilmu Kriptografi :
1. Kerahasiaan
2. Integritas Data
3. Authentikasi

Algoritma Sandi adalah Langkah-langkah yang digunakan untuk melakukan kriptografi.

Enkripsi ialah proses mengamankan suatu informasi dengan membuat informasi tersebut tidak dapat dibaca tanpa bantuan pengetahuan khusus.

Dekprisi kebalikan dari proses enkripsi yaitu proses konversi data yang sudah dienkripsi kembali menjadi data aslinya sehingga dapat dibaca/ dimengerti kembali.

Enkripsi & Dekripsi



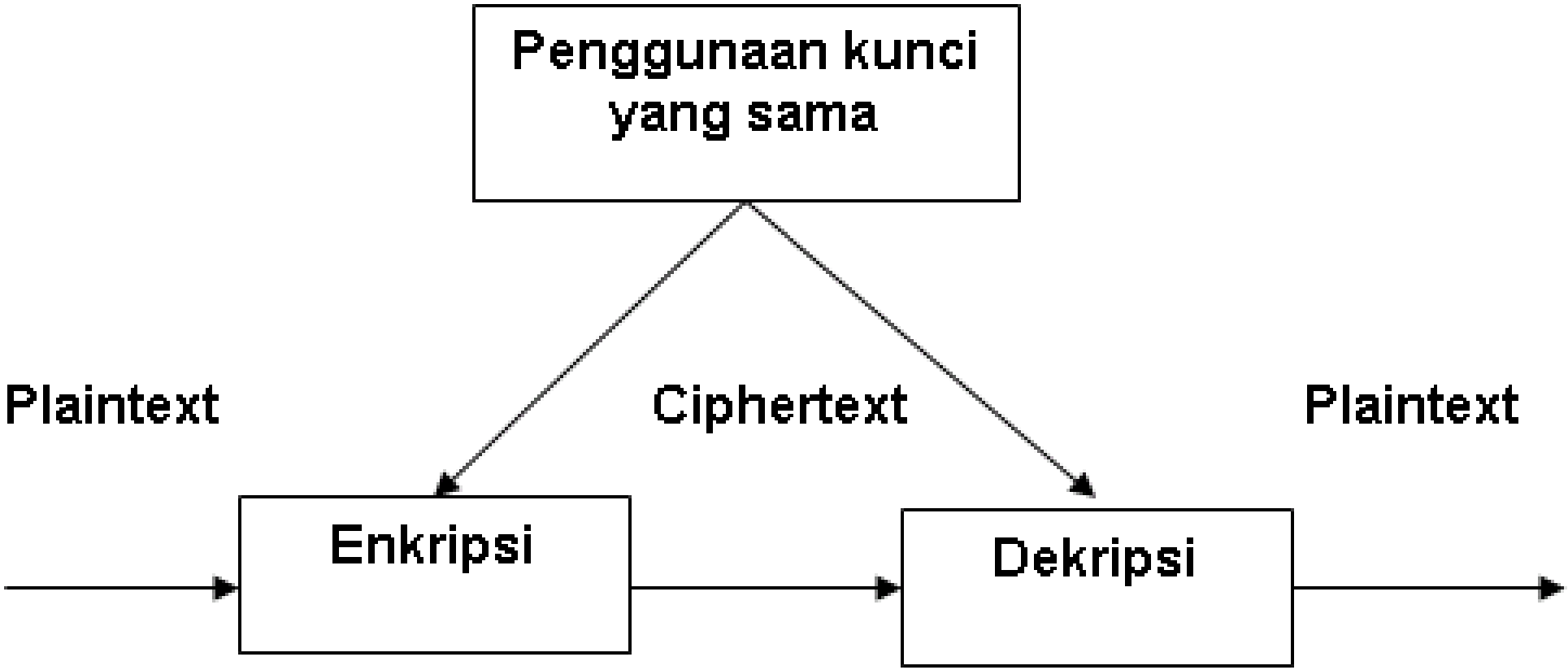
Metode Enkripsi

Algoritma kriptografi dengan menggunakan kunci dapat dikelompokkan menjadi 2 (dua) bagian yaitu :

