PERANAN KRIPTOGRAFI DALAM PENINGKATAN PENGAMANAN SISTEM INFORMASI

Dedi Purwanto
Universitas Pembangunan Panca Budi
dedipurwanto@pancabudi.ac.id

ABSTRACT

Current technological advances have affected almost all aspects of human life, which can make it easier to exchange data quickly, including in terms of communication. However, in exchange of data, it is still very poorly realized. One of the negative impacts is data theft. Therefore, the security aspect of information exchange and data storage is very important. Especially in the automotive retail sector, where there is a lot of important and confidential data such as customer identity data and financial reports. Because the data is so important, we need a method that can maintain the confidentiality of the data and the method in question is cryptography. The algorithm used is chriptogtaphic algorithm. This algorithm is part of an asymmetric algorithm, each encryption and decryption process has a different key. The purpose of this research is to find a way to implement the cryptographic algorithm into a real application and to produce a desktop-based data security application that is easy to understand and use by the user. This research uses data collection and development methods. The results of this study will be implemented in an application program using a Java-based desktop programming language that makes it easy for everyone who wants to secure important files. In this application the user must create a public key before the encryption process and a private key before the decryption process on the file.Keywords: Floyd Warshall Algorithm, Karo District, GIS
Keywords: *Current Technology, chriptogtaphic algorithm, create public key.*

PENDAHULUAN

Masalah keamanan merupakan salah satu aspek penting dari sebuah sistem informasi. Sayang sekali masalah keamanan ini seringkali kurang mendapat perhatian dari para pemilik dan pengelola sistem informasi. Seringkali masalah keamanan berada di urutan kedua, atau bahkan diurutan terakhir dalam daftar hal-hal yang dianggap penting. Apabila menggangu performansi dari sistem, seringkali keamanan dikurangi atau ditiadakan (Wibowo et al., 2017).

Informasi saat ini sudah menjadi sebuah komoditi yang sangat penting. Kemampuan untuk mengakses dan menyediakan informasi secara cepat dan akurat menjadi sangat esensial bagi sebuah organisasi, baik yang berupa organisasi komersial (perusahaan), perguruan tinggi, lembaga pemerintahan, maupun individual. Hal ini dimungkinkan dengan perkembangan pesat di bidang teknologi komputer dan telekomunikasi (Aryza et al., 2019).

Sangat pentingnya nilai sebuah informasi menyebabkan seringkali informasi diinginkan hanya boleh diakses oleh orang-orang tertentu. Jatuhnya informasi ke tangan pihak lain (misalnya pihak lawan bisnis) dapat menimbulkan kerugian bagi pemilik informasi. Sebagai contoh, banyak informasi dalam sebuah perusahaan yang hanya diperbolehkan diketahui oleh orang-orang tertentu di dalam perusahaan tersebut, seperti misalnya informasi tentang produk yang sedang dalam development, algoritma-algoritma dan teknik-teknik yang digunakan untuk menghasilkan produk tersebut. Untuk itu keamanan dari sistem informasi yang digunakan harus terjamin dalam batas yang dapat diterima (Solly Aryza, et al, 2017).

Keamanan sistem informasi pada saat ini telah banyak dibangun oleh para kelompok analis dan programmer namun pada akhirnya ditinggalkan oleh para pemakainya. Hal tersebut terjadi karena sistem yang dibangun lebih berorientasi pada pembuatnya sehingga berakibat sistem yang dipakai sulit untuk digunakan atau kurang user friendly bagi pemakai, sistem kurang interaktif dan kurang memberi rasa nyaman bagi pemakai, sistem sulit dipahami interface dari sistem menu dan tata letak kurang memperhatikan kebiasaan perilaku pemakai, sistem dirasa memaksa bagi pemakai dalam mengikuti prosedur yang

e-ISSN 2775-4049

dibangun sehingga sistem terasa kaku dan kurang dinamis, keamanan dari sistem informasi yang dibangun tidak terjamin (Siahaan et al., 2018).
Pada pengamanan data informasi sangat penting data itu di enkripsi terlebih dahulu dengan tekhnik kriptografi. Enkripsi dan dekripsi pada umumnya membutuhkan penggunaan sejumlah informasi rahasia, disebut sebagai kunci. Untuk beberapa mekanisme enkripsi, kunci yang sama digunakan baik untuk enkripsi dan dekripsi; untuk mekanisme yang lain, kunci yang digunakan untuk enkripsi dan dekripsi berbeda. Dua tipe dasar dari teknologi kriptografi adalah symmetric key (secret/private key) cryptography dan asymmetric (public key) cryptography (Sugiarto et al., 2018).

