Jurnal Komputasi

Vol 12 No. 2, 2024

KEAMANAN DATA REKAM MEDIS ELEKTRONIK MENGGUNAKAN TEKNIK KRIPTOGRAFI: *LITERATURE REVIEW*

[1,*)] Vira Febriyana, [2]Arief Ichwani

[1] Jurusan Manajemen Informatika Kesehatan, Fakultas Ilmu-Ilmu Kesehatan, Universitas Esa Unggul
[2] Jurusan Teknik Informatika, Fakultas Ilmu Komputer, Universitas Esa Unggul
[1,2] Jl. Arjuna Utara No. 9, Duri Kepa, Kec. Kebun Jeruk, Kota Jakarta Barat, DKI Jakarta, Indonesia

Abstrak — Kemajuan teknologi pada era globalisasi berkembangan dengan cepat, salah satunya adalah kemajuan Teknologi Informasi (TI). Kegiatan pada TI dilakukan dengan berbasis elektronik dan saat ini sudah banyak bidang kehidupan yang menerapkannya, salah satunya yaitu bidang kesehatan. Bukti penerapan TI di bidang kesehatan ini ditunjukkan dengan adanya Rekam Medis Elektronik (RME). Pada penyelenggaraan RME tentunya prinsip keamanan data dan informasi harus terpenuhi yang mencakup aspek *confidentiality*, *integrity* dan *availability*. Keamanan data saat ini menjadi sebuah permasalahan yang semakin serius dikarenakan meningkatnya kasus pencurian data. Usaha yang dilakukan untuk menjaga keamanan data pada RME salah satunya adalah menggunakan teknik kriptografi. Maka dari itu, penelitian ini menggunakan metode *literature review* mengenai keamanan data rekam medis elektronik menggunakan teknik kriptografi untuk mengetahui bagaimana proses dan tingkat keamanannya dalam melindungi keamanan data rekam medis elektronik berdasarkan 15 artikel jurnal yang di-*review*. Hasil dari *literature review* yang didapatkan bahwa teknik kriptografi melakukan enkripsi dan dekripsi pada data rekam medis elektronik, lalu tingkat keamanannya bergantung pada kompleksitas kunci yang digunakan. Hal tersebut menunjukkan bahwa hasil enkripsi dan dekripsi teknik kriptografi mampu melindungi keamanan data rekam medis elektronik dengan tingkat keamanannya yang tinggi.

Kata Kunci: Deskripsi; Enkripsi; Keamanan Data; Kriptografi; Rekam Medis Elektronik.

Abstract *— Technological advances in the era of globalization are developing rapidly, one of which is the advancement of Information Technology (IT). Activities in IT are carried out on an electronic basis and currently there are many fields of life that apply it, one of which is the health sector. Evidence of the application of IT in the health sector is shown by the existence of Electronic Medical Records (EMR). In organizing EMR, of course, the principles of data and information security must be fulfilled which includes aspects of confidentiality, integrity and availability. Data security is currently becoming an increasingly serious problem due to the increasing cases of data theft. One of the efforts made to maintain data security on EMR is using cryptographic techniques. Therefore, this research uses the literature review method regarding electronic medical record data security using cryptographic techniques to find out how the process and level of security in protecting electronic medical record data security based on 15 reviewed journal articles. The results of the literature review found that cryptographic techniques perform encryption and decryption on electronic medical record data, then the level of security depends on the complexity of the key used. This shows that the encryption and decryption results of cryptographic techniques are able to protect the security of electronic medical record data with a high level of security.This do*

Keywords: Cryptography; *Data Security*; *Descryption*; *Electronic Medical Record*; *Encryption*.

** Corresponding author :*
Vira Febriyana
Universitas Esa Unggul, Jakarta Barat, Indonesia
Virafebriyana9@student.esaunggul.ac.id

1. PENDAHULUAN

Saat ini kemajuan teknologi pada era globalisasi berkembang dengan pesat, salah satunya adalah kemajuan teknologi informasi (TI) [1]. Pada berbagai bidang telah menerapkan teknologi informasi (TI) termasuk bidang kesehatan [2]. Salah satu penerapan teknologi tersebut adalah rekam medis elektronik (RME) yang merupakan implementasi TI dalam melakukan pengumpulan, penyimpanan data,

pengolahan data dan akses data yang disimpan pada sebuah sistem manajemen basis data [3]. Rekam medis elektronik merupakan catatan elektronik yang berisi informasi kesehatan pasien yang dapat dibuat, dikumpulkan, dikelola serta dikonsultasikan oleh dokter dan petugas pada sebuah fasilitas pelayanan kesehatan [4]. Pada penyelenggaraan rekam medis elektronik tentunya prinsip keamanan data dan informasi harus terpenuhi yang mencakup aspek *confidentiality*, *integrity* dan *availability*. Hal yang dimaksud yaitu memastikan bahwa keamanan data dan informasi pada rekam medis elektronik, dapat terjamin dari gangguan internal maupun eksternal yang tidak memiliki kewenangan dalam mengaksesnya. Maka dari itu, hanya pihak yang memiliki kewenangan sesuai dengan kebijakan pimpinan fasilitas pelayanan kesehatan yang dapat mengakses, memperbaiki dan melihat data dalam rekam medis elektronik [5].

