SNESTIK

Seminar Nasional Teknik Elektro, Sistem Informasi, dan Teknik Informatika

https://ejurnal.itats.ac.id/snestik dan https://snestik.itats.ac.id

Informasi Pelaksanaan :
SNESTIK II - Surabaya, 26 Maret 2022
Ruang Seminar Gedung A, Kampus Institut Teknologi Adhi Tama Surabaya

Informasi Artikel:
DOI : 10.31284/p.snestik.2022.2905

Prosiding ISSN 2775-5126

Fakultas Teknik Elektro dan Teknologi Informasi-Institut Teknologi Adhi Tama Surabaya
Gedung A-ITATS, Jl. Arief Rachman Hakim 100 Surabaya 60117 Telp. (031) 5945043
Email : snestik@itats.ac.id

Keamanan Jaringan Pada Sistem Pakar Diagnosa Penyakit Ibu Hamil Menggunakan Metode Forward Chaining Dan Algoritma Affine Cipher (Studi Kasus Klinik Fatimah Medika)

Fajar Yulian Siska Utama[1], Muchamad Kurniawan*[2], Siti Agustini[3]

Jurusan Teknik Informatika, Institut Teknologi Adhi Tama Surabaya [1,2,3]
e-mail: muchamad.kurniawan@itats.ac.id

ABSTRACT

Data security is the most important part of a system., particularly in supporting information security at institutions both public and private because it can guarantee the security of messages that will be given to the intended person or institution. Basically, data can be classified into public data and private data. Public data means data that can be accessed by many people, while private data can only be accessed by people who have access. Therefore, encryption is needed to keep the secrecy of data or information. Fatimah Medika Clinic is a heart clinic that servers treatment and health checks. The clinic, which is located at Terungkulon Road, Krian, Sidoarjo. In this final project, we discuss cryptography using the Affine Cipher algorithm. This algorithm is a development of Caesar algorithm using twho keys. This application could perform the encryption and decryption processes on patient data saved in the system. The retrieval of two keys in the Affine Cipher algorithm occurred automatically by taking the patien's date and month of birth into account. The results of tests on 100 data sets in which each character had the size of 3 to 12 letters yielded an average Mean Square Error (MSE) value of 9,272 abd a Peak Signal to Noise Ratio (PSNR) value of 7,379. Accordingly, by implementing the Affine Cipher algorithm into the application, we can save information from anyone without it being readable by others.

Keywords: *Expert System, Cryptography, Forward Chaining, Affine Cipher*

ABSTRAK

Keamanan data merupakan bagian paling penting dari suatu sistem. Terutama guna menunjang keamanan informasi dalam suatu instansi baik negeri maupun swasta, karena bisa memberikan

jaminan keamanan pesan yang akan diberikan kepada orang atau lembaga yang dituju. Data dapat digolongkan kedalam data public dan data private. Data public merupakan data yang dapat diakses oleh banyak orang. Sedangkan data private hanya dapat diakses oleh orang yang memiliki hak akses saja.Oleh sebab itu, enkripsi sangatlah dibutuhkan. Jika ingin data atau informasi yang dimilikinya terjamin kerahasiaannya. Klinik Fatimah Medika merupakan sebuah klinik kesehatan yang melayani pengobatan dan check kesehatan. Klinik ini berada di JL. Terungkulon, Krian , Sidoarjo. Pada penelitian tugas akhir ini membahas tentang kriptografi menggunakan Affine Cipher. Algortima Affine Cipher merupakan perkembangan dari algoritma Caesar dimana algoritma Affine Cipher menggunakan dua kunci. Aplikasi ini dapat melakukan proses enkripsi dan dekripsi pada data pasien yang di simpan ke dalam sistem. Pengambilan dua kunci untuk algoritma Affine dilakukan secara otomatis mengambil dari tanggal dan bulan lahir dari pasien. Dari hasil pengujian, untuk 100 data dengan masing masing ukuran karakter 3 sampai 12 huruf diperoleh rata-rata nilai Mean Square Error (MSE) sebesar 9272 dan nilai Peak Signal to Noise Ratio (PSNR) sebesar 7.379. Dengan menerapkan algoritma Affine Cipher ke dalam aplikasi maka diharapkan kita bisa menyimpan informasi dari siapapun tanpa terbaca.

