Implementasi Teknik Kriptografi pada Dokumen Rekam Medis Pasien

Nicholas Chen - 13519029
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jalan Ganesha 10 Bandung
E-mail (gmail): 13519029@std.stei.itb.ac.id

***Abstrak*—Dokumen rekam medis adalah salah satu dokumen yang harus dimiliki setiap instansi rumah sakit saat menangani pasien mereka. Dokumen ini biasanya dibuat diatas kertas yang ditandatangani dan disimpan ke repositori klasik. Penyimpanan dengan cara ini memiliki beberapa masalah, terutama pada bagian keamanan informasi. Pada makalah ini, sebuah teknik penyimpanan diusulkan menggunakan beberapa konsep kriptografi, seperti cipher simetris, fungsi *hash*, algoritma Kunci-Publik, tanda tangan digital, serta konsep *blockchain*. Sebuah arsitektur cara penyimpanan dokumen rekam medis dibuat berdasarkan konsep-konsep tersebut untuk meningkatkan penyimpanan dokumen rekam medis terutama di sisi keamanan informasi.**

Kata Kunci—rekam medis; keamanan informasi; kriptografi; cipher simetri; fungsi hash; algoritma Kunci-Publik; tanda tangan digital; blockchain

I. Pendahuluan

Dewasa ini perkembangan ilmu kriptografi semakin cepat dan semakin mendisrupsi banyak cabang bidang keilmuan lainnya, seperti pada bidang ekonomi / bisnis, hukum, politik, keamanan, pendidikan, dan kesehatan. Bidang-bidang keilmuan yang membutuhkan penjagaan kerahasiaan dokumen ataupun keaslian pesan sangat bergantung pada penggunaan teknik-teknik kriptografi. Hal ini semakin diperparah dengan melesatnya teknologi yang membuat oknum semakin mudah untuk melakukan kecurangan seperti menguping tanpa izin (*eavesdropping*), serangan pengubahan pesan, pemalsuan tanda-tangan, dan tindakan–tindakan lainnya.

Saat ini, sebagian besar dokumen terutama dokumen-dokumen medis seperti rekam medis masih ditandatangani dengan cara klasik. Adanya tanda tangan klasik ini membuat pesan pada dokumen tersebut memang dapat lebih dipertanggung jawabkan, akan tetapi hal-hal seperti pemalsuan tanda tangan dan pengubahan dokumen setelah proses tanda tangan belum dapat dicegah dengan tanda tangan klasik tersebut.

Isi dari dokumen rekam medis yang telah dibuat atau diterbitkan seseorang seperti dokter ataupun tenaga medis harus dapat dijaga keasliannya agar dapat dipertanggung jawabkan isinya saat dibutuhkan untuk penanganan medis berikutnya. Isi dokumen rekam medis yang terjaga dapat mengurangi kasus seperti misdiagnosis, mistreatment, kesalahan pemberian obat, dan sebagainya. Oleh karena itu, sebuah teknik keamanan yang dapat menjaga keaslian pesan dibutuhkan agar tidak ada pihak ketiga yang tidak bertanggung jawab yang dapat mengubah isi pesan atau dokumen medis secara diam-diam.

PEMERINTAH KABUPATEN PONOROGO
DINAS KESEHATAN
UPT PUSKESMAS PONOROGO UTARA
Jl. Pahlawan No. 30 Telp (0352) -485446 Email : puskesmas_poutara@yahoo.com
PONOROGO

RM.01

PENGKAJIAN DATA UMUM PASIEN

Diisi oleh Petugas Pendaftaran pada Tanggal : ..... Jam : .....

IDENTITAS PASIEN

(Diisi sesuai Kartu Tanda Pengenal Pasien yang masih berlaku, KTP/ KK/ SIM/ Kartu Pelajar/ dsb)

Nomer Rekam Medis : .....
Nama : ..... No. NIK : .....
Jenis Kelamin : □ Laki-laki □ Perempuan
Tanggal Lahir : .....
Agama : .....
Pendidikan : □ Belum /tidak tamat SD □ SD □ SLTP □ SLTA □ Diploma □ Sarjana
Pekerjaan : .....
Alamat : Jalan ..... RT / RW .....
Lingkungan / Dukuh ..... Kelurahan / Desa .....
Kecamatan ..... Kabupaten .....
Status Perkawinan : □ Kawin □ Belum Kawin □ Janda □ Duda
Nama Suami / Istri : .....
Status Pembiayaan : □ Umum
□ BPJS (PBI / Mandiri / PNS / TNI / POLRI / .....)
No. Peserta .....

