# Bab 19

# Kebutuhan Akan Kriptografi

Penggunaan kriptografi mempunyai sejarah yang cukup panjang. Julius Caesar diketahui menggunakan *substitution cipher* untuk mengenkripsi pesan rahasia. Di jaman yang lebih modern, kriptografi digunakan oleh militer untuk merahasiakan perintah strategis melalui jalur komunikasi radio. Pesan rahasia antara pemerintahan suatu negara dengan misi diplomatiknya juga diamankan menggunakan kriptografi.

Dewasa ini, kriptografi tidak hanya dibutuhkan oleh militer dan misi diplomatik. Kemajuan teknologi komunikasi dan komputer membuat kriptografi dibutuhkan oleh kalangan yang lebih luas, bahkan boleh dikatakan bahwa semua orang yang menggunakan internet menggunakan kriptografi, meski sering tanpa disadari. Di bab ini, kita akan bahas beberapa situasi dimana kriptografi dibutuhkan.

## 19.1 Informasi Sensitif

Setiap orang, perusahaan, institusi dan instansi pemerintahan mempunyai informasi sensitif yang sebaiknya tidak jatuh ketangan orang yang tidak berhak untuk mendapatkannya. Contoh dari informasi sensitif seseorang secara pribadi antara lain:

- Informasi kesehatan pribadi.
- Informasi keuangan pribadi dan pola belanja.

Dari sisi kepentingan umum, memang ada informasi kesehatan pribadi yang dibutuhkan oleh instansi tertentu, misalnya untuk pencegahan penularan pe-

nyakit. Namun dari sisi pribadi, informasi kesehatan adalah sesuatu yang sensitif. Tentunya ada informasi yang perlu diketahui oleh dokter dan rumah sakit, misalnya kondisi jantung atau masalah alergi terhadap obat-obat tertentu. Tetapi jika informasi kesehatan pribadi disebar-luaskan, ada kemungkinan timbul tindakan atau reaksi diskriminatif terhadap yang bersangkutan. Informasi kesehatan pribadi juga bisa menjadi bahan untuk gosip. Demikian juga dengan informasi keuangan, instansi tertentu seperti instansi perpajakan mungkin perlu mengetahui informasi keuangan pribadi. Namun elemen-elemen kriminal dapat menggunakan informasi keuangan dan pola belanja seseorang untuk melakukan perbuatan kriminal.

Suatu perusahaan juga mempunyai informasi sensitif atau rahasia yang sebaiknya tidak disebar-luaskan. Contoh informasi sensitif yang perlu dirahasiakan oleh suatu perusahaan termasuk:

- Cara pembuatan suatu produk.
- Rencana strategis yang rinci.

Meskipun dari sisi pemegang saham, perusahaan diinginkan agar transparan, tentunya ada rahasia perusahaan seperti resep pembuatan suatu produk, yang jika jatuh ke perusahaan lain, akan menguntungkan perusahaan lain dan merugikan perusahaan pemilik resep. Kadang, rencana strategis yang rinci juga perlu dirahasiakan.

Untuk suatu institusi, contoh informasi sensitif termasuk:

- Alamat, nomor telpon dan email anggota institusi.
- Nilai akademis.

Kerap seorang anggota institusi tidak ingin informasi pribadinya diberikan kepada pihak ketiga. Informasi pribadinya bisa berupa alamat, nomor telpon dan email. Suatu institusi pendidikan seperti universitas juga menyimpan informasi sensitif. Sebagai contoh, nilai akademis mahasiswa sebaiknya tidak bisa begitu saja diberikan ke pihak ketiga tanpa persetujuan mahasiswa.

Suatu instansi pemerintahan juga memiliki informasi yang sensitif, sebagai contoh antara lain:

- Informasi pribadi pembayar pajak.
- Data mengenai persenjataan militer.

Meskipun publik menginginkan instansi pemerintahan yang transparan, ada informasi tertentu yang sensitif dan perlu dirahasiakan. Sebagai contoh, instansi perpajakan sebaiknya merahasiakan informasi pribadi seorang pembayar pajak, kecuali jika informasi tersebut diperlukan untuk kepentingan hukum. Contoh

lain adalah instansi militer dimana informasi tertentu mengenai persenjataan atau pergerakan pasukan dimasa perang perlu dirahasiakan.

Seseorang atau suatu organisasi tentunya bertanggung jawab atas kerahasiaan informasi sensitif yang dimilikinya, dan kriptografi dapat membantu menjaga kerahasiaan informasi sensitif yang disimpan secara elektronik. Berbagai langkah menggunakan kriptografi dapat diambil untuk menjaga kerahasiaan informasi sensitif yang disimpan secara elektronik termasuk:

- *Access control* terhadap informasi.
- Enkripsi data dalam transit.
- Enkripsi data dalam media penyimpanan.