Kata kunci: Sistem Pakar, Kriptografi, Forward Chaining , Affine Cipher

PENDAHULUAN

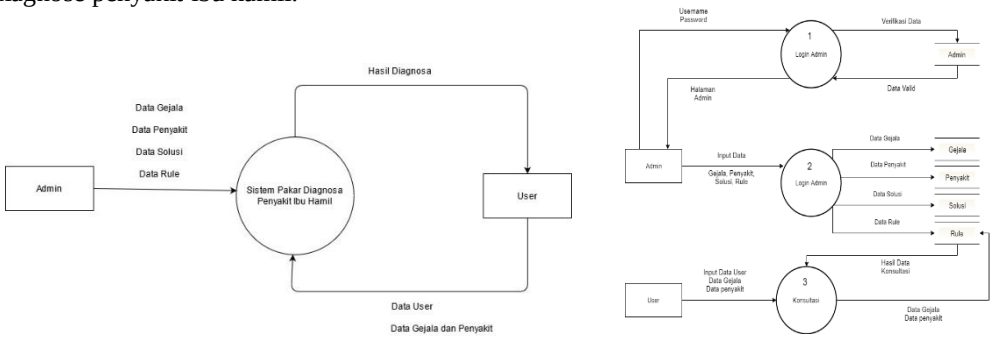
Enkripsi data atau informasi sangatlah penting untuk menunjang keamanan informasi pada suatu instansi, baik public maupun swasta, karena dapat menjamin keamanan pesan yang akan dikirimkan kepada orang atau instansi yang akan dituju[1]. Oleh karena itu, enkripsi data sangat diperlukan oleh pengguna kalau ingin data atau informasi yang dimilikinya terjaga kerahasiannya. Keamanan data merupkanan bagian penting dari suatu sistem[2]. Data dapat digolongkan kedalam data public dan data private. Data public merupakan data yang dapat diakses oleh banyak orang [3]. Sedangkan data private hanya dapat diakses oleh orang yang memiliki hak akse. Peneiltian ini bertujuan untuk keamanan jaringan pada sistem paka diagnose masalah ibu hamil memakai metode Forward Chaining dan Affine Cipher[4].

Forward Chaining merupakanan salah satu metode pencarian kedepan yang diawali dengan informasi yang ada dan menggabungkan aturan-aturan untuk menarik kesimpulan atau tujuan[5]. Affine Cipher adalah algoritma kriptogratfi klasik yang merupakan pengembangan metode Caesar Cipher dimana mengganti plaintext yang memakai sebuah nilai dan menambahkannya lewat pergeseran dengan menggunakan sebuah factor pengali beserta substitusi sehingga menghasilkan ciphertext.[6] Sandi Affine Cipher berasal dari perluasan sandi Caesar Cipher dengan menggunakan dua kunci dan aritmatik modulo. Aplikasi keamanan jaringan pada sistem pakar diagnose ibu hamil ini bertujuan untuk memberikan keamanan data pasien agar tidak disalah gunakan oleh pihak luar.[7] Sehingga adanya keamanan data seperti ini dapat membantu meningkatkan keamanan untuk data pasien [8].