Keamanan data menjadi sebuah permasalahan yang semakin serius dikarenakan meningkatnya kasus pencurian data [6]. Pada Juli 2018 di Singapura, telah terjadi kasus kebocoran data pribadi yang disimpan di institusi kesehatan SingHealth dan diperkirakan sebanyak 1.500.000 data rekam medis masyarakat Singapura telah tersebar luas [7]. Di Indonesia pada tahun 2020, sebanyak 230.000 data pasien COVID-19 diperkirakan telah dicuri dan dijual sehingga menyebabkan kerugian pada materil dan psikis korban yang memungkinkan korban mendapatkan diskriminasi dalam lingkungan masyarakat [6]. Keamanan data di bidang kesehatan mengacu pada HIPAA (*Health Insurance Portability and Accountabiliy Act*) yang sudah mengatur keamanan dan kerahasiaan informasi yaitu menjamin kerahasiaan, integritas dan ketersediaan seluruh informasi kesehatan yang dilindungi dalam membuat, menerima, mempertahankan atau mentransmisikan informasi kesehatan; melindungi terhadap bahaya atau ancaman yang diantisipasi dengan wajar; melindungi dari penggunaan atau pengungkapan informasi yang diantisipasi dengan wajar berdasarkan aturan *privacy*; dan mamastikan kepatuhan tenaga kerjanya [8]. Maka dari itu, penting memiliki suatu sistem keamanan pada rekam medis elektronik dengan salah satunya adalah menggunakan teknik kriptografi.

Kriptografi adalah salah satu tonggak terpenting dalam keamanan *cyber* dan merupakan teknik atau ilmu untuk mengamankan informasi, dimana informasi tersebut hanya bisa dipahami oleh pengirim dan penerimanya [9]. Kriptografi memiliki empat prinsip yaitu *confidentiality*, *integrity*, *authentication* dan *non-repudation* [10]. Kriptografi berfungsi untuk melindungi keamanan pesan atau informasi, baik informasi yang dikirimkan maupun yang tersimpan pada media penyimpanan. Saat ini, hampir seluruh aspek kehidupan menerapkan kriptografi sebagai alat untuk menjamin keamanan dan kerahasiaan data dengan melakukan proses enkripsi dan dekripsi [11]. Oleh karena itu, penelitian ini akan membahas penerapan teknik kriptografi yang diterapkan pada sistem keamanan data rekam medis elektronik berdasarkan *literature review* penelitian-penelitian sebelumnya dengan tujuan dapat mengetahui bagaimana proses dan tingkat keamanannya.

2. METODOLOGI PENELITIAN

Rancangan penelitian menggunakan desain *literature review* yang membahas topik keamanan data rekam medis elektronik menggunakan teknik kriptografi. Sumber data penelitian adalah data sekunder yang diambil dari artikel jurnal menggunakan *database* Google Scholar, PubMed, Hindawi, ProQuest dan Science Direct. *Keyword* dan *Boolean Operator* yang digunakan adalah “rekam medis elektronik” OR “*electronic medical record*” AND “keamanan data” OR “*data security*” AND “kriptografi” OR “*cryptography*” AND “enkripsi” OR “*encryption*”.

Tabel 1. Jumlah Artikel Pada Masing-Masing *Database*

Database	Jumlah Artikel
Google Scholar	1.134
PubMed	26
Hindawi	76
ProQuest	748
Science Direct	424
Total	2.408