Pada symmetric key cryptography, baik pengirim maupun penerima memiliki kunci rahasia yang umum. Pada asymmetric key cryptography, pengirim dan penerima masingmasing berbagi kunci publik dan privat.

Kriptografi saat ini lebih dari enkripsi dan dekripsi saja. Otentikasi menjadi bagian dari kehidupan kita sama seperti privasi. Kita menggunakan otentikasi dalam kehidupan sehari-hari, sebagai contoh saat kita menandatangani sejumlah dokumen dan saat kita berpindah ke dunia dimana keputusan dan persetujuan kita dikomunikasikan secara elektronis, kita membutuhkan tekikteknik untuk otentikasi. Kriptografi menyediakan mekanisme untuk prosedur semacam itu. Digital signature (tanda tangan digital) mengikat dokumen dengan kepemilikan kunci tertentu, sedangkan digital timestamp mengikat dokumen dengan pembuatnya pada saat tertentu.

Hal-hal yang disebutkan diatas dapat disimpulkan bahwa dalam membangun sebuah keamanan sistem informasi harus memiliki orientasi yang berbasis perspektif bagi pemakai bukan menjadi penghalang atau bahkan mempersulit dalam proses transaksi dan eksplorasi dalam pengambilan keputusan. Terdapat banyak cara untuk mengamankan data maupun informasi pada sebuah sistem. Pengamanan data dapat dibagi menjadi dua jenis yaitu : penecegahan dan pengobatan. Pencegahan dilakukan supaya data tidak rusak, hilang dan dicuri, sementara pengobatan dilakukan apabila data sudah terkena virus, sistem terkena worm, dan lubang keamanan sudah diexploitasi.

Keamanan sebuah informasi merupakan suatu hal yang harus diperhatikan. Masalah tersebut penting karena jika sebuah informasi dapat di akses oleh orang yang tidak berhak atau tidak bertanggung jawab, maka keakuratan informasi tersebut akan diragukan, bahkan akan menjadi sebuah informasi yang menyesatkan.

TINJAUAN PUSTAKA

Pengamanan Sistem Informasi

Kriptografi

Kriptografi (cryptography)merupakan ilmu dan seni untuk menjaga pesan agar aman.(Cryptography is the art and science of keeping messages secure. *40+) “Crypto” berarti “secret”(rahasia) dan “graphy” berarti “writing”(tulisan). Para pelaku atau praktisi kriptografi disebut cryptographers. Sebuah algoritma kriptografik (cryptographic algorithm), disebut cipher, merupakan persamaan matematik yang digunakan untuk proses enkripsi dan dekripsi. Biasanya kedua persamaan matematik (untuk enkripsi dan dekripsi) tersebut memiliki hubungan matematis yang cukup erat.Proses yang dilakukan untuk mengamankan sebuah pesan (yang disebut plaintext) menjadi pesan yang tersembunyi (disebut ciphertext) adalah enkripsi (encryption). Ciphertext adalah pesan yang sudah tidak dapat dibaca dengan mudah. Menurut ISO 7498-2, terminologi yang lebih tepat digunakan adalah “encipher”.

Enkripsi

Enkripsi digunakan untuk menyandikan data-data atau informasi sehingga tidak dapat dibaca oleh orang yang tidak berhak. Dengan enkripsi data anda disandikan (encrypted) dengan menggunakan sebuah Password (key). Untuk membuka (decrypt) data tersebut digunakan juga sebuah Password yang dapat sama dengan Password untuk mengenkripsi (untuk kasus privat key cryptography) atau dengan Password yang berbeda (untuk kasus public key cryptography).

