Bab 1

Pendahuluan

Di jaman Romawi kuno, Julius Caesar telah menggunakan teknik kriptografi yang dijuluki *Caesar cipher* untuk mengirim pesan secara rahasia, meskipun teknik yang digunakannya sangat tidak memadai untuk ukuran kini. Casanova menggunakan pengetahuan mengenai kriptografi untuk mengelabui Madame d'Urfé (ia mengatakan kepada Madame d'Urfé bahwa sesosok jin memberi tahu kunci rahasia Madame d'Urfé kepadanya, padahal ia berhasil memecahkan kunci rahasia berdasarkan pengetahuannya mengenai kriptografi), sehingga ia mampu mengontrol kehidupan Madame d'Urfé secara total. Sewaktu perang dunia kedua, pihak sekutu berhasil memecahkan kode mesin kriptografi Jerman, Enigma; keberhasilan yang sangat membantu pihak sekutu dalam memenangkan perang[1]. Sejarah kriptografi penuh dengan intrik dan banyak orang melihat kriptografi sebagai sesuatu yang penuh dengan misteri.

Juga banyak orang yang menganggap pengetahuan dan penggunaan kriptografi sebagai perbuatan subversif, bahkan Amerika Serikat pernah memperlakukan kriptografi sebagai senjata yang tidak dapat diekspor secara bebas, meskipun sekarang peraturan sudah diperlunak. Di satu sisi pemerintah AS tidak menginginkan warganya dan pihak lain menggunakan kriptografi untuk berbagai macam keperluan, di sisi lain kriptografi sangat diperlukan dalam aplikasi pengamanan teknologi informasi seperti transaksi perbankan. Ada beberapa negara, baik negara belum maju yang memiliki pemerintahan represif maupun negara barat yang "liberal", yang melarang atau membatasi penggunaan kriptografi.

Pro dan kontra penggunaan kriptografi tidak akan dibahas dalam buku ini. Tujuan buku ini adalah untuk mengungkap tabir misteri yang menutupi ilmu kriptografi. Ini dilakukan dengan memperkenalkan berbagai konsep dasar krip-

[1]Setelah perang berahir, konon pihak sekutu menjual mesin Enigma ke beberapa negara berkembang tanpa memberi tahu bahwa kode sudah dipecahkan.

tografi, penjelasan mengenai teori matematika dan teknik-teknik kriptografi, contoh-contoh aplikasi kriptografi, diskusi mengenai kendala aplikasi kriptografi, dan diskusi mengenai masa depan kriptografi.

Konsep-konsep dasar kriptografi sangat perlu untuk dipahami, karena tanpa konsep dasar, segala macam teori matematika tidak ada gunanya. Berbagai konsep yang akan dibahas antara lain: konsep acak, *one-time pad*, *cryptanalysis*, berbagai operasi dasar untuk kriptografi, dan manajemen kunci.

Berbagai teknik enkripsi klasik akan dibahas, mulai dari yang sederhana seperti transformasi linear dan transformasi *affine*, sampai dengan *stream cipher* dan *block cipher*. Teknik enkripsi yang lemah dibahas bukan untuk diimplementasi, tetapi agar pembaca dapat lebih memahami apa kelemahannya dan bagaimana teknik enkripsi yang lebih tangguh menanggulanginya. Teknik-teknik yang digunakan untuk mencari atau mengeksploitasi kelemahan enkripsi antara lain analisa frekuensi, *differential cryptanalysis* dan *linear cryptanalysis*. Matematika yang digunakan untuk transformasi enkripsi juga akan dibahas secara rinci sebelum pembahasan teknik enkripsi, akan tetapi pembahasan teori probabilitas dan statistika hanya sebatas penggunaan.

Buku ini tidak merekomendasikan penggunaan *stream cipher* karena sangat mudah untuk menggunakannya secara tidak aman. Algoritma RC4 jelas merupakan algoritma yang lemah. Semua ini akan dibahas di bab 6.

Cryptographically secure hashing juga akan dibahas di buku ini, termasuk MD5 dan SHA. Sebagai contoh analisa kekuatan algoritma *hashing*, *differential cryptanalysis* terhadap MD5 akan dibahas.

Teknik-teknik kriptografi *public key* yang dibahas termasuk yang berbasis pada sukarnya penguraian bilangan yang sangat besar (contohnya RSA), yang berbasis pada sukarnya komputasi logaritma diskrit (contohnya ElGamal), dan juga yang menggunakan *elliptic curve* menggantikan *finite field*. Teknik yang bersifat probabilistik, yaitu *zero-knowledge protocol*, dan algoritma Merkle-Hellman untuk enkripsi *knapsack* dengan kelemahannya, juga akan dibahas. Untuk memberi gambaran mengenai sukarnya penguraian dan komputasi logaritma diskrit, berbagai teknik penguraian dan komputasi logaritma diskrit dibahas.

