

ANALISA KRIPTOGRAFI UNTUK KEAMANAN DALAM MANAJEMEN SISTEM TERDISTRIBUSI PERUSAHAAN

Diana Laily Fithri
Program Studi Sistem Informasi Universitas Muria Kudus
diana.laily@umk.ac.id

ABSTRACT

Management of distributed system is using cryptography security. Cryptography in Greek means hidden. In this modern era, cryptography is considered as a branch of mathematics and computer applied in management of distributed system as well as related theories and information. Cryptography nowadays is used by many people such as in a system of ATM card security, passwords of computer, electronic trading, and so forth depend on cryptography. Therefore, in this modern era cryptography extremely needs more knowledge and application of modern cryptography challenge, particularly in a field of security management of distributed system.

Keywords: *cryptography, cryptanalysis, cryptology, encryption, decryption*

ABSTRAK

Manajemen dengan sistem terdistribusi menggunakan konsep keamanan kriptografi. Kriptografi dalam bahasa Yunani berarti tersembunyi. Pada zaman modern ini, kriptografi dianggap sebagai cabang dari ilmu matematika dan ilmu komputer diterapkan dalam manajemen dengan sistem terdistribusi, serta teori terkait erat dengan informasi. Kriptografi saat ini banyak digunakan dalam masyarakat maju, misalnya dalam sistem keamanan kartu ATM, password di komputer, perdagangan elektronik, dan lain-lain yang semua tergantung pada kriptografi. Oleh karena itu, di zaman modern ini masih membutuhkan lebih banyak pengetahuan yang mendalam dan pengenalan penerapan tantangan kriptografi modern, khususnya di bidang manajemen keamanan sistem terdistribusi.

Kata kunci: kriptografi, kriptanalisis, kriptologi, enkripsi, dekripsi

Pendahuluan

Keamanan dan kerahasiaan data pada jaringan komputer saat ini menjadi isu yang sangat penting dan terus berkembang. Beberapa kasus menyangkut keamanan jaringan komputer saat ini menjadi suatu pekerjaan yang membutuhkan biaya penanganan dan pengamanan yang sedemikian besar. Sistem-sistem vital, seperti sistem pertahanan, sistem perbankan, sistem bandara udara dan sistem-sistem yang lain setingkat itu, membutuhkan tingkat keamanan yang sedemikian tinggi. Hal ini lebih disebabkan karena kemajuan bidang jaringan komputer dengan konsep open system-nya sehingga siapapun, di manapun dan kapanpun, mempunyai kesempatan untuk mengakses kawasan-kawasan vital tersebut.

Untuk menjaga keamanan dan kerahasiaan pesan, data, atau informasi dalam suatu jaringan komputer maka diperlukan beberapa upaya pengamanan guna membuat pesan, data, atau informasi agar tidak dapat diakses atau gagal pada saat pembacaan.

Saat ini telah banyak metode pengamanan pesan, data, atau informasi yang dikembangkan oleh perusahaan ataupun perorangan. Pengamanan tersebut bisa meliputi pengamanan fisik maupun pengamanan secara digital. Dengan adanya sistem keamanan tersebut, pengguna akan lebih terjamin saat berinteraksi ataupun bertukar data melalui jaringan.