METODE

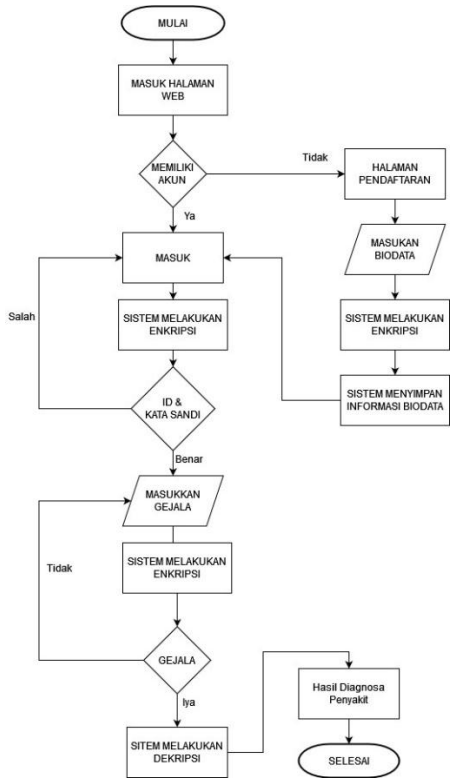
Gambar 1 a) merupakan gambar context diagram, dari diagram tersebut dapat dipahami alur yang terjadi pada system yaitu admin melakukan input data gejala,penyakit, solusi dan data rule. Sedangkan untuk user input data user dan data gejala serta penyakit ibu hamil. Gambar 1 b) dfd aplikasi atau data flow diagram dimana admin melakukan login dengan mengisi username dan password, apabila username dan password valid maka akan menampilkan halaman admin. Pada halaman admin dapat dilakukan proses input data gejala, penyakit solusi dan rule. Sedangkan user dapat melakukan konsultasi melalui sistem dengan melakukan input data user, gejala dan penyaki. Pada proses konsultasi dihasilkan diagnose penyakit pada ibu hamil.

Gambar 2 merupakan gambar flowchart seluruh sistem pada aplikasi dimulai dengan user melakukan konsultasi dan datanya akan di enkripsi. Sebelum masuk user harus masuk terlebih dahulu, jika tidak punya akun maka harus daftar untuk bisa masuk mengakses ke sistem. Data dari pasien nantinya akan di simpan dalam database dan sudah terenkripsi. Kemudian user masuk ke halaman konsultasi untuk menjawab beberapa pertanyaan gejala yang nantinya menghasilkan hasil diagnose penyakit ibu hamil.



(a) (b)

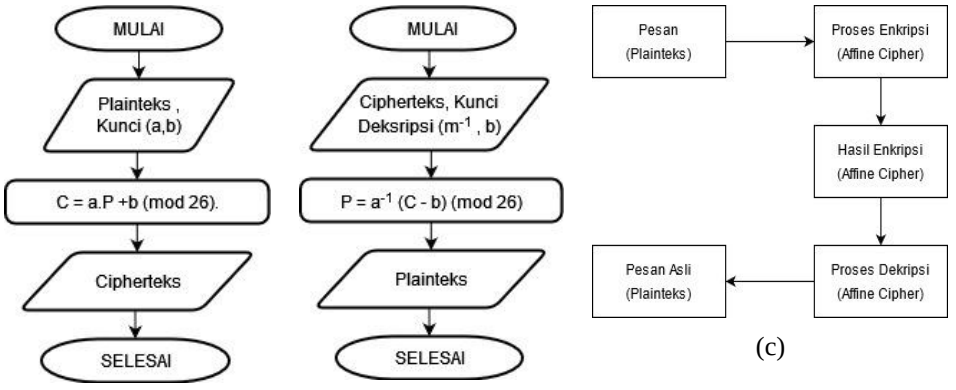
Gambar 1. a) Context Diagram, b) Data Flow Diagram.



Gambar 2 Flowchart Sistem

Gambar 3 a) merupakan gambar Flowchart Enkripsi menggunakan kunci dari tanggal lahir dan bulan lahir pasien memakai metode *Affine Cipher* , setelah sistem melakukan enkripsi

nanti akan di simpan kedalam database. Gabmar 3 b) Gambar Flowchart untuk proses Deskripsi dilakukan saat pasien melihat datanya sendiri. Gambar 3 c) proses enkripsi *Affine Cipher*.



