

## BAB V

### PENGAMANAN PADA PROTOKOL TCP/IP

#### 5.1 KONSEP PENGAMANAN JARINGAN (*NETWORK SECURITY*)

##### 5.1.1 Perencanaan Pengamanan

Salah satu problem *network security* yang paling penting, dan mungkin salah satu yang paling tidak enak, adalah menentukan kebijakan dalam *network security*. Kebanyakan orang menginginkan solusi teknis untuk setiap masalah, berupa program yang dapat memperbaiki masalah-masalah *network security*. Padahal, perencanaan keamanan yang matang berdasarkan prosedur dan kebijakan dalam *network security* akan membantu menentukan apa-apa yang harus dilindungi, berapa besar biaya yang harus ditanamkan dalam melindunginya, dan siapa yang bertanggungjawab untuk menjalankan langkah-langkah yang diperlukan untuk melindungi bagian tersebut.

##### 5.1.2 Mengenali ancaman terhadap network security

Langkah awal dalam mengembangkan rencana *network security* yang efektif adalah dengan mengenali ancaman yang mungkin datang. Dalam RFC 1244<sup>1</sup>, Site security Handbook, dibedakan tiga tipe ancaman :

- Akses tidak sah, oleh orang yang tidak mempunyai wewenang.
- Kesalahan informasi, segala masalah yang dapat menyebabkan diberikannya informasi yang penting atau sensitif kepada orang yang salah, yang seharusnya tidak boleh mendapatkan informasi tersebut.
- Penolakan terhadap service, segala masalah mengenai *security* yang menyebabkan sistem mengganggu pekerjaan-pekerjaan yang produktif.

---

<sup>1</sup>RFC : Request For Comment, definisi-definisi standar yang menjadi dasar perencanaan dan implementasi dalam networking

Disini ditekankan *network security* dari segi perangkat lunak, namun *network security* sebenarnya hanyalah sebagian dari rencana keamanan yang lebih besar, termasuk rencana keamanan fisik dan penanggulangan bencana.

### **5.1.3 Kontrol terdistribusi**

Salah satu pendekatan dalam *network security* adalah dengan mendistribusikan tanggung jawab kontrol terhadap segmen-segmen dari jaringan yang besar ke grup kecil dalam organisasi. Pendekatan ini melibatkan banyak orang dalam keamanan, dan berjalan berlawanan dengan prinsip kontrol terpusat.

Pada prinsipnya, tanggung jawab dan kontrol yang terdistribusi dalam grup-grup kecil menciptakan lingkungan jaringan kecil yang terdiri dari *trusted hosts*. Meminjam analogi keamanan kota, maka hal ini sesuai dengan sistem keamanan tingkat RT, dimana terjadi kerjasama antar RT untuk menjaga lingkungan yang lebih besar. Jadi keamanan suatu segmen dipercayakan kepada manajer jaringan pada segmen tersebut. Dengan terjaganya keamanan tiap segmen, maka secara keseluruhan keamanan jaringan akan terjaga.

Dalam mendistribusikan kontrol network, digunakan berbagai cara. Salah satunya adalah dengan memanfaatkan pembagian subnet. Di setiap subnet terdapat *subnet administrator* (admin subnet) yang bertanggungjawab untuk keamanan network dan mempunyai kekuasaan untuk mengalokasikan / menetapkan IP address untuk *device* yang terhubung pada network. Penetapan IP address memberi admin subnet suatu kontrol terhadap siapa yang terhubung ke subnet. Sewaktu admin subnet menetapkan IP address untuk suatu sistem, dia juga menetapkan tanggungjawab keamanan tertentu ke admin sistem tersebut. Demikian juga, bila admin sistem menetapkan suatu account bagi user, maka ia memberikan tanggungjawab keamanan tertentu kepada user. Hirarki ini mengalir dari admin network, ke admin subnet, admin sistem, dan ke user. Mereka mendapat tanggungjawab, dan juga wewenang untuk menurunkan tanggungjawabnya. Untuk itu, setiap user harus mengetahui tanggungjawabnya.

Dalam kontrol terdistribusi, informasi dari luar disaring dahulu oleh admin network, kemudian disaring lagi oleh admin subnet, demikian seterusnya, sehingga user tidak perlu

menerima terlalu banyak informasi yang tidak berguna. Bila informasi ke user berlebihan, maka user akan mulai mengabaikan semua yang mereka terima.