Di jaman sekarang dimana komputer saling terhubung, *access control* bukan semata kontrol secara fisik, namun juga harus meliputi kontrol *access* secara *online*. Ini biasanya dilakukan menggunakan *password* atau *passphrase* dan diamankan menggunakan kriptografi sebagai berikut:

- menggunakan *secure hashing* untuk penyimpanan di *server*, dan
- menggunakan enkripsi untuk transmisi.

Data sensitif dalam transit juga perlu diamankan menggunakan enkripsi. Definisi data dalam transit juga mungkin perlu diperluas, bukan saja data yang sedang ditransmisi melalui jalur komunikasi, tetapi meliputi juga data dalam *notebook computer* dan *flash disk* yang keduanya dapat saja dicuri atau hilang. Dalam prakteknya, pengamanan data dalam transit dapat dilakukan dengan:

- Menggunakan *secure session* seperti SSL/TLS, SSH dan IPsec (akan dibahas di bab 20).
- Mengenkripsi *file* atau *file system* dalam *flash disk* dan *hard drive notebook computer*.

Untuk tingkat pengamanan yang lebih tinggi lagi, bukan hanya data sensitif yang disimpan dalam *flash disk* dan *hard drive notebook computer* saja yang perlu dienkripsi, tetapi juga data sensitif yang disimpan di media penyimpanan lain seperti *hard drive* untuk *desktop computer*. Ini terutama jika media dapat diakses oleh orang yang tidak diinginkan mengakses data sensitif tersebut.

## 19.2 Mencegah Penyadapan

Jika mendengar kata "penyadapan" maka yang terbayang di pikiran pembaca mungkin penyadapan oleh agen asing atau penyadapan oleh penegak hukum. Namun dewasa ini penyadapan komunikasi dapat dilakukan oleh siapa saja,

termasuk elemen kriminal, dengan peralatan yang relatif murah. Secara umum, komunikasi nirkabel rentan terhadap penyadapan karena penyadap tidak perlu akses fisik ke kabel komunikasi. Berikut adalah beberapa macam penyadapan yang sebagian diantaranya dapat dicegah menggunakan enkripsi:

- Penyadapan komunikasi nirkabel.
- Penyadapan komunikasi dengan kabel (tembaga maupun optik).
- Penyadapan radiasi elektromagnetik.
- Penyadapan akustik.

Dua standard komunikasi lokal nirkabel yang populer adalah Wi-Fi (IEEE 802.11) dan Bluetooth. Kedua protokol sebenarnya sudah menyediakan enkripsi, Wi-Fi melalui WEP dan WPA, dan Bluetooth melalui *security mode* 2, 3 dan 4 dan *encryption mode* 2 dan 3. Untuk Wi-Fi, sebaiknya WPA digunakan jika ada karena WEP terlalu mudah untuk dipecahkan (lihat 6.1). Akan tetapi ini tidak cukup jika kunci WPA atau WEP yang digunakan adalah kunci bersama, jadi sebaiknya gunakan enkripsi tambahan untuk data yang sensitif, contohnya menggunakan SSH (lihat bagian 20.2). Jika pembaca ingin rekomendasi yang lebih rinci mengenai pengamanan Wi-Fi yang sudah mendukung WPA, silahkan membaca [nis07]. Untuk Wi-Fi yang belum mendukung WPA, silahkan membaca [nis08a]. Bluetooth lebih rentan terhadap penyadapan karena limitasi perangkat, baik limitasi fitur keamanan yang ada dalam perangkat, maupun limitasi yang diakibatkan kesalahan implementasi fitur keamanan dalam perangkat. Jadi untuk Bluetooth, sebaiknya gunakan enkripsi tambahan untuk data sensitif. Untuk informasi yang lebih rinci mengenai pengamanan Bluetooth, silahkan membaca [nis08b]. Untuk komunikasi data sensitif melalui jaringan selular, jelas enkripsi tambahan diperlukan.

Hampir semua komunikasi melalui kabel menggunakan protokol internet yaitu TCP/IP. Sebetulnya, pada *layer* IP sudah tersedia pengamanan menggunakan enkripsi yaitu IPsec, yang akan dibahas di bagian 20.3. Namun untuk orang awam, *deployment* IPsec agak lebih sulit dibandingkan pengamanan sesi pada *layer* atas seperti SSL/TLS (akan dibahas di bagian 20.1) dan SSH (akan dibahas di bagian 20.2).

Untuk mencegah informasi bocor lewat radiasi elektromagnetik dari perangkat, biasanya perangkat dilindungi dengan *Faraday's cage*, yaitu "sangkar" dari bahan logam. Tentunya enkripsi sebaiknya tetap digunakan untuk komunikasi data sensitif dari/ke perangkat.