PERSETUJUAN UMUM / GENERAL CONSENT

PASIEN / WALI PASIEN HARUS MEMBACA, MEMAHAMI DAN MENGISI INFORMASI BERIKUT

Yang bertanda tangan di bawah ini, saya :
Nama Lengkap : ..... L / P
Tempat/ tgl lahir : .....
Alamat : .....
No. Telepon : .....
Bertindak atas nama : diri saya sendiri / ..... *(nama pasien yang identitasnya tersebut di atas)*

Menyatakan

I. PERSETUJUAN UNTUK PERAWATAN DAN PENGOBATAN

1. Saya mengetahui bahwa saya memiliki kondisi yang membutuhkan perawatan medis, saya mengijinkan dokter/tenaga kesehatan lainnya di Puskesmas Ponorogo Utara untuk melakukan pemeriksaan dan memberikan pengobatan / tindakan / asuhan sesuai prosedur.
2. Saya sadar bahwa praktik kedokteran bukanlah ilmu pasti dan saya mengakui bahwa tidak ada jaminan atas hasil apapun terhadap prosedur pengobatan/ asuhan/ tindakan lainnya yang dilakukan kepada saya.
3. Saya mengerti dan memahami bahwa :
   a. Saya memiliki hak untuk menyatakan persetujuan atau menolak untuk setiap prosedur atau terapi yang akan diberikan kepada saya.
   b. Saya memiliki hak untuk mengajukan pertanyaan tentang rencana pelayanan yang akan diberikan kepada saya, termasuk identitas setiap orang yang akan memberikan pelayanan pemeriksaan / tindakan kepada saya.

II. PERSETUJUAN PELEPASAN INFORMASI

1. Saya memahami bahwa informasi yang ada dalam diri saya terkait dengan kondisi kesehatan saya, berdasarkan pemeriksaan yang saya jalani di Puskesmas Ponorogo Utara, akan terjamin kerahasiaannya.
2. Saya memberi wewenang kepada Puskesmas Ponorogo Utara untuk memberikan informasi terkait kondisi kesehatan saya bila diperlukan untuk keperluan proses klaim asuransi (JKN dan sebagainya).
3. Saya memberi wewenang kepada Puskesmas Ponorogo Utara untuk memberikan informasi tentang kondisi kesehatan saya kepada yang tersebut berikut ini :
   a. .....
   b. .....
   c. .....

III. HAK DAN KEWAJIBAN PASIEN

Saya telah mendapat informasi tentang "Hak dan Kewajiban Pasien" di Puskesmas Ponorogo Utara melalui media informasi yang disediakan oleh petugas Puskesmas.

IV. INFORMASI BIAYA PELAYANAN PUSKESMAS

Saya telah memahami tentang informasi biaya pengobatan dan biaya tindakan yang disampaikan oleh pihak Puskesmas, dan saya bersedia untuk membayar biaya tersebut sesuai peraturan yang berlaku.

Demikian Persetujuan Umum (*"General Consent"*) ini telah saya baca dan saya pahami.

Petugas	Ponorogo, ... Pasien / Wali Pasien
.....	.....
Tanda Tangan dan Nama Terang	Tanda Tangan dan Nama Terang

Gambar 1. Contoh Template Rekam Medis Klasik pada salah satu Instansi Rumah Sakit

Dokumen dari rekam medis yang dibuat atau diterbitkan oleh sebuah instansi kesehatan juga perlu dapat diidentifikasi pembuatnya. Hal ini bertujuan agar dapat mempermudah proses hukum saat terjadi kasus atas dokumen tersebut. Jika terjadi kesalahan hasil diagnosa ataupun kesalahan resep obat

oleh karena kesalahan pada rekam medis sebelumnya, penanggung jawab atas dokumen rekam medis tersebut jelas dan dapat diketahui dengan mudah. Hal ini juga akan jauh lebih baik jika terdapat teknik yang membuat pembuat dokumen tidak dapat mengelak bahwa dirinya bukan pembuat dokumen tersebut.

Berdasarkan masalah-masalah yang telah dijabarkan sebelumnya, sebuah teknik keamanan kriptografi yang dapat menanganinya dibutuhkan pada bidang kesehatan. Dengan adanya teknik kriptografi yang dapat memenuhi kebutuhan tersebut, maka dokumen-dokumen rekam medis dapat lebih aman dan lebih dapat dipertanggung jawabkan.