#### **5.1.4 Menentukan security policy<sup>2</sup>**

Dalam *network security*, peranan manusia yang memegang tanggungjawab keamanan sangat berperan. *Network security* tidak akan efektif kecuali orang-orangnya mengetahui tanggung jawabnya masing-masing. Dalam menentukan *network security policy*, perlu ditegaskan apa-apa yang diharapkan, dan dari siapa hal tersebut diharapkan. Selain itu, kebijakan ini harus mencakup :

- Tanggung jawab keamanan *network user*, meliputi antara lain keharusan user untuk mengganti passwordnya dalam periode tertentu, dengan aturan tertentu, atau memeriksa kemungkinan terjadinya pengaksesan oleh orang lain, dll.
- Tanggung jawab keamanan *system administrator*, misalnya perhitungan keamanan tertentu, memantau prosedur-prosedur yang digunakan pada host.
- Penggunaan yang benar sumber-sumber network, dengan menentukan siapa yang dapat menggunakan sumber-sumber tersebut, apa yang dapat dan tidak boleh mereka lakukan.
- Langkah-langkah yang harus diperbuat bila terdeteksi masalah keamanan, siapa yang harus diberitahu. Hal ini harus dijelaskan dengan lengkap, bahkan hal-hal yang sederhana seperti menyuruh user untuk tidak mencoba melakukan apa-apa atau mengatasi sendiri bila masalah terjadi, dan segera memberitahu system administrator.

## **5.2 METODA-METODA NETWORK SECURITY**

### **5.2.1 Pembatasan akses pada network**

- **Internal password authentication (password pada login system)**

---

<sup>2</sup>security policy : kebijakan yang diambil berkaitan dengan keamanan jaringan

Password yang baik menjadi bagian yang paling penting namun sederhana dalam keamanan jaringan. Sebagian besar dari masalah network security disebabkan password yang buruk. Biasanya pembobolan account bisa terjadi hanya dengan menduga-duga passwordnya. Sedangkan bentuk yang lebih canggih lagi adalah *dictionary guessing*, yang menggunakan program dengan kamus ter-enkripsi, dibandingkan dengan password ter-enkripsi yang ada. Untuk itu, file `/etc/passwd` harus dilindungi, agar tidak dapat diambil dengan ftp atau tftp (berkaitan dengan *file-mode*). Bila hal itu bisa terjadi, maka tftp harus dinonaktifkan. Ada juga sistem yang menggunakan *shadow password*, agar password yang ter-enkripsi tidak dapat dibaca. Sering mengganti password dapat menjadi salah satu cara menghindari pembobolan password. Namun, untuk password yang bagus tidak perlu terlalu sering diganti, karena akan sulit mengingatnya. Sebaiknya password diganti setiap 3-6 bulan.

Algoritma enkripsi password tidak dapat ditembus, dalam arti password yang ter-enkripsi tidak dapat didekripsikan. Yang paling mungkin adalah bila kata-kata dalam kamus di-enkripsi, dan dibandingkan dengan password ter-enkripsi. Bila password yang digunakan buruk, mudah ditemukan dalam kamus, maka akan mudah terbongkar.

Beberapa hal yang sebaiknya diperhatikan dalam memilih password :