Algoritma Euclid, *Fermat's Little Theorem* dan *Chinese Remainder Theorem* adalah 3 topik sangat penting dan umum yang wajib dikuasai oleh setiap murid kriptografi atau ilmu komputer. Sebaliknya, bab mengenai *algebraic number* dan bagian yang membahas metode *number field sieve* berisi bahan tingkat sangat lanjut dan khusus, jadi mungkin sebaiknya tidak digunakan dalam mata kuliah tingkat awal.

Quantum key distribution juga akan dibahas. Jika *quantum key distribution* menjadi sesuatu yang praktis, maka enkripsi *one-time pad* juga akan menjadi sesuatu yang praktis. Namun *quantum key distribution* bersifat *point-to-point* secara fisik, jadi aplikasinya terbatas.

Berbagai aplikasi kriptografi akan dibahas, termasuk aplikasi untuk pengamanan sesi, aplikasi pengamanan *email*, aplikasi *authentication*, *public key infrastructure* dan *cryptographic library*.

Kendala aplikasi kriptografi terutama disebabkan oleh kurangnya pemahaman mengenai kriptografi sehingga banyak terjadi penggunaan kriptografi dengan cara yang salah, terutama dalam hal *key management*. Penggunaan kriptografi harus dengan cara yang benar, dan implementasi harus dengan teliti dan hati-hati. Kalau tidak, akibatnya adalah kriptografi yang mudah untuk dipecahkan. Penggunaan kriptografi secara benar bukan sesuatu yang mudah dan sejarah penggunaan kriptografi menunjukkan bahwa kesalahan tidak hanya dilakukan oleh mereka yang "gagap teknologi." Perusahaan besar dibidang teknologi informasi seperti Microsoft dan Netscape juga pernah melakukan implementasi yang tidak aman seperti enkripsi *password* yang sangat mudah untuk dipecahkan. Pakar-pakar protokol komunikasi juga telah sering membuat kesalahan, sebagai contoh versi pertama dari pengamanan Wi-Fi (protokol komunikasi nirkabel) yaitu WEP menggunakan *stream cipher* RC4 secara tidak aman (lihat bab 6). Selain masalah sulitnya manajemen kunci, rumitnya sistem dan sistem yang tidak sesuai kebutuhan menjadi kendala penggunaan kriptografi.

Cara kerja protokol yang digunakan untuk sistem pengamanan dengan kriptografi sangat menentukan keamanan sistem. Oleh sebab itu suatu metode untuk menganalisa protokol kriptografi akan dibahas. Metode ini menggunakan pendekatan logika klasik.

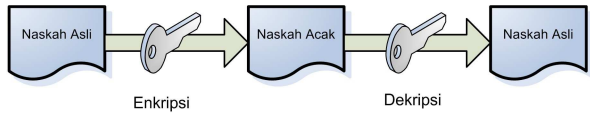
Masa depan kriptografi akan dipengaruhi oleh perkembangan matematika, terutama dalam hal algoritma, dan juga akan dipengaruhi oleh perkembangan di bidang *hardware*. Potensi *quantum computing* juga berperan sangat besar: jika *quantum computer* dapat direalisir maka teknik kriptografi yang digunakan sekarang tidak akan berfungsi efektif karena kunci akan dapat dengan mudah dipecahkan.

Bab 2

Konsep-konsep Dasar

Apakah sebenarnya kriptografi itu? Kriptografi adalah ilmu mengenai teknik enkripsi dimana data diacak menggunakan suatu kunci enkripsi menjadi sesuatu yang sulit dibaca oleh seseorang yang tidak memiliki kunci dekripsi. Dekripsi menggunakan kunci dekripsi mendapatkan kembali data asli. Proses enkripsi dilakukan menggunakan suatu algoritma dengan beberapa parameter. Biasanya algoritma tidak dirahasiakan, bahkan enkripsi yang mengandalkan kerahasiaan algoritma dianggap sesuatu yang tidak baik. Rahasia terletak di beberapa parameter yang digunakan, jadi kunci ditentukan oleh parameter. Parameter yang menentukan kunci dekripsi itulah yang harus dirahasiakan (parameter menjadi ekuivalen dengan kunci).

Dalam kriptografi klasik, teknik enkripsi yang digunakan adalah enkripsi simetris dimana kunci dekripsi sama dengan kunci enkripsi. Untuk *public key cryptography*, diperlukan teknik enkripsi asimetris dimana kunci dekripsi tidak sama dengan kunci enkripsi. Enkripsi, dekripsi dan pembuatan kunci untuk teknik enkripsi asimetris memerlukan komputasi yang lebih intensif dibandingkan enkripsi simetris, karena enkripsi asimetris menggunakan bilangan-bilangan yang sangat besar. Namun, walaupun enkripsi asimetris lebih "mahal" dibandingkan enkripsi simetris, *public key cryptography* sangat berguna untuk *key management* dan *digital signature*.



Gambar 2.1: Proses enkripsi dan dekripsi

Gambar diatas menunjukkan efek dari proses enkripsi dan proses dekripsi.