II. Dasar Teori

A. Dokumen Medis

Tenaga medis dan pekerja rumah sakit dalam melakukan pekerjaannya, mereka membutuhkan sebuah media untuk mencatat berbagai hal seperti, mencatat rekam medis pasien, membuat surat izin dokter, menuliskan resep, dan sebagainya. Dokumen-dokumen yang telah dibuat ini sebagian besar bersifat sensitif dan privat, tidak sembarang pihak boleh mengaksesnya. Oleh karena itu terhadap dokumen-dokumen ini perlu diberi proteksi agar isi dokumen tetap terjaga.

Terdapat beberapa kriteria yang perlu diperhatikan pada penjagaan dokumen-dokumen ini (sebagian dokumen tidak perlu memiliki seluruh kriteria), diantaranya seperti:

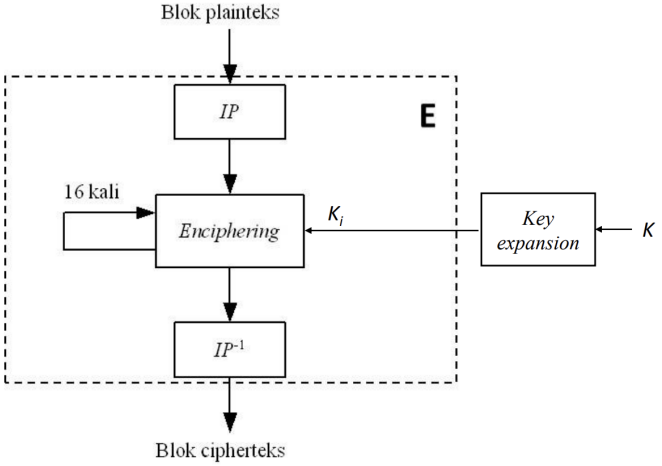
1. Kerahasiaan pesan (*confidentiality*) agar dokumen tidak dapat dilihat pihak ketiga;
2. Keaslian pesan (*integrity*) agar keutuhan isi pada dokumen tetap terjamin;
3. Otentikasi (*authentication*) agar pembuat atau penerbit dokumen dapat diidentifikasi dengan jelas; serta
4. Anti Penyangkalan (*nonrepudiation*) untuk dokumen yang penulisnya perlu diketahui agar isi dokumen memiliki penanggung jawab.

Pada dokumen rekam medis yang dibuat oleh dokter, isi dari dokumen tersebut tidak boleh diketahui publik demi kepentingan privasi pasien.Selain itu, isi dari dokumen rekam medis tidak boleh diubah seenaknya tanpa sepengetahuan pihak yang bersangkutan agar tidak terjadi masalah medis pada pasien. Berikutnya, pada setiap dokumen rekam medis harus tercantum juga tanda tangan dari dokter atau tenaga medis yang melakukan operasi pada pasien terkait. Hal ini bertujuan agar dokumen rekam medis yang telah diterbitkan dapat dipertanggungjawabkan.

B. Algoritma Cipher Simetri

Algoritma cipher simetri adalah teknik yang memanfaatkan sebuah kunci untuk melakukan enkripsi dan dekripsi pada sebuah pesan agar isi pesan dapat dirahasiakan dari pihak ketiga. Ukuran dari pesan umumnya akan dibagi menjadi blok-blok berukuran kelipatan 2^n seperti 64 bit, 128 bit, 256 bit, dan seterusnya. Setelah masing-masing blok dienkripsi, hasilnya dapat digabung kembali menjadi pesan rahasia yang utuh (*cipher text*). Ukuran pesan awal dan pesan rahasia umumnya sama panjang.

Salah satu algoritma cipher simetri yang umum digunakan adalah DEA (*Data Encryption Algorithm*) yang juga telah ditetapkan sebagai standar dari enkripsi data (*DES*). Pada DES, setiap blok pada pesan awal akan dienkripsi dalam 16 putaran menggunakan kunci internal yang berbeda. Kunci-kunci internal dengan ukuran 48-bit untuk masing-masing putaran dibangkitkan dari sebuah kunci eksternal yang harus dirahasiakan. Sebelum putaran untuk masing-masing kunci internal dimulai, blok-blok pesan awal akan dipermutasi terlebih dahulu menggunakan fungsi IP. Setelah proses putaran selesai, hasil akan dikembalikan semula urutannya menggunakan fungsi inverse IP^{-1}.



Gambar 2. Skema global algoritma DES

C. Algoritma Kunci-Publik

Algoritma Kunci-Publik adalah salah satu algoritma kriptografi yang dapat digunakan untuk mengenkripsi sebuah pesan agar isinya tidak dapat diketahui oleh pihak ketiga. Algoritma ini menggunakan kunci asimetri, yang artinya kunci yang digunakan untuk melakukan enkripsi dan melakukan dekripsi pesan tidak sama.