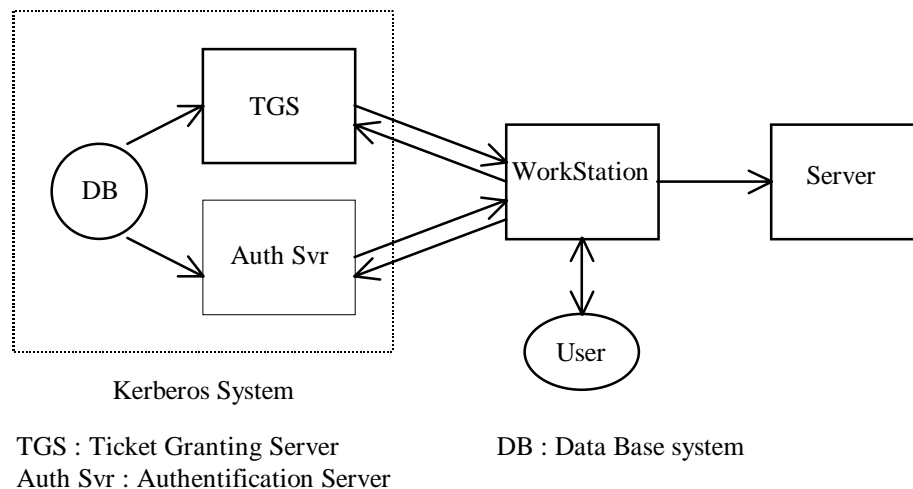
- ⇒ Jangan memakai nama login.
- ⇒ Jangan memakai nama siapapun atau apapun.
- ⇒ Jangan memakai kata-kata singkatan.
- ⇒ Jangan memakai informasi pribadi yang berhubungan dengan pemilik account.  
Misalnya, inisial, nomor telepon, jabatan, unit organisasi, dll.
- ⇒ Jangan memakai deretan kunci keyboard, seperti qwerty.
- ⇒ Jangan memakai semua yang disebut di atas walaupun dibalik urutannya, atau kombinasi huruf besar kecil.
- ⇒ Jangan memakai password serba numerik.
- ⇒ Jangan memakai contoh password yang ada di buku keamanan jaringan, sebaik apapun password tersebut.
- ⇒ Gunakan kombinasi angka dan campuran huruf besar kecil.
- ⇒ Gunakan minimal 6 karakter

⇒ Gunakan pilihan angka dan huruf yang kelihatannya acak.

⇒ Namun password sebaiknya yang gampang diingat. Hindari password yang sukar diingat, sehingga harus ditulis dahulu untuk mengingatnya. Selain itu, password jangan terlalu panjang. Ada juga software yang dapat menjaga agar user mematuhi peraturan-peraturan yang dibuat. Sehingga dalam memasukan password, user dipaksa untuk memasukkan password yang unik, dan sesuai dengan peraturan-peraturan tertentu.

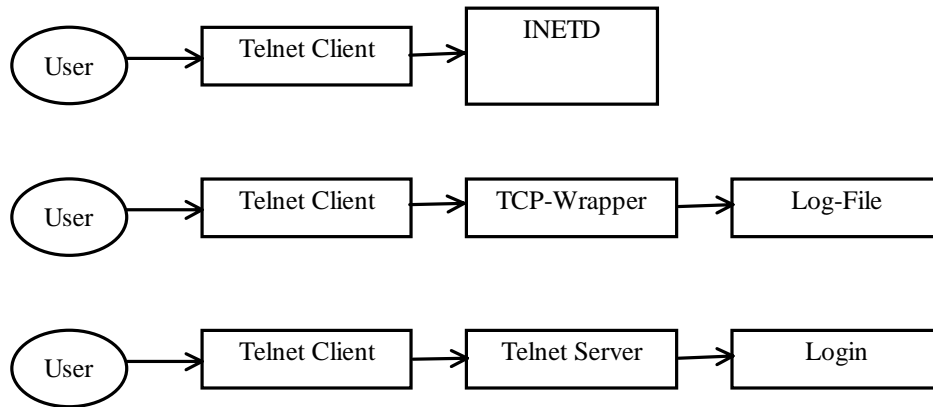
- **server-based password authentication**

Termasuk dalam metoda ini misalnya sistem Kerberos server, TCP-wrapper, dimana setiap service yang disediakan oleh server tertentu dibatasi dengan suatu daftar host dan user yang boleh dan tidak boleh menggunakan service tersebut.



Kerberos server diimplementasikan pada setiap service, dan dimulai ketika seorang user melakukan login pada suatu sistem. Pada prinsipnya, saat seorang user melakukan login, maka program login akan menghubungi Kerberos system untuk mendapatkan 'ticket' untuk akses pada sistem yang disediakan. User sendiri tidak merasakan perbedaan (tidak perlu memberikan password tambahan). Bila user akan menggunakan service-service pada server lainnya, maka sistem dimana user tersebut login akan kembali menghubungi Kerberos system untuk mendapatkan ticket baru untuk service pada server tersebut. Dengan cara ini, dapat dihindari penyusupan melalui metoda 'protocol spoofing', dimana user dari sistem lain yang berusaha menggunakan service-service yang dilindungi

pada sistem tersebut, tidak akan melalui Kerberos system lebih dahulu, sehingga permintaan servicenya akan ditolak oleh server. Disini setiap server (penyedia service) hanya akan melayani permintaan yang disertai ticket dari Kerberos. Tentu saja Kerberos system ini tidak berpengaruh bila si penyusup sudah berhasil memasuki salah satu local account.



