Indonesian Journal of Technology, Informatics and Science (IJTIS) DOI: 10.24176/ijtis.v3i2.8255
Vol. 3, No. 2, Juni 2022, hlm. 57-60 p-ISSN: 2715-940X
e-ISSN: 2721-4303

PERANCANGAN MODEL IMPLEMENTASI KRIPTOGRAFI DALAM SEBUAH SISTEM INFORMASI BERBASIS WEB

Alif Catur Murti[1], Wiwit Agus Triyanto[2]

[1]Program Studi Teknik Informatika, Fakultas Teknik, Universitas Muria Kudus
[2] Program Studi Sistem Informasi,Fakultas Teknik, Universitas Muria Kudus
Email: [1]alif.catur@umk.ac.id, [2]at.wiwit@umk.ac.id

(Naskah masuk: 29 Juni 2022, diterima untuk diterbitkan: 30 Juni 2022)

Abstrak

Dalam era digital sekarang ini, banyak sekali sistem dikembangkan semata-mata untuk mempermudah manusia dalam mengelola kebutuhan data dan informasi. Data dan informasi disimpan dalam sebuah database yang tersimpan dalam sebuah server local ataupun cloud server. Dalam prakteknya banyak sekali sistem dibangun dan dikembangkan dengan tampilan yang *user friendly* tetapi melupakan sisi keamanannya. Perlu adanya sebuah teknik pendekatan tambahan yang membuat informasi dan data kita menjadi lebih aman. Kriptografi merupakan teknik atau seni dalam penyandian pesan yang mampu membuat sebuah informasi menjadi ciphertext melalui proses enkripsi sehingga sudah ketika diakses oleh orang yang tidak berhak maka tidak akan memiliki arti. Ciphertext akan kembali menjadi sebuah data apabila telah dilakukan proses dekripsi. Proses enkripsi dan dekripsi memerlukan sebuah kunci sebagai sebuah parameter penentu.

Kata kunci: *Kriptografi, Sistem Informasi, Enkripsi, Dekripsi*

DESIGN OF CRYPTOGRAPHY IMPLEMENTATION MODEL IN A WEB-BASED INFORMATION SYSTEM

Abstract

In today's digital era, many systems are developed solely to make it easier for humans to manage data and information needs. Data and information are stored in a database stored on a local server or cloud server. In practice, many systems are built and developed with a user-friendly appearance but forget about the security side. There needs to be an additional approach technique that makes our information and data more secure. Cryptography is a technique or art in encoding messages that is able to make information into ciphertext through an encryption process so that when it is accessed by unauthorized people, it will have no meaning. The ciphertext will return to a data when the decryption process has been carried out. The encryption and decryption process requires a key as a determining parameter.

Keywords: *Cryptography, Information System, Encryption, Decryption*

1. PENDAHULUAN

Dalam era digital sekarang ini, banyak sekali sistem dikembangkan semata-mata untuk mempermudah manusia dalam mengelola kebutuhan data dan informasi. Sistem informasi ini merupakan kesatuan dari beberapa bagian yang saling bekerjasama untuk mengolah data dan informasi secara digital sehingga ketersediaan akan data tersebut terjamin, mudah untuk diakses dan dapat dimanfaatkan untuk mencapai tujuan. Pengelolaan data yang berbasis digital memungkinkan segala keputusan juga bisa dibuat dengan lebih mudah sehingga dengan demikian tentunya memudahkan setiap orang pekerjaannya. Data dan informasi disimpan dalam sebuah database yang tersimpan dalam sebuah server local ataupun *cloud server*. Data-data tersimpan dalam sebuah tabel dengan struktur dan tipe data tertentu yang saling berelasi satu dengan yang lain. Setiap tabel memiliki sebuah *primary key* yang bisa digunakan untuk mencari data dan menjadi penghubung antar tabel. Kebutuhan informasi yang *realtime* menjadi tuntutan saat ini, hal ini yang menjadikan suatu alasan peningkatan penggunaan internet untuk saling bertukar informasi. Imbas dari penggunaan fasilitas internet berpengaruh juga terhadap penyimpanan sebuah data. Penyimpanan data dalam sebuah cloud server saat ini menggantikan peran penyimpanan dalam bentuk hardisk maupun flashdisk yang rentan terhadap kerusakan. Tingginya tingkat transaksi untuk mengakses penyimpanan data memunculkan kekhawatiran karena dengan penggunaan internet

juga merupakan tempat dimana semua orang dapat mengakses. Baik digunakan untuk untuk kebutuhan positif ataupun negatif. Sehingga diperlukan layanan untuk menjaga keamanan data tersebut. (Qurniawan, 2012)

