BAB 1
PENDAHULUAN

1.1 Latar Belakang

Data dan informasi sangat penting dalam segala aspek kehidupan pada masa ini. Selaras dengan kemajuan teknologi yang semakin berkembang, memungkinkan data dan informasi dapat diakses dan dimanipulasi oleh siapa saja, tak terkecuali data dan informasi pribadi. Tentu kebocoran informasi pribadi itu bisa sangat meresahkan bila terkait hal yang begitu penting seperti data dan informasi rekam medis. Dijelaskan dalam Peraturan Menteri Kesehatan Nomor 269 tahun 2008 Tentang Rekam Medis. Bab 1 Ketentuan Umum Pasal 1 Ayat (1), rekam medis adalah berkas yang berisikan catatan dan dokumen tentang identitas pasien, pemeriksaan, pengobatan, tindakan dan pelayanan lain yang diberikan kepada pasien (Kementrian Kesehatan RI, 2008). Pentingnya menjaga keaslian dan keamanan citra merupakan integritas pada rekam medis, yaitu untuk mengacu kepercayaan, konsistensi dan keyakinan terhadap rekan medis (Susanto and Sugiharto, 2017). Institusi kesehatan di seluruh dunia perlu bertukar dan berbagi informasi medis, namun informasi yang dipertukarkan harus diamankan agar tidak adanya modifikasi yang dapat terjadi pada informasi yang dikirimkan lewat internet (Al-Haj, *et. al.*, 2016).

Rekam medis dilihat dari jenisnya, dapat dibedakan menjadi dua, yaitu rekam medis konvensional dan rekam medis elektronik (Depkes, 2006, p. 3). Rekam medis elektronik salah satunya adalah hasil rekam medis PET (*Positron Emission Tomography*). Hasil rekam medis PET digunakan sebagai salah satu cara untuk mendiagnosis penyakit pasien, terutama penyakit ganas seperti kanker dan penyakit dalam. Dengan munculnya *telemedicine*, ada peningkatan kebutuhan bagi dokter untuk saling berbagi citra medis, untuk mencari diagnosa berkualitas tinggi atau untuk bertukar pendapat. Akibatnya, keamanan citra medis telah menjadi masalah penting ketika citra ditransmisi lewat jaringan terbuka seperti internet, di mana informasi sensitif pasien dapat diakses oleh peretas yang bermaksud jahat, kemungkinan pelanggaran keamanakan termasuk merusak citra untuk dimodifikasi

atau dimasukan data palsu yang dapat menyebabkan kesalahan diagnosis dan pengobatan (Tan *et al.*, 2011). Salah satu kasus pencurian data yang pernah terjadi di Indonesia, adalah pencurian dan penipuan data pasien di rumah sakit Samarinda Medika Citra pada tahun 2019, dilansir dari laman berita https://kaltimkece.id/, orang tua pasien dari seorang bayi bernama Keizha yang mengidap gangguan pernafasan, menerima telepon tidak dikenal yang mengatas namakan pihak rumah sakit Samarinda Medika Citra, pada sambungan telepon tersebut, korban diminta mentransfer uang sebagai biaya peminjaman alat operasi sebesar 8,8 juta, korban mempercayai telepon pelaku karena pelaku mengetahui kondisi dan penyakit pasien serta data rekam medis dan informasi pasien dengan akurat, padahal informasi tersebut haruslah informasi yang tidak diketahui pihak luar selain keluarga pasien dan rumah sakit. Selain di Indonesia, berdasarkan berita dari http://dunia.tempo.co, pada tahun 2018 kasus pencurian data rekam medis juga pernah terjadi di Singapura, yaitu pencurian 1.5 juta data medis masyarakat Singapura termasuk di dalamnya data medis Perdana Menteri Lee Hsien Loong, dibobol peretas. Berdasarkan kasus yang pernah terjadi, pengamanan rekam medis perlu dilakukan dengan ketat untuk menghindari setiap kerugian yang dapat terjadi.

Hasil pemeriksaan rekam medis tentu sangat penting bagi seorang pasien, sehingga perlu dijaga kerahasiaan dan keasliannya. Institusi kesehatan di seluruh dunia perlu bertukar dan berbagi informasi medis, namun informasi yang dipertukarkan harus diamankan agar tidak adanya modifikasi yang dapat terjadi pada informasi yang dikirimkan lewat internet (Al-Haj, *et. al.*, 2016). Untuk mencegah kebocoran dan manipulasi data oleh pihak yang tidak berwenang terjadi, perlu adanya upaya pengamanan terhadap citra rekam medis. Impelementasi apapun pada aplikasi *telemedicine* harus memenuhi standar *confidentiality, integrity,* dan *authentication (Al-Haj, et. al.*, 2016).