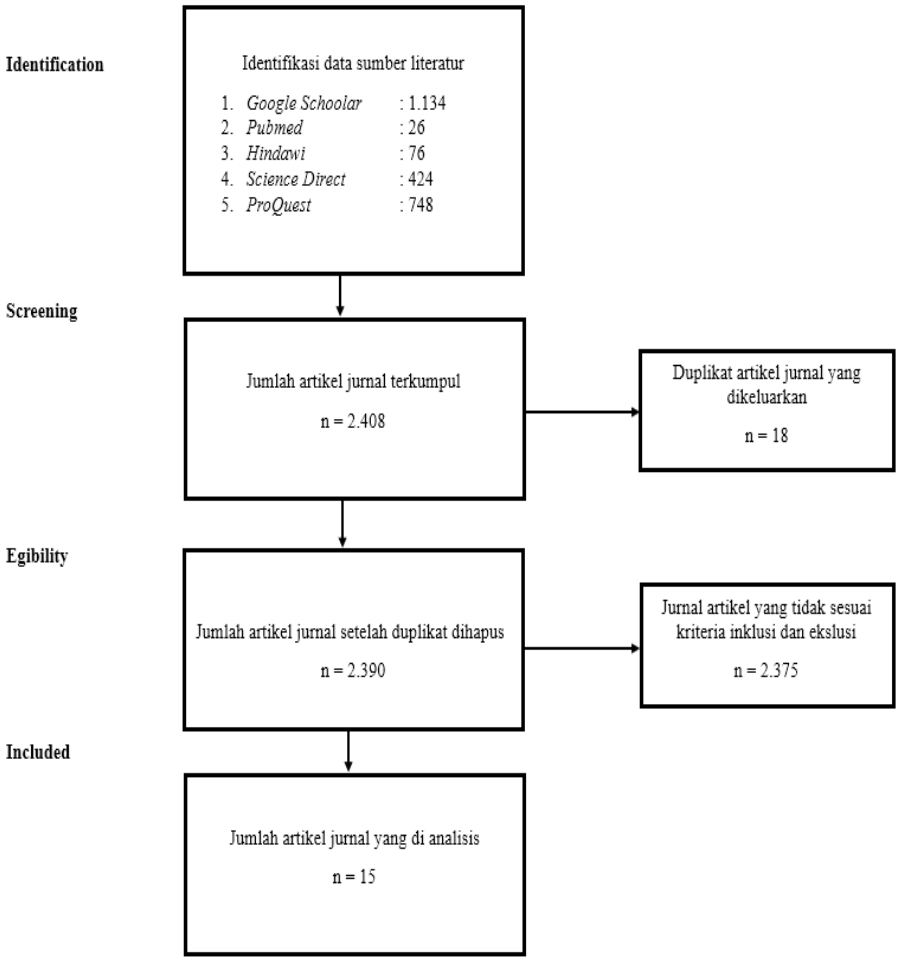
2.1. Kriteria Egibilitas

Berikut adalah kriteria egibilitas yang terdiri dari inklusi dan ekslusi yang digunakan pada penelitian ini:

1. Inklusi
   a. Artikel jurnal yang membahas keamanan data rekam medis elektronik menggunakan teknik kriptografi.
   b. Artikel jurnal yang dipublikasi tahun 2018 – 2024.
   c. Bahasa yang digunakan bahasa Indonesia dan bahasa Inggris.
   d. Jurnal terakreditasi SINTA atau sudah memiliki ISSN/DOI.
2. Eksklusi
   a. Artikel jurnal tidak full text atau hanya menampilkan abstrak.
   b. Artikel jurnal tidak dapat diakses atau berbayar.
   c. Tujuan tidak relevan.
   d. Metode yang digunakan literature review.

2.2. Data Sintesis

Data sintesis pada penelitian ini dilakukan berdasarkan tema-tema yang diidentifikasi dari hasil tinjauan. Adapun tema-tema tersebut yaitu rekam medis elektronik, keamanan data dan teknik kriptografi. Pada penyeleksian *literature* digunakan metode PRISMA (*Preferred Reporting Items for Systematic Review and Meta-Analyses*). Berikut adalah *flow* PRISMA yang dapat dilihat pada gambar 1.



Gambar 1. *Flow* PRISMA

3. HASIL DAN PEMBAHASAN

Penerapan teknik kriptografi dalam melindungi keamanan data rekam medis elektronik dilakukan dengan proses enkripsi dan dekripsi data. Data yang ingin dilindungi akan diubah menjadi data yang sulit dipahami (*cipher text*) melalui enkripsi, lalu untuk mengembalikan data yang sudah dienkripsi menjadi bentuk semula (*plain text*) dilakukan proses dekripsi. Proses enkripsi dan dekripsi ini memiliki alur yang berbeda-beda sesuai dengan algoritma kriptografi yang digunakan. Pada kriptografi kunci simetris untuk proses enkripsi dan dekripsi menggunakan satu kunci yang sama. Sedangkan kriptografi asimetris untuk proses enkripsi dan dekripsi menggunakan sepasang kunci yaitu kunci privat dan kunci publik. Pada kriptografi kunci *hybrid* menggunakan penggabungan antara kunci simetris dengan asimetris. Berikut adalah tabel daftar algoritma kriptografi yang diperoleh.Hasil penelitian berupa data atau angka disajikan dalam bentuk tabel atau grafik. Jika pada penelitian dilakukan pengembangan aplikasi/perangkat lunak, dapat disajikan beberapa *screenshot* yang penting. Setiap tabel, grafik atau gambar harus dirujuk di dalam tulisan/paragraf.

