RESUME

ACCESS CONTROL

Mata Kuliah Keamanan Informasi

Dosen : Triawan Adi Cahyanto, M.Kom

Oleh :

DIAH SUSANTIKA

1310652022

FAKULTAS TEKNIK

PROGRAM STUDI TEKNIK INFORMATIKA

UNIVERSITAS MUHAMMADIYAH JEMBER

2015

KRIPTOGRAFI

Kriptografi (atau kriptologi; dari bahasa Yunani κρυπτός *kryptós*, "tersembunyi, rahasia"; dan γράφειν *graphein*, "menulis", atau -λογία logi, "ilmu") merupakan keahlian dan ilmu dari cara-cara untuk komunikasi aman pada kehadirannya di pihak ketiga. Secara umum, kriptografi ialah mengenai mengkonstruksi dan menganalisis protokol komunikasi yang dapat memblokir lawan; berbagai aspek dalam keamanan informasi seperti data rahasia, integritas data, autentikasi, dan non-repudansi merupakan pusat dari kriptografi modern. Kriptografi modern terjadi karena terdapat titik temu antara disiplin ilmu matematika, ilmu komputer, dan teknik elektro. Aplikasi dari kriptografi termasuk ATM, password komputer, dan E-commerce.

Kriptografi sebelum pada termodernisasi merupakan sinonim dari *enkripisi*, konversi dari kalimat-kalimat yang dapat dibaca menjadi kelihatan tidak masuk akal. Pembuat dari pesan enkripsi membagi teknik pemecahan sandi yang dibutuhkan untuk mengembalikan informasi asli jika hanya dengan penerima yang diinginkan, sehingga dapat mencegah orang yang tidak diinginkan melakukan hal yang sama. Sejak Perang Dunia I dan kedatangan komputer, metode yang digunakan untuk mengelola kriptologi telah meningkat secara komplek dan pengaplikasiannya telah tersebar luar.

Kriptografi modern sangat didasari pada teori matematis dan aplikasi komputer; algoritma kriptografi didesain pada asumsi ketahanan komputasional, membuat algoritma ini sangat sulit dipecahkan oleh musuh. Secara teoritis, sangat sulit memecahkan sistem kriptografi, namun tidak layak melakukannya dengan cara-cara praktis. Skema ini oleh karena itu disebut sangat aman secara komputasional; kemajuan teoritis dapat meningkatkan algoritma faktorisasi integer, dan meningkatkan teknologi komputasi yang membutuhkan solusi ini untuk diadaptasi terus-meneus. Terdapat skema keamanan informasi yang benar-benar tidak boleh dapat ditembuh bahkan dengan komputasi yang tak terbatas namun skema ini sangat sulit diimplementasikan.

Teknologi yang berhubungan dengan kriptologi memiliki banyak masalah legal. Di Inggris, penambahan Regulasi Penyelidikan Aksi Wewenang membutuhkan kriminal yang tertuduh harus menyerahkan kunci dekripsinya jika diminta oleh penegah hukum. Jika tidak pengguna akan menghadapi hukum pidana. Electronic Frontier Foundation (EFF) terlibat dalam sebuah kasus di Amerika Serikat yang mempertanyakan jika seorang tersangka harus untuk menyerahkan kunci dekripsi mereka kepada pengak hukum merupakan inkonstitusionil. EFF memperdebatkan bahwa regulasi ini merupakan pelanggaran hak untuk tidak dipaksa mencurigai dirinya sendiri, seperti dalam Amandemen Kelima Konsitusi Amerika