TCP-wrapper adalah sistem yang menggunakan metoda ‘access control’ dimana akses terhadap suatu service ke server diblokkan, dilakukan pengecekan terlebih dahulu asal dari permintaan service tersebut, bila ada dalam daftar yang diperbolehkan, maka diteruskan ke server yang sebenarnya.

- **server-based token authentication**

Metoda ini menggunakan authentication system yang lebih ketat, yaitu dengan penggunaan token / smart card, sehingga untuk akses tertentu hanya bisa dilakukan oleh login tertentu dengan menggunakan token khusus.

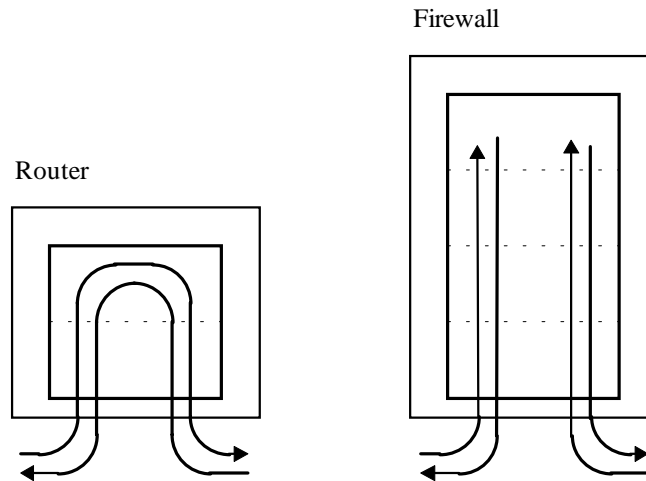
- **Firewall dan Routing Control**

Komputer dengan firewall menyediakan kontrol akses ketat antara sistem dengan sistem lain. Konsepnya, firewall mengganti IP router dengan sistem host multi-home, sehingga IP forwarding<sup>3</sup> tidak terjadi antara sistem dengan sistem lain yang dihubungkan melalui

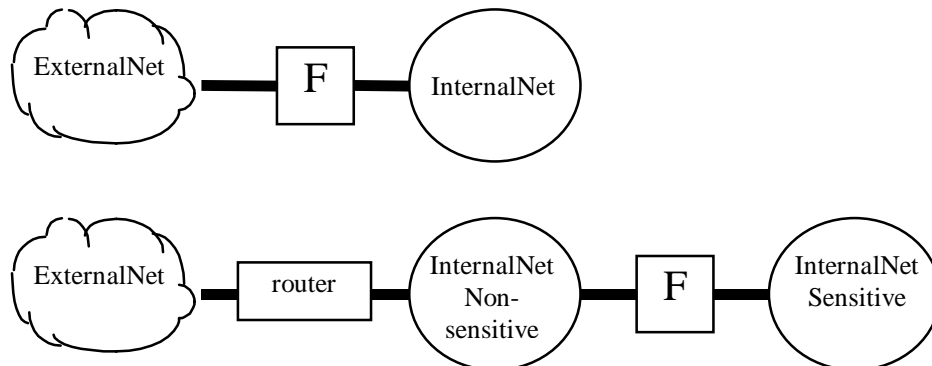
---

<sup>3</sup>IP Forwarding : lihat Configuring routing.

firewall tsb. Agar jaringan internal dapat berhubungan dengan jaringan diluarnya dalam tingkat konektifitas tertentu, firewall menyediakan fingsi-fungsi tertentu.