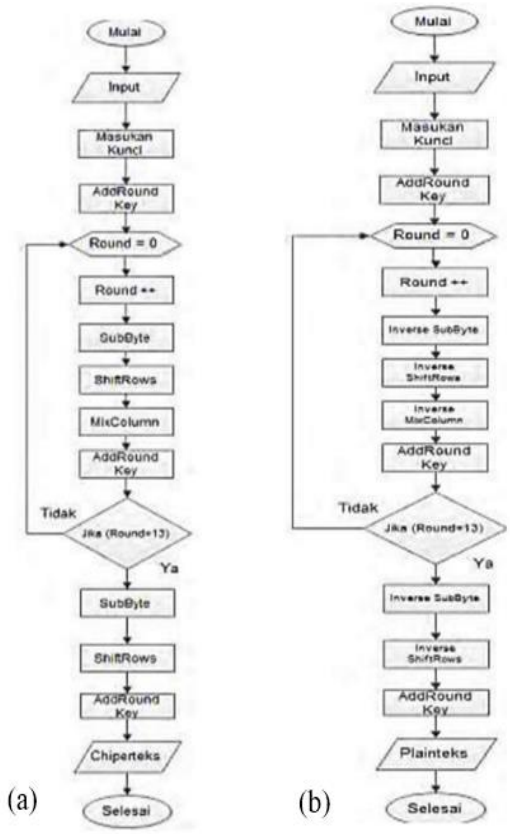
Tabel 2. Daftar Algoritma Kriptografi

Jenis Kriptografi	Kunci Kriptografi	Algoritma Kriptografi	Artikel Jurnal
Klasik	Simetris	Caesar Chiper	[12]
Modern	Simetris	Advanced Encryption Standard (AES)	[13], [14], [15]
		SPECK	[16]
		Triple Data Encryption (3DES)	[17]
		Blowfish	[18], [19]
	Asimetris	Rivest Shamir Adleman (RSA)	[20], [21]
		Identity-Based Cryptography	[22], [23]
	Hybrid	Digital Signature Algoritma (DSA) dan International Data Encryption Algorithm (IDEA)	[24]
		Identity-Based Encryption (IBE) dan Advanced Encryption Standard (AES)	[25]
		Advanced Encryption Standard (AES) dan Rivest Shamir Adleman (RSA)	[26]

3.1. Proses Teknik Kriptografi dalam Keamanan Data Rekam Medis Elektronik

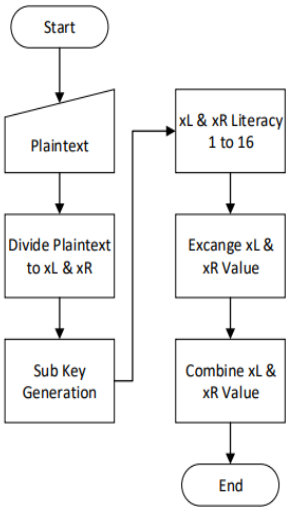
Algoritma *Caesar Cipher* merupakan kriptografi klasik dengan teknik enkripsi yang paling sederhana karena hanya melakukan substitusi pada setiap huruf dan besaran substitusinya ditentukan melalui kesepakatan. Sebelum nantinya data rekam medis elektronik dienkripsi, akan dilakukan perubahan ke dalam angka menggunakan operator aritmetika modulo 26 [12].

Kriptografi modern pada algoritma *Advanced Encryption Standard* (AES) yang menggunakan kunci simetris melakukan transformasi *byte* pada data yang akan dienkripsi melalui empat tahap, yaitu *SubBytes*, *ShiftRows*, *MixColums* dan *AddRoundKey* sehingga akan menghasilkan sebuah *chiper text*. Pada proses tranformasi *byte*, AES akan melakukan pengulangan round mulai dari *SubBytes* hingga *AddRoundKey* tergantung pada panjang kunci yang digunakan yaitu 128 bit, 192 bit atau 256 bit. Jika data rekam medis yang sudah diubah menjadi chiper text ingin dikembalikan ke bentuk semula, maka AES akan melakukan proses *Inverse SubBytes*, *Inverse ShiftRows*, *Inverse MixColumns* dan *AddRoundKey* [13], [15].



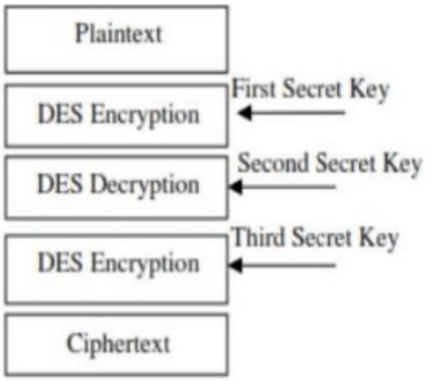
Gambar 2. Alur Enkripsi (a) dan Dekripsi (b) Algoritma AES

Pada algoritma *Blowfish* juga melakukan iterasi atau pengulangan dalam melakukan enkripsi yaitu sebanyak 16 kali putaran. Panjang kunci algoritma *Blowfish* berkisar antara 32 bit sampai 448 bit yang digunakan untuk enkripsi dan dekripsi [19]. Pada prosesnya, data yang disimpan dalam *database* akan dibagi menjadi dua yaitu xL dan xR, kemudian membangkitkan subkunci dengan melakukan iterasi sebanyak 16 kali. Hasil dari iterasi dilanjutkan dengan penukaran nilai xL dan xR dan terakhir menggabungkan kedua nilai tersebut hingga menghasilkan *cipher text*. Proses enkripsi dan dekripsi pada *Blowfish* dibutuhkan waktu selama 0,28 detik [18].