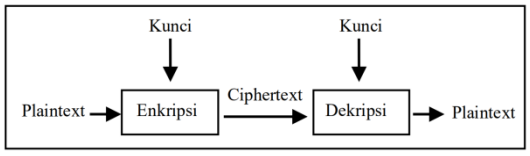
Kriptografi merupakan kegiatan pengamanan data untuk file yag berupa dokumen, gambar maupun audio. Kriptografi ini juga bisa digunakan untuk mengatasi permasalahan dalam pengamanan dalam hal meningkatnya tindak pencurian serta publikasi ini dilakukan oleh rekan sesama media lain. (Rosmasari, 2018)

Dalam prakteknya banyak sekali sistem dibangun dan dikembangkan dengan tampilan yang *user friendly* tetapi melupakan sisi keamanannya. Perlu adanya sebuah teknik pendekatan tambahan yang membuat informasi dan data kita menjadi lebih aman. Kriptografi merupakan teknik atau seni dalam penyandian pesan yang mampu membuat sebuah informasi menjadi chipertext melalui proses enkripsi sehingga sudah ketika diakses oleh orang yang tidak berhak maka tidak akan memiliki arti. Chipertext akan kembali menjadi sebuah data apabila telah dilakukan proses dekripsi. Proses enkripsi dan dekripsi memerlukan sebuah kunci sebagai sebuah parameter penentu. Data – data yang tersimpan ini biasanya masih tersimpan dalam bentuk yang masih bisa dibaca dan memiliki arti (plaintext) dan hanya pada bagian penyimpanan password saja yang dilakukan enkripsi menggunakan MD5. Dengan hanya membatasi keamanan pada bagian login ke sistem tidak menjamin sistem tersebut aman. Berdasarkan kondisi diatas perlu adanya model implementasi kriptografi untuk mengamankan data yang ada pada database.

2. LANDASAN TEORI

2.1 Kriptografi

Kriptografi adalah seni dalam penyandian pesan. (Munir, Rinaldi. 2006) Dimana didalamnya terdapat proses enkripsi dan dekripsi. Gambaran proses enkripsi dan dekripsi dapat dilihat pada gambar 1 .



Gambar 1. Enkripsi dan Dekripsi

Keterangan gambar 1:

a. plaintext adalah merupakan teks asli yang dapat dibaca dan memiliki arti.
b. enkripsi adalah proses penyandian (encode) menggunakan kunci atau parameter tertentu.
c. ciphertext adalah adalah hasil dari sebuah proses enkripsi yang berupa informasi yang tidak memiliki arti.
d. dekripsi adalah proses yang digunakan untuk mengembalikan kembali (decode) sebuah ciphertext ke sebuah palintext.

Tujuan penggunaan kriprografi disamping untuk menjaga kerahasiaan (*confidentiality*) pesan, juga dapat digunakan untuk mengetahui keabsahan pengirim (*user authentication*) dan keaslian pesan (*message authentication*). Dua hal tersebut untuk menjamin keaslian pengirim dan keaslian pesan yang dikirimkan. Berikut ini adalah contoh beberapa metode kriptografi :

a. Caesar Cipher
b. Hill Cipher
c. Vigenere Cipher
d. DES
e. AES
f. RSA

2.2. Sistem Informasi

Sistem informasi adalah gabungan komponen-komponen dalam suatu organisasi untuk mencapai tujuan memberikan informasi kepada (stakeholder) pengambil keputusan dan mengelola organisasi. (Ladjamudin, 2005)

Sistem informasi adalah merupakan suatu sistem yang dibangun dan dikembangkan untuk sebuah organisasi yang sudah disesuaikan kebutuhan akan pengolahan transaksi harian, *feature* manajerial yang bersifat strategis, semata-mata untuk dapat mennyajikan informasi kepada pihak luar atau pihak lain dengan laporan – laporan yang diperlukan. (Sutabri,T., 2012)

3. TINJAUAN PUSTAKA

Perkembangan teknologi terutama pada sistem pengamanan data dalam menjaga keamanan data informasi telah berkembang pesat. Dalam menjaga keamanan data informasi terdapat cabang ilmu dalam pengembangannya seperti kriptografi dan steganografi. Pada penerapannya dilakukan tidak hanya pada satu teknik keamanan saja, melainkan bisa dilakukan dengan kombinasi dalam keamanan data informasi. Penelitian ini bertujuan untuk membuat sebuah sistem keamanan data dengan mengimplementasikan kriptografi pada pesan teks, isi file dokumen, dan file dokumen dengan melakukan perhitungan algoritma Advanced Encryption Standard (AES). (Pabokory, 2015)