Firewall mencegah paket IP diteruskan melalui layer IP. Namun, seperti host multi-home, firewall menerima paket dan memprosesnya melalui layer aplikasi. Sebetulnya ada juga router yang mempunyai fasilitas keamanan khusus seperti firewall, dan biasanya disebut 'secure router' atau 'secure gateway'. Namun firewall bukan router, karena tidak meneruskan (forwarding) paket IP. Firewall sebaiknya tidak digunakan untuk memisahkan seluruh jaringan internal dari jaringan luar. Firewall dapat dipakai untuk memisahkan beberapa bagian dari jaringan internal yang sensitif terhadap jaringan non sensitif dan jaringan luar, sedangkan antara jaringan non sensitif dengan jaringan luar digunakan router. Firewall seperti ini disebut firewall internal. Memisahkan sistem bagian yang sensitif dengan yang non sensitif biasanya sulit, sehingga umumnya digunakan firewall external, atau kombinasi keduanya. Namun bila bagian yang sensitif dapat dipisahkan, dan digunakan firewall internal, maka akan lebih baik, sebab tidak seluruh jaringan terisolasi dari jaringan luar.



Dengan adanya firewall, semua paket ke sistem di belakang firewall dari jaringan luar tidak dapat dilakukan langsung. Semua hubungan harus dilakukan dengan mesin firewall. Karena itu sistem keamanan di mesin firewall harus sangat ketat. Dengan demikian lebih mudah untuk membuat sistem keamanan yang sangat ketat untuk satu mesin firewall, daripada harus membuat sistem keamanan yang ketat untuk semua mesin di jaringan lokal (internal).

Kerugiannya, host lokal tidak dapat mengakses jaringan luar. Untuk itu, firewall harus menyediakan beberapa fungsi yang tidak ada di router :

- ⇒ DNS, name service untuk dunia luar. Name service untuk host lokal ditangani sistem internal. Firewall menyediakan name service terbatas untuk jaringan luar. Name server ini tidak menyediakan nama atau informasi tentang host lokal.
- ⇒ E-mail forwarding. Pada sistem firewall, sendmail dikonfigurasi untuk meneruskan mail ke tiap user pada semua sistem internal. Setiap user dikenali melalui alias. Mail keluar di-rewrite sehingga user internal seakan-akan ada pada sistem firewall. Nama login dengan nama host internal tidak dikenal dari luar.
- ⇒ Service ftp. Semua transfer dengan ftp harus melalui firewall. Jadi dari luar hanya bisa ftp ke sistem firewall. Anonymous ftp hanya ada di firewall. Dari dalam, untuk ftp keluar, harus login dahulu ke firewall, baru bisa ftp keluar.
- ⇒ Telnet atau rlogin. Untuk bisa telnet atau rlogin dari atau keluar, maka harus rlogin atau telnet dahulu ke firewall.

Hanya fasilitas tersebut diatas saja yang disediakan oleh firewall. Fasilitas lainnya, seperti NIS, NFS, rsh, rcp, finger dll tidak boleh ada pada firewall. Pada sistem firewall, keamanan lebih penting daripada fasilitas.

Sistem firewall bekerja dengan cara menginterupsi proses routing antara sistem yang dilindungi dengan sistem luar. Jadi menggunakan metoda control routing. Dengan routing table statis hal ini dapat dilakukan. Dalam routing table, ditentukan network mana saja yang dapat berkomunikasi, dan lewat mana hubungan dilakukan. Jadi routing table-nya tidak mempunyai default route, dan hanya mempunyai routing untuk host luar tertentu saja, selain routing lokal. Misalnya, beberapa host ee.itb.ac.id pada subnet

167.205.8.64 (4 bit untuk host address) dengan routernya 167.205.8.80, dilindungi dengan sistem routing control seperti firewall, untuk subnet tersebut. Host-host tersebut hanya berhubungan dengan host lokal, dan host luar tertentu, yaitu dns.paume.itb.ac.id pada address 167.205.22.120 dan maingtw.paume.itb.ac.id pada 167.205.31.131. Maka routing table pada host hampton.ee.itb.ac.id dengan address 167.205.8.79 sebagai berikut :

Destination	Gateway	Interface
127.0.0.1	127.0.0.1	lo0
167.205.8.64	167.205.8.79	ed0
167.205.22.120	167.205.8.80	ed0
167.205.31.131	167.205.8.80	ed0

Disini tidak ada default route. Selain itu tidak boleh ada program dynamic routing protocol yang sedang dijalankan atau yang dijalankan sewaktu startup sistem. Default routing pun tidak boleh didefinisikan saat startup. Yang ada hanya route static tertentu saja yang didefinisikan saat startup.