Gambar 3. Alur Enkripsi Algoritma *Blowfish*

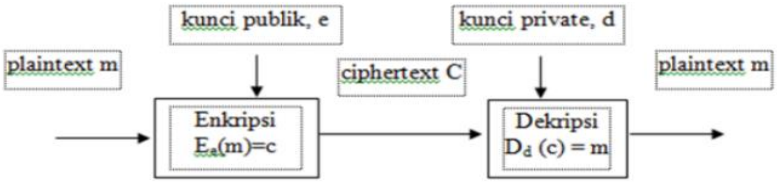
Keamanan data rekam medis elektronik yang menggunakan kriptografi algoritma *Triple Data Encryption Standard* (3DES), akan dilakukan proses enkripsi dengan merubah letak huruf pada data yang akan dienkripsi, sedangkan untuk melakukan dekripsi hanya cukup mengembalikan posisi huruf pada data berdasarkan kunci dan *shift algorithm* yang sudah disepakati oleh pengirim dan penerima. Data yang dienkripsi akan dibagi menjadi blok yang berukuran 64 bit lalu digunakan kunci 56 bit untuk melakukan enkripsi pada setiap blok tersebut. Pada 3DES, enkripsi akan dilakukan sebanyak tiga kali dengan kunci 56 bit untuk mengubah data masukan 64 bit menjadi keluaran yang sama sehingga menciptakan *cipher text* [17].



Gambar 4. Alur Enkripsi Algoritma 3DES

Pada perancangan sistem keamanan rekam medis elektronik menggunakan algoritma SPECK dilakukan dengan mengenkripsi *plain text* dengan panjang 128 bit dan kunci sebesar 128 bit. Pengujian *perfomance* pada algoritma ini dalam melakukan enkripsi dan dekripsi membutuhkan waktu sekitar 10-12 milisecond [16].

Berbeda dengan algoritma kunci simetris, pada kunci asimetris menggunakan kunci publik (d) dan kunci privat (e) untuk proses enkripsi dan dekripsi yang bisa dilihat pada gambar 5 [27].



Gambar 5. Alur Enkripsi dan Dekripsi Kunci Asimetris

Rivest Shamir Adleman (RSA) merupakan metode kriptografi modern dengan kunci asimetris terbaik. Proses utama algoritma RSA adalah membuat kunci privat dan kunci publik yang akan digunakan untuk enkripsi dan dekripsi. Penerapan RSA dilakukan ketika petugas mengisi seluruh inputan ke dalam *form* yang ada di sistem RME dan di submit, maka proses enkripsi akan dimulai. Data yang di-input akan diubah ke bentuk ASCII lalu data tersebut akan dibagi menjadi beberapa blok (mi). Setelah memenuhi syarat, maka data akan terenkripsi dengan pasangan kunci publik pada *database* rekam medis elektronik. Sedangkan untuk proses dekripsi, data hasil enkripsi akan diubah kembali ke kode ASCII untuk mengembalikan data ke bentuk semula. Proses dekripsi ini menggunakan pasangan kunci privat, namun proses dekripsi akan gagal ketika kunci privat yang digunakan salah atau berbeda dari pembuatan kunci sebelumnya [20].

Pada sistem rekam medis elektronik berbasis *cloud*, digunakan algoritma *Identity-Based Encryption* (IBE) untuk mengatasi masalah keamanan data. Hasil simulasi didapatkan bahwa dalam melakukan enkripsi memberikan waktu yang lebih singkat, efisien dan kinerja yang lebih baik [22], [23]. Pada

proses enkripsi, digunakan identitas pengguna untuk membuat kunci publik misalnya dengan memanfaatkan nomor telepon dan *ID email*. Data yang sudah terenkripsi nantinya akan disimpan di *cloud*, sedangkan untuk proses dekripsi digunakan kunci privat untuk mengembalikan data ke bentuk asli [23].