Implementasi terkait penerapan kriptografi dalam pengiriman pesan (Short Message Service) dilakukan sebagai langkah mitigasi terhadap penyadapan pada jalur komunikasi, Sehingga ketika pesan berhasil disadap maka akan tidak dapat dibaca karena yang disadap pesan dalam bentuk ciphertext. (Febriana, 2017)

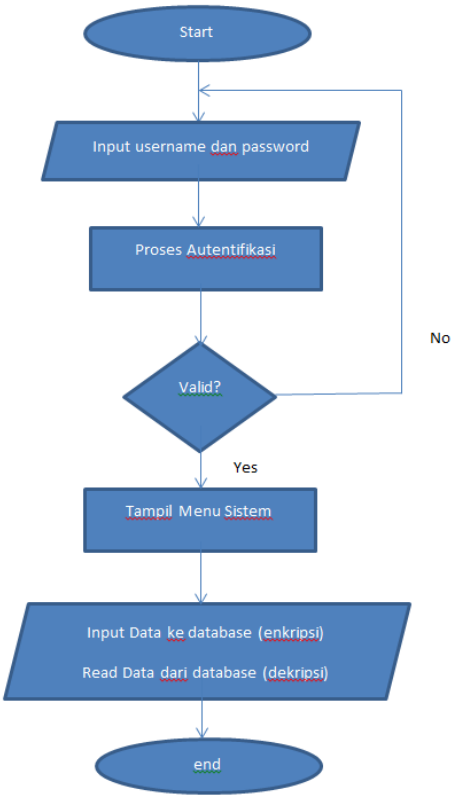
Di era modern saat ini, Anjungan Tunai Mandiri atau yang sering disingkat menjadi ATM ini bergelut dalam transaksi online yang tentu sangat rawan keamanannya. Dalam hal ini berarti terdapat banyak jalur untuk dapat menerobos sistem keamanannya, maka untuk mencegahnya diperlukan suatu tembok penghalang dan dipakailah salah satu bidang dalam ilmu komputer yaitu Kriptografi. Pembuatan Sistem keamanan pada Anjungan Tunai Mandiri ini menggunakan salah satu algoritma kriptografi DES (Data Encryption Standart), dengan menggunakan metode Personal identification number (PIN). (Efendy, F., 2019)

Sinkronisasi file adalah proses sinkronisasi atau penyesuaian antara satu file di suatu lokasi dengan file lain jika ada perubahan yang akan digunakan dan dijalankan dalam suatu sistem. Sinkronisasi file umumnya merupakan proses pertukaran data agar memiliki jumlah data yang sama. Untuk mempertahankan kerahasiaan data yang diperlukan untuk menjaga layanan demi keamanan data (Qurniawan W,2012)

4. HASIL DAN PEMBAHASAN

4.1 Perancangan

Dalam penelitian ini model implementasi kriptografi terletak pada proses input (enkripsi) dan read data (dekripsi) dari sebuah database. Gambar implementasi model kriptografi dapat dilihat pada gambar 2 berikut ini.



Gambar 2. Implementasi Model Kriptografi

Keterangan gambar 2 :

a. Proses masuk kedalam sistem informasi diawalai dengan menginputkan data username dan password.
b. Dilanjutkan proses autentikasi / validasi apakah data yang diinputkan valid atau tidak.
c. Jika tidak maka akan kembali ke proses awal, sedagkan jika hasilnya valid maka akan diarahkan ke dalam menu sistem.
d. Dalam prosesnya pasti akan terjadi transaksi input dan read data dari sebuah database.
e. Implementasi kriptografi untuk proses enkripsi digunakan pada saat input data (enkripsi) dan proses read data (dekripsi).