a. Kunci Simetris
b. Kunci Asimetris

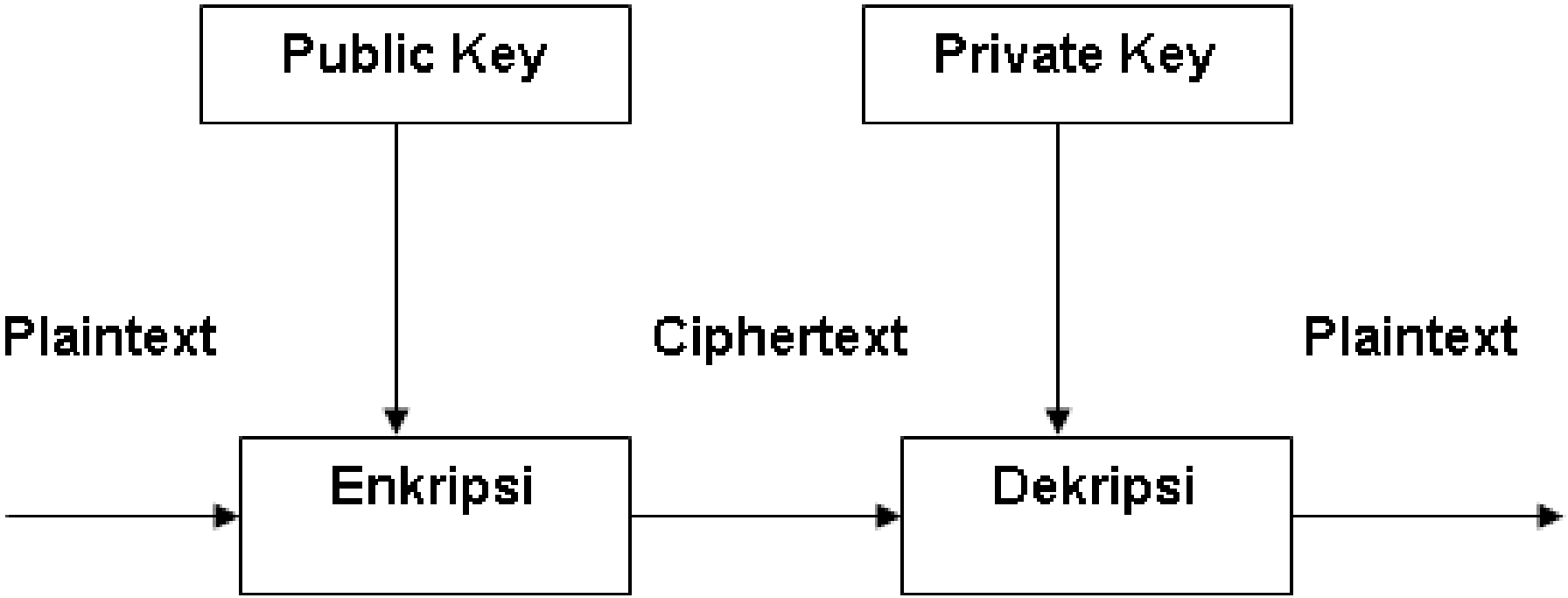
Kunci Simetris hanya menggunakan satu kunci dalam proses enkripsi dan dekripsi.

Kunci Simetris



Kunci Asimetris

Menggunakan dua kunci yang berbeda untuk melakukan enkripsi dan dekripsi.