Penyadapan akustik bukan hanya penyadapan percakapan. Suara dari penggunaan *keyboard* dapat disadap, dan dengan analisa statistik frekuensi penggunaan setiap kunci di *keyboard*, apa yang diketik di *keyboard* dapat diketahui. Kemungkinan penyadapan akustik mungkin tidak terlalu besar dibandingkan kemungkinan adanya *trojan* yang melakukan *keyboard logging*. Namun

jika pembaca paranoid atau sedang menginput suatu rahasia negara yang sangat sensitif, maka pembaca sebaiknya menggunakan *keyboard* dalam ruangan kedap suara. Enkripsi secara tradisional tidak akan membantu untuk masalah ini. Yang mungkin dapat dilakukan adalah memancarkan juga secara *acak* bunyi berbagai kunci bersamaan dengan penggunaan *keyboard*. Jadi bunyi kunci yang ditekan bercampur dengan bunyi kunci secara acak. Konsep ini mirip dengan *steganography*, yaitu penyembunyian pesan dalam sesuatu yang lebih besar (contohnya dalam *file* gambar atau *file* audio). Bedanya, dalam *steganography*, orang yang kepada siapa pesan ditujukan, diharapkan dapat membaca pesan yang terpendam.

## 19.3 Mencegah Penyamaran

Di era *online* dimana komunikasi dilakukan melalui jaringan internet, identitas orang atau komputer yang hendak berkomunikasi dengan kita kadang perlu dipastikan. Sebagai contoh, jika akses ke suatu sistem informasi hanya diperbolehkan untuk pengguna yang telah terdaftar, maka sistem harus memastikan bahwa seorang yang ingin mengakses sistem adalah pengguna yang telah terdaftar. Berbagai contoh situasi dimana identitas perlu dipastikan antara lain:

- Seorang yang mengaku pengguna dan ingin mengakses sistem memang benar pengguna yang telah terdaftar.
- *Website* yang sedang kita kunjungi dan kepada siapa kita hendak mengirim nomor kartu kredit memang benar *website* yang kita kehendaki.
- Perangkat yang sedang mencoba untuk bergabung dalam jaringan komunikasi lokal nirkabel memang perangkat yang diperbolehkan untuk bergabung.

Memastikan identitas pengguna adalah bagian dari *access control* yang telah sedikit dibahas di bagian 19.1. Memastikan identitas kerap disebut *authentication*. Tren saat ini adalah menggunakan *multiple-factor authentication* yaitu menggunakan beberapa atribut unik pengguna sistem untuk identifikasi. Sifat atribut dapat berupa:

- Atribut langsung pengguna (*what you are*) misalnya sidik jari.
- Benda yang dimiliki pengguna (*what you have*) misalnya suatu *token*.
- Apa yang diketahui pengguna (*what you know*) misalnya *password* atau kunci privat.

Enkripsi berperan dalam mengamankan komunikasi mengenai apa yang diketahui pengguna, baik *password* maupun *authentication* menggunakan *public*

*key cryptography*. Tentunya *access control* bukan hanya memastikan identitas, tetapi juga meliputi kontrol terhadap apa yang dapat diakses oleh pengguna sistem. Kerap apa yang dapat diakses oleh satu pengguna berbeda dengan apa yang dapat diakses pengguna lain. Kontrol terhadap apa yang dapat diakses berbagai pengguna sistem dapat diamankan menggunakan kriptografi misalnya dengan mengenkripsi *file*.

Memastikan bahwa suatu *website* bukan merupakan penyamaran biasanya dilakukan menggunakan protokol SSL/TLS (lihat bagian 20.1) dimana identitas *website* didukung penggunaan *certificate* yang dikeluarkan suatu *certificate authority*. Akan tetapi kerap ini sebenarnya bukan apa yang diperlukan pengguna (lihat pembahasan di bagian 26.3).

Memastikan bahwa perangkat yang akan bergabung dalam jaringan komunikasi lokal nirkabel adalah perangkat yang diperbolehkan untuk bergabung sudah didukung oleh standard Wi-Fi dan Bluetooth. Untuk Wi-Fi, biasanya perangkat yang ingin bergabung (melalui *access point*) harus mengetahui kunci WPA untuk jaringan (tentunya ini hanya bisa jika jaringan menggunakan WPA). Untuk Bluetooth versi sebelum 2.1, dengan *security mode* 2 atau 3, *authentication* dilakukan menggunakan PIN. Untuk versi 2.1, dengan *security mode* 4, *authentication* dilakukan menggunakan Elliptic Curve Diffie-Hellman (lihat bab 17). Untuk informasi lebih rinci mengenai pengamanan Bluetooth, silahkan membaca [nis08b].

## 19.4 Ringkasan

Di bab ini telah dibahas berbagai situasi dimana kriptografi dibutuhkan. Telah dibahas kebutuhan pengamanan informasi sensitif, pencegahan penyadapan dan pencegahan penyamaran. Kriptografi berperan besar dalam melayani tiga kebutuhan tersebut. Bab-bab selanjutnya akan menjelaskan secara lebih rinci penggunaan kriptografi dalam melayani tiga kebutuhan tersebut.