Gambar 3 a) Flowchart Enkripsi, b) Flowchart Deskripsi, c) Proses Enkripsi *Affine Cipher*

Perhitungan Affine Cipher Enkripsi dan Deskripsi

Enkripsi contoh :
Plaintext : EVA
Dengan menggunakan kunci dari tanggal dan bulan lahir pasien.
Kunci 1 = 17 dan kunci 2 = 11

A	B	C	D	E	F	G	H	I	J
1	2	3	4	5	6	7	8	9	10
K	L	M	N	O	P	Q	R	S	T
11	12	13	14	15	16	17	18	19	20
U	V	W	X	Y	Z				
21	22	23	24	25	26				

Enkripsi : C = $((PxK_1)+K_2)$ mod 26
c1 = ((4x17)+11) = 79 (mod26) = 1 (huruf ’B’)
c2 = ((21x17)+11) = 368 (mod26) = 4 (huruf ‘E’)
c2 = ((0x17)+11) = 11 (mod26) = 11 (huruf ‘L’)
Hasil enkripsi dari plaintext = EVA dengan key1 dan key . Cipherteks yang terbentuk adalah BEL.
Data Pasien yang telah disimpan harus didekripsi terlebih dahulu agar bisa dibaca lagi oleh pasien.
Deskripsi :
Ciphertext : BEL untuk kuncinya sama kunci 1 = 17 dan kunci 2 = 11

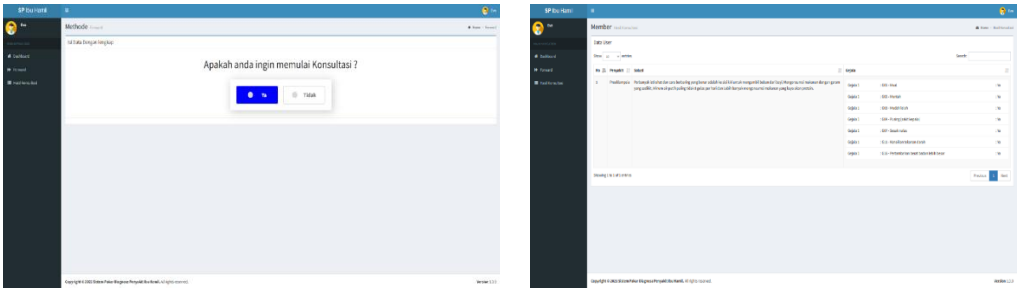
A	B	C	D	E	F	G	H	I	J
1	2	3	4	5	6	7	8	9	10
K	L	M	N	O	P	Q	R	S	T
11	12	13	14	15	16	17	18	19	20
U	V	W	X	Y	Z				
21	22	23	24	25	26				

Deskripsi : P = m^{-1} (C-b) mod 26
c1 = 23x(1-11) = -230 (mode 26) = 4 (huruf ‘E’)
c2 = 23x(4-11) = -161 (mod 26) = 21 (hutuf ‘V’)
c3 = 23x(11-11) = 0 (mod 26) = 0 (huruf ‘ A’)
Hasil deskripsi dari ciphertext = BEL dengan kunci 1 = 17 dan kunci 2 = 11. Plaintext yang terbentuk adalah EVA.

HASIL DAN PEMBAHASAN

Halaman Forward Chaining Dan Hasil Forward Chaining

Gambar 4 a) halaman ini berfungsi untuk melakukan konsultasi dan gambar b) untuk melihat hasil analisis berupa jenis penyakit yang dialami dan solusi penanganan penyakit berdasarkan gejala penyakit yang telah di jawab oleh pasien.

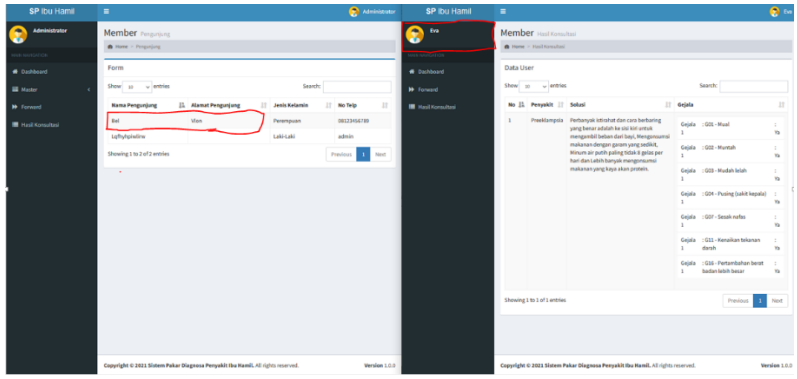


(a) (b)

Gambar 4. a) Halaman Forwad Chaining, b) Halaman Hasil Forward Chaining.