Kunci Asimetris

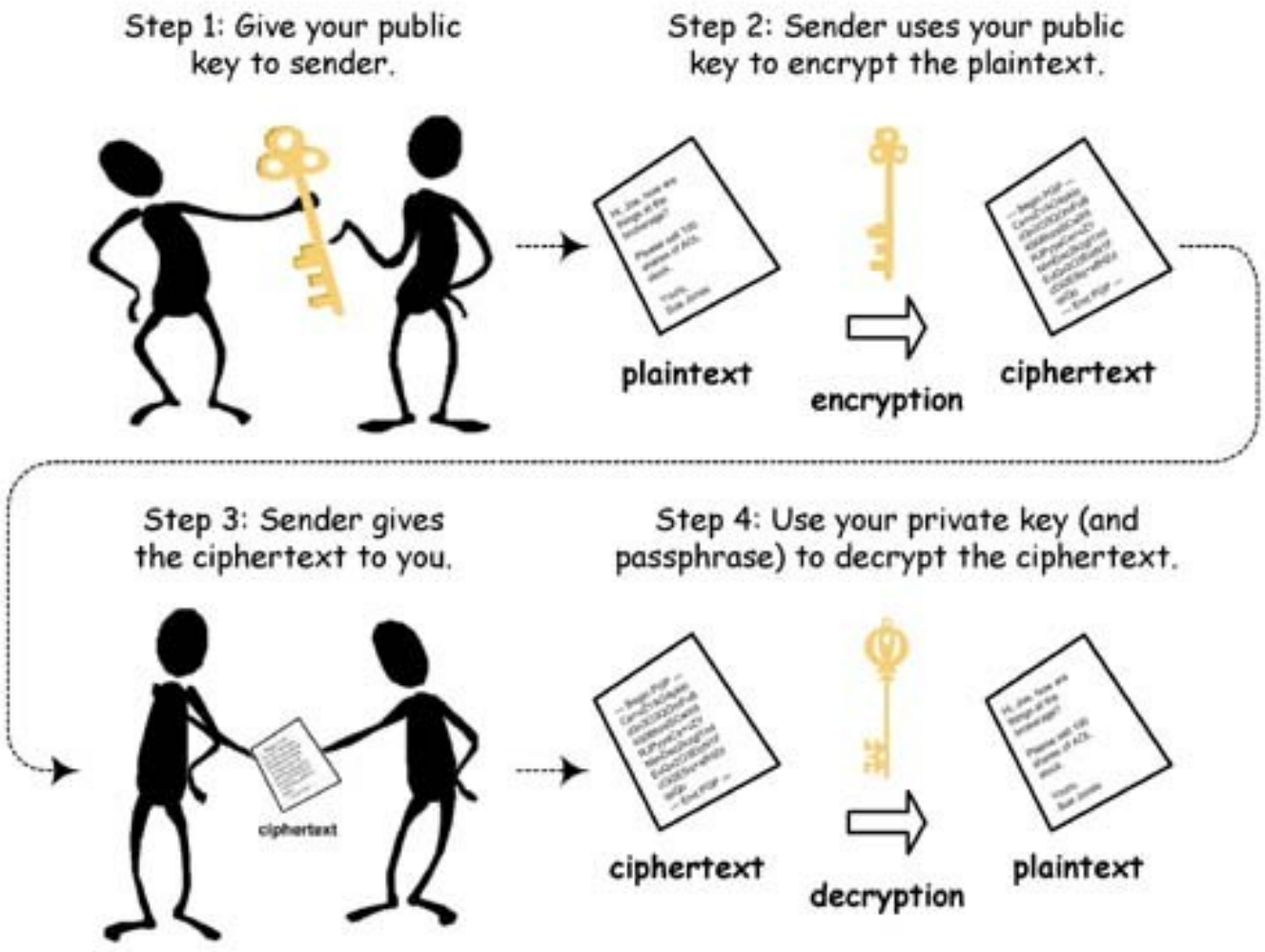
Terdapat 2 host yang ingin berkomunikasi :

- Host A mengirimkan permintaan komunikasi
- Host B menerima permintaan komunikasi

Host A ingin mengirim pesan ke Host B :

- Host A mengirim public key ke Host B (Host B meminta Public Key)
- Host B mengirim pesan dengan menggunakan public key milik host A
- Host A menerima pesan dan melakukan dekripsi pesan menggunakan private key miliknya dan membaca pesan dari host B

Public and Private Key



Algoritma Caesar Cipher

Metode Algoritma klasik Caesar cipher dengan cara menggeser karakter tertentu.