Layanan *cloud* untuk penyimpanan data di fasilitas pelayanan kesehatan juga dapat mengkombinasikan kriptografi kunci simetris dengan asimetris atau yang disebut dengan kunci *hybrid*, seperti kombinasi algoritma *Digital Signature Algoritma* (DSA) sebagai kunci asimetris dan *International Data Encryption Algorithm* (IDEA) sebagai kunci simetris. Gabungan antara kedua algoritma tersebut tidak hanya menjamin data privasi penggunanya tetapi juga menjamin bahwa data tidak dapat dirusak atau diubah oleh pengguna yang tidak berwenang [24].

Penggabungan algoritma yang digunakan pada teknik kriptografi tentunya dapat meningkatkan keamanan data tetapi juga bisa memiliki kelemahan pada prosesnya. Penggunaan algoritma kunci hybrid, yaitu *Advanced Encryption Standard* (AES) dengan *Identity-Based Encryption* (IBE) atau disebut mIBE-AES walaupun didapatkan total waktu komputasi secara keseluruhan lebih unggul namun tetap saja untuk waktu proses enkripsi dan dekripsi data rekam medis lebih lama. Cara kerja kedua algoritma ini adalah dengan membuat *key generator* menggunakan IBE sedangkan proses enkripsi dan dekripsi menggunakan AES. Uji performa waktu proses enkripsi dan dekripsi dibutuhkan waktu selama 0,799 detik. Penggabungan kedua algoritma ini mampu melindungi data rekam medis dari serangan *Man In The Middle* [25]. Selain itu, penggunaan algoritma *Advanced Encryption Standard* (AES) dengan *Rivest Shamir Adleman* (RSA) dalam proses enkripsi dan dekripsi juga lebih efisien, memerlukan memori komputasi dan daya yang lebih kecil. Proses enkripsi dan dekripsi membutuhkan waktu selama 5,5 detik [26].

3.2. Tingkat Keamanan Teknik Kriptografi dalam Keamanan Data Rekam Medis Elektronik

Pada tingkat keamanannya, penerapan kriptografi ini dapat dilihat dari seberapa kompleks kunci algoritma yang dipakai. Pada kunci simetris, semakin panjang kunci yang digunakan maka semakin tinggi pula tingkat keamanannya. Sebagaimana diketahui pada algoritma AES yang memiliki tiga panjang kunci, yaitu 128 bit, 192 bit dan 256 bit, maka jika digunakan panjang kunci 256 bit proses enkripsi dan dekripsi akan dilakukan sebanyak 14 iterasi [14], [15]. Jika diterapkan untuk melindungi data rekam medis elektronik, tentunya akan meningkatkan keamanan data tersebut dibandingkan menggunakan panjang kunci 128 bit dengan 10 putaran dan 192 bit dengan 12 putaran.

Sedangkan algoritma SPECK dalam melindungi keamanan data rekam medis elektronik, memiliki berbagai macam panjang kunci dengan panjang blok yang berbeda. SPECK dengan panjang blok 128 bit memiliki tiga macam panjang kunci yaitu 128 bit, 192 bit dan 256 bit. Pada jurnal yang dianalisis, dipakai kunci sepanjang 128 bit dengan proses enkripsi dan dekripsi sebanyak 32 iterasi [16].

Berbeda dengan kunci simetris, penggunaan kunci asimetris ini berfokus pada rumitnya pembuatan kunci privat dan kunci publik. Seperti pada algoritma RSA, tahap pertama yang dilakukan adalah menentukan nilai p dan q yang berupa bilangan prima. Kedua nilai ini akan digunakan dalam pembuatan kunci privat dan kunci publik. Semakin besar bilangan prima yang digunakan, maka akan semakin tinggi tingkat keamanannya [20], [21]. Sedangkan untuk kunci *hybrid* yang merupakan gabungan dari kunci simetris dan asimetris, proses enkripsi dan dekripsinya akan semakin rumit sehingga hal ini tentu akan sangat meningkatkan tingkat keamanan dalam melindungi data rekam medis elektronik.

Sedangkan dalam menguji keamanan kriptografi dilakukan pengujian sistem keamanan apakah sudah berjalan sesuai dengan kebutuhan dan pengujian lainnya jika diperlukan seperti *test vector* untuk mengetahui hasil enkripsi apakah sudah sesuai dengan pencipta algoritma, uji *sniffing* dan uji *chosen-plaintext* untuk mengetahui bahwa sistem keamanan terlindungi dari serangan *Man In The Middle* (MITM) dan analisis serangan diferensial.

4. KESIMPULAN

Penerapan teknik kriptografi dilakukan dengan proses enkripsi yaitu merubah data asli menjadi data yang sulit dipahami (*cipher text*) dan proses dekripsi untuk merubah data kembali ke bentuk asli (*plain text*) apabila diperlukan, sehingga akan menjamin keamanan data pada rekam medis elektronik. Tingkat keamanan teknik kriptografi dapat dilihat melalui seberapa kompleks kunci yang digunakan untuk enkripsi dan dekripsi. Semakin kompleks kunci yang digunakan, maka tingkat keamanan kriptografi akan semakin tinggi.