Cara seperti ini tingkat keamanannya tidak sekeras firewall, tidak membutuhkan program-program khusus. Namun konfigurasi sistem harus dilakukan pada semua host pada sistem tersebut, sedangkan pada firewall, konfigurasi sistem cukup dilakukan pada mesin firewall saja. Namun cara di atas dapat menjadi alternatif yang mungkin dilakukan.

### **5.2.2 Metoda enkripsi**

Salah satu cara pembatasan akses adalah dengan enkripsi. Proses enkripsi meng-encode data dalam bentuk yang hanya dapat dibaca oleh sistem yang mempunyai kunci untuk membaca data. Proses enkripsi dapat dengan menggunakan software atau hardware. Hasil enkripsi disebut cipher. Cipher kemudian didekripsi dengan device dan kunci yang sama tipenya (sama hardware/softwarenya, sama kuncinya). Dalam jaringan, sistem enkripsi harus sama antara dua host yang berkomunikasi. Jadi diperlukan kontrol terhadap kedua sistem yang berkomunikasi. Biasanya enkripsi digunakan untuk suatu sistem yang seluruhnya dikontrol oleh satu otoritas.

Beberapa alasan penggunaan enkripsi :

- mencegah orang yang tidak berwenang melihat data-data sensitif
- mengurangi kemungkinan terbukanya data rahasia tanpa sengaja
- mencegah orang-orang yang mempunyai akses istimewa (mis: sistem admin) agar tidak dapat melihat data pribadi
- untuk mempersulit usaha intruder memasuki sistem

Metoda enkripsi bukan solusi terbaik keamanan jaringan, karena ada enkripsi yang bisa menyebabkan hilangnya data. Selain itu, enkripsi juga masih bisa dipecahkan. Pada sistem unix, biasanya digunakan standar enkripsi crypt dan/atau des. Data encryption standard, des, teknik enkripsi modern yang dibentuk tahun 70-an. Sedangkan crypt berdasar dari teknik enkripsi mesin Enigma Jerman (perang dunia dua). Dari keduanya, des lebih bagus.

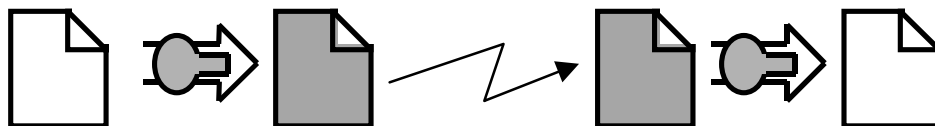
Program crypt dan des membaca data dari standar input, menghasilkan keluaran di standar output, membutuhkan kunci untuk enkripsi. Kunci ini , seperti password harus sukar untuk diduga, namun mudah untuk diingat. Hal-hal untuk password berlaku juga untuk kunci ini. Penggunaan des dan crypt ini dapat dilihat dari manual perintah tersebut pada sistem.

Bila file yang di-enkripsi adalah file teks, maka kemungkinan file tersebut dapat di-dekripsi oleh program pemecah enkripsi lebih besar, dibanding bila file data yang di-enkripsi tersebut adalah file binary. Karena itu sebaiknya file-file data penting yang akan di-enkripsi sebaiknya digabungkan dahulu dengan program tar, lalu di-compress atau dengan program gzip. Hasilnya baru di-enkripsi.

Metoda enkripsi dalam pengiriman data yang dapat dilakukan ada bermacam-macam, antara lain :

- **Data Encryption Standard, des**

Diperlukan satu kunci untuk meng-encode dan men-decode data.