Halaman Hasil Enkripsi Dan Deskripsi Affine Cipher

Gambar 5 merupakan halaman adnim data pasien sudah terenkripsi nama EVA jadi BEL dan didata pasien sendiri sudah terdeskripsi.



Gambar 5 Hasil Enkripsi dan Deskripsi Affine Cipher

Pengujian MSE Dan PSNR

Pengujian dilakukan dengan cara mendapatkan nilai PSNR antara pesan asli dan pesan dari hasil enkripsi pada aplikasi yang menggunakan algortima Affine Cipher. Pengujian dilakukan denan 100 data dari 100 data dikategorikan 3 huruf sampai 12 huruf dapat dilihat pada Tabel 1.

Tabel 1. Data Hasil Pengujian MSE dan PSNR

No	Jumlah Data	Jumlah Karakter	Nilai Rata-Rata MSE	Nilai Rata-Rata PSNR
1	10	3	147	4.041
2	10	4	144	4.179
3	10	5	241	4.674
4	10	6	156.6	5.133
5	10	7	45707	7.205
6	10	8	72.75	7.522
7	10	9	121	8.921
8	10	10	64.27	10.049
9	10	11	70.6	9.153
10	10	12	64.3	9.571

KESIMPULAN

Sistem pakar dapat berfungsi untuk menghasilkan solusi penyakit serta bisa mengenkripsi data pasien menggunakan kunci dari tanggal dan bulan lahir secara otomatis saat disimpan kedalam databse dan melakukan deskripsi otomatis saat pasien melihat datanya sendiri. Hasil menggunakan 100 data dengan masing-masing ukuran karakter diperoleh rata-rata nilai MSE 9272 dan PSNR 7.379 presentase kualitas pesan adalah 20 unusable.

DAFTAR PUSTAKA

[1] S. Wibowo and F. E. Nilawati, "IMPLEMENTASI ENKRIPSI DEKRIPSI ALGORITMA AFFINE CIPHER BERBASIS ANDROID," vol. 13, no. 4, p. 7.

[2] E. R. Febrianto and E. A. Sarwoko, "Kriptografi Citra Digital Menggunakan Algoritma Hill Cipher Dan Affine Cipher Berbasis Android," *J. Masy. Inform.*, vol. 10, p. 11.

[3] D. Susianto and D. Mustika, "MEMBANGUN SISTEM INFORMASI INVENTORY MENGGUNAKAN ALGORITMACAESAR CIPHER SEBAGAI MEDIA ENKRIPSI (Studi Kasus: Klinik Ridho Husada)," p. 7, 2019.

[4] M. Rahmayu, "PENDETEKSIAN DIAGNOSA PENYAKIT KANDUNGAN PADA IBU HAMIL DENGAN MENGGUNAKAN METODE FORWARD CHAINING," no. 2, p. 8, 2013.

[5] S. Agustini and M. Kurniawan, "PENINGKATAN KEAMANAN TEKS MENGGUNAKAN KRIPTOGRAFI DAN STEGANOGRAFI," *SCAN - J. Teknol. Inf. Dan Komun.*, vol. 14, no. 3, pp. 33–38, Oct. 2019, doi: 10.33005/scan.v14i3.1685.

[6] A. Abdillah, N. Nurajijah, and I. Nawawi, "PERANCANGAN SISTEM PAKAR DIAGNOSA PENYAKIT KEHAMILAN BERBASIS WEB," *J. Techno Nusa Mandiri*, vol. 15, no. 2, p. 115, Sep. 2018, doi: 10.33480/techno.v15i2.910.

[7] H. Aryanti, "Pilar Nusa Mandiri Vol. IX No.1 Maret 2013," p. 7, 2013.

[8] R. Maryani and D. Haryanto, "SISTEM PAKAR DIAGNOSA PENYAKIT PADA IBU HAMIL DENGAN METODE FORWARD CHAINING," vol. 1, no. 1, p. 10, 2018.