DAFTAR PUSTAKA

[1] B. Setiaji and P. A. K. Pramudho, "Pemanfaatan Teknologi Informasi Berbasis Data dan Jurnal," *Jurnal Inovasi Riset Ilmu Kesehatan*, vol. 1, no. 3, 2022, *Accessed*: Oct. 28, 2023. [*Online*]. *Available*: https://jurnalp4i.com/index.php/healthy/article/view/1649/1579.

[2] R. Andriani, D. Septiana Wulandari, and R. Siwi Margianti, "Rekam Medis Elektronik sebagai Pendukung Manajemen Pelayanan Pasien di RS Universitas Gadjah Mada," *Jurnal Ilmiah Perekam dan Informasi Kesehatan Imelda*, vol. 7, no. 1, pp. 96–107, 2022, *Accessed*: Nov. 19, 2023. [Online]. Available: https://jurnal.uimedan.ac.id/index.php/JIPIKI/article/view/599/597.

[3] M. K. Maha Wirajaya and N. Made Umi Kartika Dewi, "Analisis Kesiapan Rumah Sakit Dharma Kerti Tabanan Menerapkan Rekam Medis Elektronik," *Jurnal Kesehatan Vokasional*, vol. 5, no. 1, pp. 1–9, Feb. 2020, doi: 10.22146/jkesvo.53017.

[4] Z. Lokmic-Tomkins et al., "*Integrating interprofessional electronic medical record teaching in preregistration healthcare degrees: A case study*," Int J Med Inform, vol. 169, pp. 1–8, Jan. 2023, doi: 10.1016/j.ijmedinf.2022.104910.

[5] R. Pradita and R. Kusumo, "Pentingnya Aspek Keamanan Informasi Data Pasien Pada Penerapan RME di Puskesmas," *Journal of Sustainable Community Service*, vol. 2, no. 2, pp. 52-62. 2022, [*Online*]. *Available*: https://transpublika.co.id/ojs/index.php/JSCS/article/view/437.

[6] S. Sofia, E. T. Ardianto, N. Muna, Sabran, "Analisis Aspek Keamanan Informasi Data Pasien Pada Penerapan RME di Fasilitas Kesehatan," *Jurnal Rekam Medik dan Manajemen Informasi Kesehatan*, 2022, [*Online*]. *Available*: https://rammik.pubmedia.id/index.php/rmik/article/view/29.

[7] P. Mahardika Herlambang, S. Anjani, H. Wijayanto, and Murni, "Model Perilaku Keamanan Siber Pada Pengguna Sistem Informasi Kesehatan Pada Masa Pandemi COVID-19," *J-TIT: Jurnal Teknologi Informasi dan Terapan*, vol. 3, no. 2, pp. 28–33, 2020, *Accessed*: Oct. 28, 2023. [*Online*]. *Available*: https://jtit.polije.ac.id/index.php/jtit/article/view/272.

[8] R. Setiawan, "Konsep Enkripsi & Dekripsi untuk Keamanan Data," *Dicoding Blog*. *Accessed*: Feb. 10, 2024. [*Online*]. *Available*: https://www.dicoding.com/blog/enkripsi-untuk-keamanan-data/.

[9] M. Kumar, "Post-Quantum Cryptography Algorithm's Standardization and Performance Analysis," Array, vol. 15, pp. 2–27, Sep. 2022, doi: 10.1016/j.array.2022.100242.

[10] B. E. Widodo and A. S. Purnomo, "Implementasi Advanced Encryption Standard Pada Enkripsi dan Dekripsi Dokumen Rahasia Ditintelkam Polda DIY," *Jurnal Teknik Informatika (JUTIF)*, vol. 1, no. 2, pp. 69–77, Dec. 2020, doi: 10.20884/1.jutif.2020.1.2.21.

[11] L. Silalahi, A. Sindar, and S. Pelita Nusantara, "Penerapan Kriptografi Keamanan Data Administrasi Kependudukan Desa Pagar Jati Menggunakan SHA-1," *Jurnal Nasional Komputasi dan Teknologi Informasi*, vol. 3, no. 2, 2020.

[12] A. Sellyana and N. B. Nugraha, "Penerapan Caesar Chiper dan Least Significant Bit Untuk Mengamankan Data Rekam Medis*," Jurnal Publikasi Ilmu Komputer dan Multimedia*, 2023, [*Online*]. *Available*: https://ejurnal.stie-trianandra.ac.id/index.php/jupikom/article/view/1001.

[13] A. Sarce Joel, F. Abdussalaam, and Y. Yunengsih, "Tata Kelola Rekam Medis Berbasis Teknologi Informasi dalam Penanganan Kerahasiaan dan Keamanan Data Pasien dengan Metode Kriptografi," *Jurnal Indonesia : Manajemen Informatika dan Komunikasi*, vol. 4, no. 3, pp. 837–848, Sep. 2023, doi: 10.35870/jimik.v4i3.287.