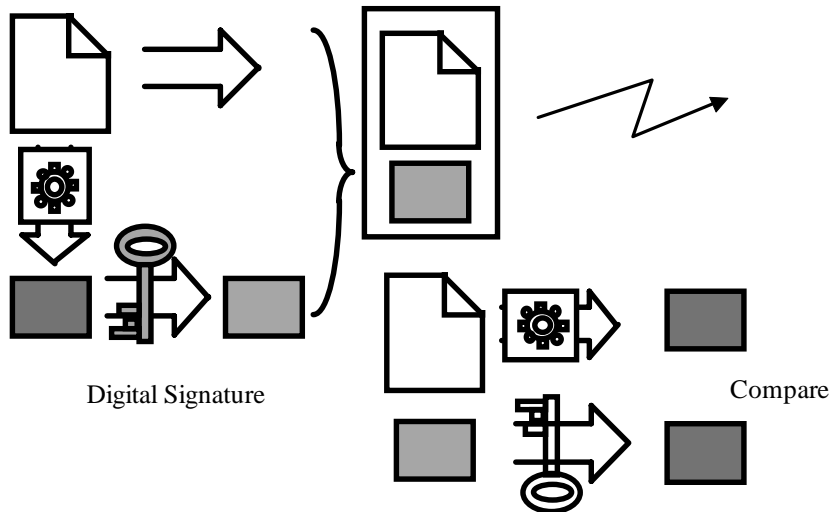
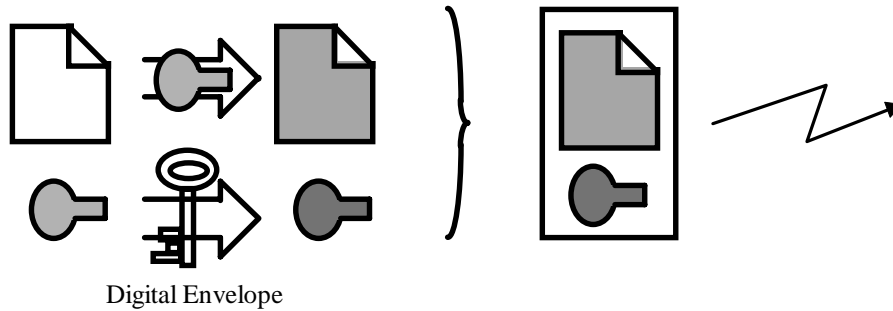
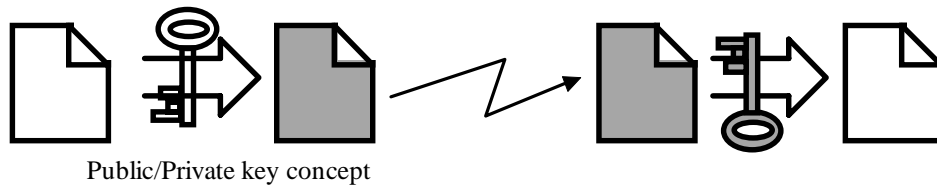


- **RSA Public/Private key concept**

Pengirim data memerlukan satu Public key untuk meng-encode data, si penerima data akan men-decode data dengan satu kunci khusus Private key yang hanya dimiliki olehnya saja. Sistem ini lebih baik keamanannya daripada des, namun kurang cepat. Misal : PGP

- **Digital Envelope**

Merupakan gabungan des dengan Public/Private key concept. Data dikirimkan dengan ter-enkripsi des, dengan kunci tertentu. Kunci des tersebut kemudian dienkripsi dengan Public key milik si penerima, dan digabungkan dengan data yang sudah ter-enkripsi. Penerima data akan membuka kunci des yang ter-enkripsi dengan Private key yang dimilikinya. Lalu kunci des yang dihasilkan digunakan untuk membuka data. Disini digunakan des sebagai enkriptor data, karena kecepatannya yang lebih baik dibandingkan penggunaan Public/Private key. Sedangkan keamanannya terjamin oleh penggunaan Public/Private key terhadap kunci des yang dipakai.



- **Digital Signature**

Digunakan untuk data yang terbuka untuk umum (public accessible) namun dijaga kebenarannya (seperti penggunaan checksum pada sistem kompresi file, sistem transmisi data). Untuk itu pada data tersebut ditambahkan 'signature'. Signature ini dibuat dari data yang akan dikirimkan, yang diproses dengan algoritme tertentu (hashing algorithm) menjadi 'message digest', lalu message digest tersebut di-encode dengan Private key si pengirim, menjadi digital signature untuk data tersebut. Si penerima dapat memastikan kebenaran (authentication) data yang dikirimkan dengan men-decode digital signature menjadi message digest dengan menggunakan Public key, lalu membandingkannya dengan message digest yang dibuat dari data yang diproses dengan algoritme tertentu (dalam hal ini hashing algorithm).