METODE PENELITIAN

Didalam keamanan sistem informasi melingkupi empat aspek, yaitu privacy, integrity, authentication, dan availability. Selain keempat hal di atas, masih ada dua aspek lain yang juga sering dibahas dalam kaitannya dengan electronic commerce, yaitu access control dan nonrepudiation.

1. Privacy / Confidentiality

Inti utama aspek privacy atau confidentiality adalah usaha untuk menjaga informasi dari orang yang tidak berhak mengakses.Privacy lebih kearah data-datayang sifatnya privat sedangkan confidentiality biasanya berhubungan dengan data yang diberikan ke pihak lain untuk keperluan tertentu (misalnya sebagai bagian dari pendaftaran sebuah servis) dan hanya diperbolehkan untuk keperluan tertentu tersebut.Contoh hal yang berhubungan dengan privacy adalah e-mail seorang pemakai (user) tidak boleh dibaca oleh administrator.Contoh confidential information adalah data-data yang sifatnya pribadi (seperti nama, tempat tanggal lahir, social security number, agama, status perkawinan, penyakit yang pernah diderita, nomor kartu kredit, dan sebagainya) merupakan data-data yang ingin diproteksi penggunaan dan penyebarannya.Contoh lain dari confidentiality adalah daftar pelanggan dari sebuah Internet Service Provider (ISP).

2. Integrity

Aspek ini menekankan bahwa informasi tidak boleh diubah tanpa seijin pemilik informasi.Adanya virus,Trojan horse, atau pemakai lain yang mengubah informasi tanpa ijin merupakan contoh masalah yang harus dihadapi. Sebuah e-mail dapat saja “ditangkap” (intercept) di tengah jalan, diubah isinya (altered, tampered, modified), kemudian diteruskan ke alamat yang dituju.Dengan kata lain, integritas dari informasi sudah tidak terjaga. Penggunaan enkripsi dan digital signature, misalnya, dapat mengatasi masalah ini.Salah satu contoh kasus trojan horse adalah distribusi paket program TCP Wrapper

3. Authentication

Aspek ini berhubungan dengan metoda untuk menyatakan bahwa informasi betul-betul asli, orang yang mengakses atau memberikan informasi adalah betul-betul orang yang dimaksud, atau server yang kita hubungi adalah betul-betul server yang asli. Ada tiga hal yang dapat ditanyakan kepada orang untuk menguji siapa dia:

a. What you have (misalnya kartu ATM)
b. What you know (misalnya PIN atau password)
c. What you are (misalnya sidik jari, biometric)

4. Availability

Aspek availability atau ketersediaan berhubungan dengan ketersediaan informasi ketika dibutuhkan. Sistem informasi yang diserang atau dijebol dapat menghambat atau meniadakan akses ke informasi. Contoh hambatan adalah serangan yang sering disebut dengan “denial of service attack” (DoS attack), dimana server dikirimi permintaan (biasanya palsu) yang bertubi- tubi atau permintaan yang diluar perkiraan sehingga tidak dapat melayani permintaan lain atau bahkan sampai down, hang, crash.

5. Access Control

e-ISSN 2775-4049

Aspek ini berhubungan dengan cara pengaturan akses kepada informasi. Hal ini biasanya berhubungan dengan klasifikasi data (public, private, confidential,top secret)& user (guest,admin,top manager, dsb.), mekanisme authentication dan juga privacy. Access control seringkali dilakukan dengan menggunakan kombinasi userid/password atau dengan menggunakan mekanisme lain (seperti kartu, biometrics).

HASIL PENELITIAN DAN DISKUSI

Kriptografi berasal dari bahasa Yunani, terdiri dari dua suku kata yaitu kripto dan graphia. Kripto artinya menyembunyikan sedangkan graphia artinya tulisan. Kriptografi adalah ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi, seperti kerahasiaan data, keabsahan data, integritas data, serta autentikasi data. Tetapi tidak semua aspek keamanan informasi dapat diselesaikan dengan kriptografi. (Ariyus. 2008)

Kriptografi dapat pula diartikan sebagai ilmu atau seni untuk menjaga keamanan pesan. Jika suatu pesan dikirim dari suatu tempat ke tempat lain, isi pesan tersebut mungkin dapat disadap oleh pihak lain yang tidak berhak untuk mengetahui isi pesan tersebut. Untuk menjaga pesan maka pesan tersebut dapat diubah menjadi suatu kode yang tidak dapat dimengerti pihak lain. Enkripsi adalah sebuah proses penyandian yang melakukan perubahan sebuah kode atau pesan dari yang bisa dimengerti, disebut plainteks, menjadi sebuah kode yang tidak bisa dimengerti, disebut dengan cipherteks.