[14] P. H. Yosi Tanjung, "Penerapan Algoritma AES 256 Dalam Pengamanan Data Rekam Medis," *Journal Global Tecnology Computer*, vol. 1, no. 3, pp. 77–83, 2022, *Accessed*: Dec. 21, 2023. [*Online*]. *Available*: http://ejurnal.seminar-id.com/index.php/jogtc/article/view/2054.

[15] S. Wulandari et al., "Addition of Cryptographic Algorithm for Bitmap Image Security of Medical Record Information System Electronics (RME)," *Jurnal Ilmu Fisioterapi dan Ilmu Kesehatan Ssithana*, 2020, [*Online*]. *Available*: https://jurnal.stikeskesdam4dip.ac.id/index.php/JUFDIKES/article/view/380.

[16] H. A. Kartika, A. Kusyanti, and M. Data, "Implementasi Algoritme SPECK dan SHA-3 Pada Database Rekam Medik," *Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer*, 2018, [*Online*]. *Available*: http://j-ptiik.ub.ac.id/index.php/j-ptiik/article/view/3804.

[17] M. Yunus et al., "File Security Design in Electronic Health Record (EHR) System with Triple DES Algorithm (3DES) at Jember Family Health Home Clinic," *International Journal of Health and Information System*, 2023, [*Online*]. *Available*: https://ijhis.pubmedia.id/index.php/ijhis/article/view/2.

[18] P. Irfan et al., "Application of The Blowfish Algorithm in Securing Patient Data in the Database," Matrix: *Jurnal Manajemen Teknologi dan Informatika*, 2022, [*Online*]. *Available*: https://ojs2.pnb.ac.id/index.php/MATRIX/article/view/495.

[19] N. O. Akande, C. O. Abikoye, M. O. Adebiyi, A. A. Kayode, A. A. Adegun, and R. O. Ogundokun, "Electronic Medical Information Encryption Using Modified Blowfish Algorithm," ICCSA, pp. 166–179, 2019, doi: 10.1007/978-3-030-24308-1_14.

[20] S. Sutejo, "Implementasi Algoritma Kriptografi Rsa (Rivest Shamir Adleman) Untuk Keamanan Data Rekam Medis Pasien," INTECOMS: *Journal of Information Technology and Computer Science*, 2021, [*Online*]. *Available*: https://journal.ipm2kpe.or.id/index.php/INTECOM/article/view/2437.

[21] V. C. Osamor and I. B. Edosomwan, "Employing Scrambled Alpha-Numberic Randomization and RSA Algorithm To Ensure Enhanced Encryption In Electronic Medical Record," *Inform Med Unlocked*, pp. 1–7, Jan. 2021, doi: 10.1016/j.imu.2021.100672.

[22] S. Mittal, P. Singh, and R. Malhotra, "An Efficient Approach for Secured E-Health Cloud System Using Identity Based Cryptography Techniques in Cloud Computing Environment," *Journal of Mechanics of Continua and Mathematical Sciences*, vol. 14, no. 3, pp. 124–134, Jun. 2019, doi: 10.26782/jmcms.2019.06.00010.

[23] S. Mittal et al., "Using Identity-Based Cryptography as a Foundation for an Effective and Secure Cloud Model for E-Health," *Comput Intell Neurosci*, pp. 1–8, 2022, doi: 10.1155/2022/7016554.

[24] P. Semwal, S. Sharma, and N. Uniyal, "A Three Level Cryptographic Security Module to Ensure Security of Health Care Data Stored In The Cloud," *Neuroquantology*, vol. 20, no. 14, pp. 1420–1425, 2022, doi: 10.4704/nq.2022.20.14.

[25] D. N. Purnamasari, A. Sudarsono, and P. Kristalina, "Modifikasi Identity-Based Encryption Pada Keamanan Dan Kerahasiaan Data Rekam Medis," *Jurnal Inovtek Polbeng*, vol. 9, no. 2, pp. 196–203, 2019, Accessed: Dec. 21, 2023. [*Online*]. *Available*: https://core.ac.uk/download/pdf/270221347.pdf.

[26] S. A. Ajagbe, H. Florez, and J. B. Awotunde, "AESRSA: A New Cryptography Key for Electronic Health Record Security," *Communications in Computer and Information Science*, pp. 237–251, 2022, doi: 10.1007/978-3-031-19647-8_17.

[27] Jamaludin et al., Kriptografi Teknik Keamanan Data, vol. 1. Yayasan Kita Menulis, 2022. *Accessed*: Feb. 14, 2024. [*Online*]. *Available*: https://www.researchgate.net/publication/373655214_Kriptografi_Teknik_Keamanan_Data.