Salah satu bentuk pengamanan citra yang dapat digunakan pada citra rekam medis adalah dengan teknik kriptografi (Prastyo, 2019). Pengamanan citra rekam medis tersebut diantaranya dapat dilakukan dengan menggabungkan aspek *Confidentiality* dan *Integrity* pada teknik kriptografi, yaitu dengan menerapkan Algoritma *Rivest Code 6* dalam proses enkripsi dan dekripsi citra, yang dapat

mengamankan kerahasiaan citra rekam medis, serta dipadukan dengan Algoritma *Keccak* sebagai fungsi nilai *hash* yang dapat menjaga *integrity* atau keaslian citra. *Confidentiality* pada kriptografi merupakan proses mengamankan pesan dengan proses enkripsi-dekripsi. Salah satu algoritma untuk proses enkripsi adalah *Rivest Code 6* (RC 6), algoritma ini merupakan algoritma *block cipher* yang memiliki aturan *RC6-w/r/b*, yaitu algoritma yang setiap katanya (*w*) memiliki panjang 32 bit, bekerja dengan 20 *round* (*r)* iteras, dan rentang kunci *b* dari 0 sampai 255 byte (Rhee, 2003). Berdasarkan penelitian Studi dan Analisis Algoritma *Rivest Code 6* (RC6) dalam Enkripsi/Dekripsi Data oleh Halik dan Prayudi tahun 2005, adanya fungsi $f(x) = x(2x+1)$ dan pergeseran 5 bit ke kiri membuat tingkat keamanan algoritma yang tinggi. Adanya *avalanche effect* juga memberikan kesulitan kepada kriptanalis untuk melakukan serangan (Halik and Prayudi, 2005). Namun terdapat kekurangan jika hanya menerapkan algoritma RC6 saja, yaitu hasil proses enkripsi dan dekripsi tidak dapat membuktikan bahwa citra rekam medis tersebut adalah file citra yang asli. Untuk itu dibutuhkan Algoritma *Keccak* dalam upaya menjaga keaslian citra yang dapat dipercaya. Algoritma *Keccak* akan membuat nilai *hash* yang berfungsi sebagai nilai *integrity* dari sebuah citra rekam medis.

Kegiatan ini berkonsep mengamankan keaslian citra digital *PET Scan* dengan menerapkan algoritma *Keccak* yang berfungsi sebagai keamanan *integrity* pada citra, sehingga menghasilkan nilai *hash*, yang kemudian akan digunakan sebagai validasi untuk citra yang diamankan dengan proses enkripsi dan dekripsi menggunakan algoritma RC6. Nilai *hash* yang didapatkan ketika proses dekripsi akan dibandingkan dengan nilai *hash* pada citra asli yang belum melalui proses enkripsi dan dekripsi. Kemudian hasil dari proses pengamanan citra akan diuji untuk meninjau keberhasilan dari proses perpaduan kedua algoritma. Pengujian yang dilakukan yaitu menguji keberhasilan algoritma RC6 dalam proses pengamanan citra, pengujian algoritma *Keccak* dalam menjaga *integrity* citra, dan pengaruh proses pengamanan citra terhadap kualitas citra.

Dengan memadukan algoritma *Keccak* dan RC6 apakah dapat mengamankan citra digital rekam medis dengan baik tanpa mengubah kualitas citra? Diharapkan, nantinya perpaduan algoritma ini dapat memperbaiki tingkat

keamanan citra digital *PET Scan*. Pada kegiatan sebelumnya yang dilakukan oleh Yugo Bayu Prastyo (2019), pengamanan citra medis dilakukan dengan mengkombinasikan algoritma *Advanced Encryption Standard* (AES) sebagai enkripsi dan dekripsi, dan algoritma Diffie-Hellman sebagai pertukaran kunci. (Prastyo, 2019).

1.2 Rumusan Masalah

Berdasarkan penjabaran pada latar belakang, permasalahan yang akan dibahas adalah:

1. Bagaimana proses memadukan *hashing* algoritma *Keccak* dengan algoritma *Rivest Code 6* dalam mengamankan citra dapat mengamankan integritas digital rekam medis?
2. Apakah algoritma *Keccak* dapat mengamankan *integrity* pada citra digital *PET Scan*?
3. Apakah algoritma RC6 dapat mengamankan kerahasiaan citra digital *PET Scan*?
4. Apakah proses pengamanan citra dapat mempengaruhi kualitas citra?