Sedangkan proses kebalikannya untuk mengubah cipherteks menjadi plainteks disebut deskripsi. Proses enkripsi dan deskripsi memerlukan suatu mekanisme dan kunci tertentu, dan kesatuan sistem ini sering disebut dengan cipher, Berdasarkan sifat kuncinya, kriptografi dibagi menjadi dua, yaitu kriptografi simetris dan kriptografi asimetris. Pada kriptografi simetris, proses enkripsi dan dekripsi dilakukan kunci rahasia yang sama. Sedangkan pada kriptografi asimetris, proses enkripsi dan dekripsinya menggunakan kunci yang berbeda, yaitu kunci publik untuk enkripsi, dan kunci rahasia yang digunakan untuk dekripsi. (Kristanto. 2004)

Berdasarkan waktu kemunculannya, kriptografi dibedakan menjadi dua, yaitu kriptografi klasik dan kriptografi modern. Pada kriptografi klasik, proses enkripsi menggunakan perhitungan yang sederhana dan dapat dilakukan secara manual. Sedangkan pada kriptografi modern, Proses enkripsi menggunakan perhitungan yang rumit dan melibatkan bilangan yang besar, sehingga diperlukan bantuan computer. (Riyanto dan Lestari. 2010)

Pengguna diberikan ID dan password untuk mengakses sistem yang ada. Password dienkripsi untuk mencegah terjadinya akses ilegal terhadap sistem misalnya pencurian data-data penting oleh mereka yang tidak berhak. Demikian juga enkripsi pada file-file penting dapat dilakukan, misalnya file yang berisi data keuangan. Metode enkripsi yang digunakan dapat berbentuk enkripsi kunci simetris, misalnya menggunakan algoritma DES akronim dari Data Enciyption Standart, mulanya dirancang untuk implementasi hardware. Saat digunakan untuk komunikasi, baik pengirim maupun penerima harus mengetahui kunci rahasia yang sama, yang dapat digunakan untuk mengenkripsi dan mendekripsi pesan, atau untuk menggenerate dan memverifikasi message authentication code (MAC).

Jika dibutuhkan mekanisme enkripsi password lain yang lebih aman sesuai dengan kebutuhan keamanan data yang lebih tinggi dapat digunakan mekanisme One Time Password untuk menggantikan mekanisme password statis. Keunggulan dari mekanisme One Time Password hanya digunakan satu kali saja setiap pengguna akan log in kedalam sistem ini adalah walaupun penyerang berhasil mindapatkan password namun ia tidak dapat menggunakannya lagi untuk melakukan akses terhadap sistem.

e-ISSN 2775-4049

Teknik enkripsi yang dapat digunakan untuk mekanisme ini adalah teknik-teknik enkripsi simetris / kunci rahasia. Banyak algoritma yang dapat digunakan untuk mengenkripsi password, misalnya DES akronim dari Data Enciyption Standart. Yang dibutuhkan disini adalah sumber daya manusia yang mampu untuk mengimplementasikan algoritma ini. Aplikasi kriptografi lain yang dapat diimplementasikan adalah enkripsi email.

Enkripsi email dibutuhkan untuk melindungi surat-surat penting yang akan dikirim. Misalnya saja pengiriman data-data laporan kepada pihak tertentu maupun pengiriman surat-surat berharga lainnya. Untuk mengimplementasikan enkripsi email ini harus sudah terkoneksi internet. Aplikasi enkripsi email yang dapat diadopsi misalnya Pretty Good Privacy (PGP) yang dapat diperoleh secara gratis. Selain mengenkripsi email, PGP juga dapat digunakan untuk tanda tangan digital jika dibutuhkan level keamanan yang lebih tinggi.