Data yang enkripsi adalah data yang memiliki value (nilai) yang rentan terhadap potensi pencurian data misalnya :

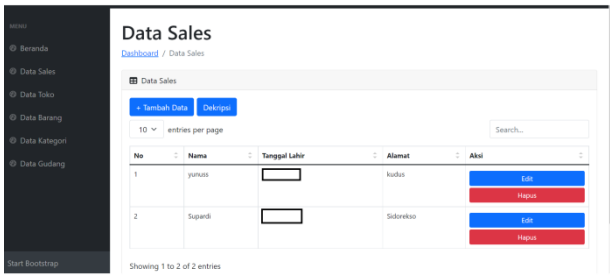
a. nomor KK;
b. NIK;
c. tanggal/bulan/tahun lahir;
d. keterangan tentang kecacatan fisik dan/atau mental;
e. NIK ibu kandung;
f. NIK ayah; dan
g. beberapa isi catatan Peristiwa Penting

(Pasal 84 ayat (1) UU Adminduk)

Ketika data tersebut diperlukan untuk ditampilkan bagi yang berwenang maka baru dilakukan proses dekripsi untuk mengembalikannya kedalam sebuah plaintext. Dengan menerapkan konsep ini maka apabila ada serangan langsung kedalam database maka masih ada proteksi keamanan bagi data yang tersimpan.

4.2 Desain

Desain tampilan terkait implementasi model kriptografi dapat dilihat pada gambar 3.



Gambar 3. Desain implementasi model kriptografi

Dalam tampilan website data sales tersebut setelah dapat masuk kedalam sistem (proses autentikasi) user dapat mengakses data sales yang berada dalam database. Pada data sales data yang bersifat rentan (tanggal lahir) ditampilkan dalam bentuk ciphertext (disimbolkan dengan kotak warna hitam). Data tersebut juga terenkripsi pada database, dan baru akan bisa ditampilan dalam halaman web ketika dilakukan proes dekripsi.Proses enkripsi dan dekripsi ini juga bisa diterapkan untuk mengamankan data yang berupa file (Contoh : Scan Dokumen KTP, SIM, Ijzah)

Algoritma kriptografi yang digunakan bisa menggunakan kriptografi modern karena akan lebih aman dibandingkan menerapkan algoritma kriptografi klasik. Perlu dipertimbangkan juga terkait dengan waktu yang diperlukan baik dalam proses enkripsi maupun dekripsi. Karena setiap metode kriptografi memiliki tahapan yang berbeda-beda dan pastinya akan berpengaruh terhadap proses transaksi input (enkripsi) dan read (dekripsi).

5. KESIMPULAN

Kesimpulan yang dapat diambil dari hasil analisis, perancangan, serta desain dan pembahasan tentang implementasi model kriptografi dalam sebuah sistem informasi berbasi web antara lain adalah sebagai berikut :

a. Sistem ini dirancang untuk meningkatkan perlindungan terhadap data yang bersifat rentan.
b. Sistem ini juga mengamankan data yang tersimpan dalam database.
c. Bisa diterapkan menggunakan beberapa model kriptografi.
d. Tingkat keamanan dan waktu proses enkripsi dan dekripsi bergantung pada model kriptografi yang digunakan.

DAFTAR PUSTAKA

Bin Ladjamudin, A.-B. (2005). Analisa dan Desain Sistem Informasi. Yogyakarta: Graha Ilmu

Efendi, F., Dewanti, N,P., 2019, Implementasi Kriptografi dalam Sistem Keamanan Anjungan Tunai Mandiri, JURNAL INFORMATIKA UPGRIS Vol. 5, No. 1,

Febriana, Ika., Aji S, G., 2017, Penerapan Teknik Kriptografi Pada Keamanan Smsandroid, JOEICT (Jurnal of Education and Information Communication Technology) Volume 1, Nomor 1, T

Munir, Rinaldi. 2006. Kriptografi. Informatika, Bandung

Pabokory, F,N., Astuti, I,F., Kridalaksana,A,H., 2015, Implementasi Kriptografi Pengamanan Data Pada Pesan Teks, Isi File Dokumen, Dan File Dokumen Menggunakan Algoritma Advanced Encryption Standard, Jurnal Informatika Mulawarman Vol. 10 No. 1

Qurniawan, W.,Wintolo,H., Nugraheny, D., 2012. Penerapan Sistem Keamanan Dengan Kriptografi Advanced Encryption Standard (AES) Dan Key Administrator Pada Sinkronisasi File. Teknik Informatika STTA Yogyakarta : Volume 1 Nomor 2.

Rosmasari., Dwi RA, R, A., Dengen, N., Taruk, M., 2018, Implementasi Metode Kriptografi International Data Encryption Algorithm (IDEA) Untuk Pengamanan Data Berita Publik Khatulistiwa Televisi Bontang, JURTI, Vol.2 No.2

Sutabri, Tata. 2012. Analisis Sistem Informasi. Yogyakarta: Andi

Undang-undang Republik Indonesia nomor Nomor 23 Tahun 2006 Tentang Administrasi Kependudukan