1.3 Batasan Masalah

Adapun batasan masalah pada kegiatan ini, terbatas sebagai berikut:

1. Penelitian terfokus pada analisa dan pengujian algoritma *Keccak* dan RC6 dalam mengamankan citra digital
2. File citra digital *PET Scan* yang digunakan berupa citra PET dalam format JPG atau JPEG
3. Algoritma *Keccak* diterapkan sebagai *hashing* atau *integrity*
4. Algoritma RC6 digunakan sebagai enkripsi dan dekripsi citra.

1.4 Tujuan dan Manfaat

Adanya kegiatan ini bertujuan menganalisis keamanan citra digital rekam medis menggunakan kombinasi algoritma Keccak dan RC6 dalam menjaga keaslian citra digital *PET Scan*, yaitu memadukan fungsi *hashing* menggunakan algoritma *Keccak* dan mengembangkan sistem keamanan citra menggunakan algoritma RC6

pada proses enkripsi-dekripsi serta pengaruh proses enkripsi-dekripsi terhadap citra.

1.5 Manfaat Penelitian

Manfaat yang dapat diambil dari kegiatan ini, sebagai berikut:

a. Untuk Ilmu Pengetahuan dan Penelitian

   Sebagai alternatif pengamanan citra digital terutama pada citra digital rekam medis. Pengembangan keilmuan di bidang kriptografi, yaitu dengan adanya kombinasi dua algoritma antara algoritma *Keccak* dan RC6 yang dapat dikembangkan dan diimplementasikan dalam bidang teknologi informasi.

b. Untuk Penulis

   Meningkatkan kemampuan dan wawasan dalam bidang kriptografi terutama mengenai algoritma RC6 dan algoritma *Keccak*.

1.6 Ruang Lingkup

Terdapat ruang lingkup pada kegiatan ini, yaitu pembahasan mengenai algoritma *Keccak* dalam penerapan *integrity* pada citra digital *PET Scan*, dan proses enkripsi dan dekripsi citra dalam upaya mengamankan citra digital *Positron Emission Tomography (PET) scan.* Perancangan aplikasi algoritma *Keccak* dan algoritma RC6, menggunakan Bahasa pemrograman C++. Data yang digunakan pada penelitian merupakan data sekunder dari website http://cancerimagingarchive.net yang terdiri dari 20 sampel citra digital rekam medis PET Scan. Analisa pengujian terhadap algoritma Keccak dan RC6 dalam mengamankan citra digital rekam medis, dengan medifikasi data menggunakan *hexadecimal editor* .Serta pengujian kualitas citra berdasarkan perbandingan ukuran dan informasi histogram pada citra asli dan citra hasil dekripsi.

1.7 Luaran yang Diharapkan

Luaran yang diharapkan ialah mengetahui tingkat keberhasilan algoritma *Keccak* dalam penerapan *integrity* dan keberhasilan algoritma RC6 dalam proses mengamankan citra digital *PET Scan* melalui proses pengujian, sebagai upaya

mengetahui performa dan ketahanan algoritma dalam mengamankan citra digital rekam medis.

1.8 Sistematika Penulisan

Sistematika penulisan yang digunakan pada kegiatan ini disusun dalam lima bab yang dibagi menjadi beberapa sub-bab di dalamnya, dan daftar pustaka yang disusun sebagai berikut:

BAB 1 PENDAHULUAN

Bab ini berisi Latar Belakang, Rumusan Masalah, Batasan Masalah, Tujuan Kegiatan, Manfaat Kegiatan, Ruang Lingkup, Luaran yang Diharapkan, dan Sistematika Penulisan pada kegiatan ini.

BAB 2 LANDASAN TEORI

Bab ini membahas teori dasar dari objek dan metode yang digunakan pada kegiatan ini.

BAB 3 METODOLOGI KEGIATAN

Bab ini membahas metode kegiatan yang digunakan oleh penulis beserta urutan tahapan yang dilakukan dalam proses kegiatan.

BAB 4 HASIL DAN PEMBAHASAN

Bab ini menjelaskan bagaimana hasil penerapan algoritma *Keccak* dalam proses penerapan *hashing* sebagai *integrity* pada citra digital *PET Scan*, dan enkripsi-dekripsi pada citra menggunakan algoritma RC6.

BAB 5 PENUTUP

Bab ini berisi kesimpulan dan saran dari hasil kegiatan sebagai acuan pada kegiatan berikutnya.

DAFTAR PUSTAKA

RIWAYAT HIDUP

LAMPIRAN