Teori yang berkaitan adalah Teori Preventif yang dikemukakan oleh E.H. Sutherland, yang ditekankan adalah menghilangkan kesempatan untuk melakukan kejahatan. Mencegah kejahatan lebih baik daripada mendidik penjahat menjadi lebih baik kembali, sebagaimana semboyan dalam kriminologi yaitu usaha-usaha memperbaiki penjahat perlu diperhatikan dan diarahkan agar tidak terjadi lagi kejahatan yang di ulang. Pihak Kepolisian dalam upaya ini melakukan penyuluhan hukum terkait dengan kejahatan dan memberikan pelajaran tentang pengaturan hukum terkait dengan kejahatan. Sehingga bisa meminimalisasi pelaku melakukan kejahatan khususnya di internet.

KESIMPULAN

Kriptografi merupakan salah satu media komunikasi dan informasi kuno yang masih dimanfaatkan hingga saat ini. Kriptografi di Indonesia disebut persandian yaitu secara singkat dapat berarti seni melindungi data dan informasi dari pihak yang tidak dikehendaki baik saat ditransmisikan maupun saat disimpan. Sedangkan ilmu persandiannya disebut kriptografi yaitu ilmu yang mempelajari tentang bagaimana tehnik melindungi data dan informasi tersebut beserta seluruh ikutannya. Pengguna diberikan ID dan password untuk mengakses sistem yang ada. Password dienkripsi untuk mencegah terjadinya akses illegal terhadap sistem misalnya pencurian data-data penting oleh mereka yang tidak berhak. Demikian juga enkripsi pada file-file penting dapat dilakukan misalnya file yang berisi data keuangan dan data informasi pribadi. Oleh karena itu, dapat disimpulkan bahwa kriptografi masih merupakan sistem yang efektif dalam hal keamanan dan proteksi serta dapat digunakan secara luas di berbagai bidang usaha dan teknologi. Keamanan sistem informasi tidak dilihat hanya dari kaca mata timbulnya serangan dari virus, mallware, spy ware dan masalah lain, akan tetapi dilihat dari berbagai segi sesuai dengan domain keamanan sistem itu sendiri.

DAFTAR PUSTAKA

Aryza, S., Irwanto, M., Lubis, Z., & Siahaan, A. P. U. (n.d.). *A Novelty Stability Of Electrical System Single Machine Based Runge Kutta Orde 4 Method*.

Purwanto, D. (2012). *Survey Kondisi Fisik Dan Keterampilan Teknik Dasar Bola Voli Pada Klub Bola Voli Putri Bravo Banjarnegara Tahun 2012* (Doctoral dissertation, Universitas Negeri Semarang).

Iqbal, M., Siahaan, A. P. U., Purba, N. E., & Purwanto, D. (2017). Prim's Algorithm for Optimizing Fiber Optic Trajectory Planning. *Int. J. Sci. Res. Sci. Technol*, *3*(6), 504-509.

Siahaan, A. P. U., Aryza, S., Hariyanto, E., Rusiadi, Lubis, A. H., Ikhwan, A., & Kan, P. L. E. (2018). Combination of Levenshtein Distance and Rabin-Karp to Improve the

Accuracy of Document Equivalence Level. *International Journal of Engineering & Technology*, *7*(2.27), 17–21. https://doi.org/10.14419/ijet.v7i2.27.12084

Solly Aryza, Hermansyah, Muhammad Irwanto, Zulkarnain Lubis, A. I. (2017). a Novelty of Quality Fertilizer Dryer Based on Solar Cell and Ann. *Scopus*, 1–5.

Sugiarto, A., Sihombing, M., Rini, E. S., & Utara, U. S. (2018). *ENHANCEMENT TECHNOLOGY IN ROLES AND INFLUENCE OF HEADMAN FOR IMPROVEMENT URBAN AFFAIRS IN BINJAI* ,. *9*(11), 1772–1780.

Wibowo, P., Lubis, S. A., Hermansyah, ., Hamdani, ., & Tharo, Z. (2017). Smart Home Security System Design Sensor Based on Pir and Microcontroller. *International Journal of Global Sustainability*, *1*(1), 67. https://doi.org/10.5296/ijgs.v1i1.12053