Kunci yang digunakan untuk mengenkripsi pesan dinamakan kunci publik (*public key*), sedangkan kunci yang digunakan untuk mendekripsi pesan adalah kunci privat (*private key*). Kunci publik dapat disebarkan kepada orang yang ingin mengirim pesan kepada penerima pesan, sedangkan kunci privat harus dijaga oleh sang penerima pesan agar pesan yang dikirimkan orang lain untuknya tidak dapat didekripsi oleh orang lain.

Salah satu algoritma kunci publik yang saat ini digunakan adalah RSA. Algoritma RSA memanfaatkan kesulitan untuk memfaktorkan bilangan bulat yang besar menjadi faktor-faktor prima. Untuk membuat sepasang kunci publik dan kunci privat algoritma RSA, terdapat langkah-langkah yang harus dipenuhi yaitu:

1. Pilih dua bilangan prima p dan q yang tidak sama nilainya
2. Hitung nilai $n = pq$
3. Hitung nilai $\phi(n) = (p - 1)(q - 1)$

4. Pilih sebuah bilangan bulat e sebagai kunci publik, dengan e relatif prima terhadap nilai n
5. Hitung nilai d dari persamaan ed ≡ 1 (mod ϕ(n))

Dari langkah diatas akan dihasilkan kedua kunci publik dan privat, yaitu (e, n) sebagai kunci publik dan (d, n) sebagai kunci privat. Untuk melakukan proses enkripsi, pesan dibagi menjadi blok-blok pesan yang lebih kecil dengan besar masing-masing blok lebih kecil dari nilai (n - 1). Setelah itu, masing-masing blok pesan akan dihitung blok ciphernya dengan persamaan sebagai berikut:

$$c_i = m_i^e \bmod n$$

Setelah pesan yang terenkripsi sampai kepada penerima, pesan yang terenkripsi tersebut dibagi kembali menjadi ukuran yang sama dengan proses sebelumnya. Kemudian masing-masing blok tersebut akan didekripsi dengan persamaan sebagai berikut:

$$m_i = c_i^d \bmod n$$

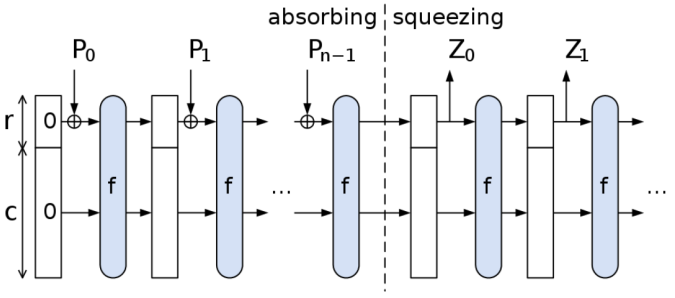
D. Fungsi Hash

Fungsi Hash adalah sebuah fungsi yang dapat mengkompresi sebuah pesan yang memiliki ukuran sembarang menjadi nilai hash (*string*) yang memiliki panjang tetap. Keluaran dari fungsi ini dinamakan pesan ringkas (*message digest*) yang berisi karakter acak dan tidak dapat dikembalikan menjadi pesan semula (*irreversible*). Pesan yang dimasukkan ke dalam fungsi ini selalu memiliki keluaran pesan ringkas yang sama.

Terdapat 3 sifat yang harus dipenuhi oleh sebuah fungsi hash, yaitu:

1. collision resistance (sangat sukar menemukan dua buah input yang memiliki nilai ringkas yang sama),
2. preimage resistance (sangat sukar untuk menemukan pesan awal jika diketahui nilai pesan ringkasnya), serta
3. second preimage resistance (sangat sukar menemukan sebuah pesan b yang memiliki nilai H(a) jika diketahui sebuah pasangan input a dan output H(a)).

Salah satu fungsi hash yang saat ini digunakan adalah SHA-3 atau disebut juga sebagai Keccak. Fungsi Hash Keccak dapat menerima input yang memiliki panjang sebarang dan dapat mengeluarkan output pesan ringkas sepanjang 224, 256, 384, atau 512 bits. Fungsi ini memiliki 2 fase dalam membuat pesan awal menjadi pesan ringkas, antara lain fase penyerapan (*absorbing phase*) dan fase pemerasan (*squeezing phase*).



Gambar 3. Alur Kerja Fungsi SHA-3 (Keccak)

Pada tahap praproses, pesan awal yang ingin diringkas sebelumnya ditambahkan bit *padding* sehingga panjangnya dapat habis dibagi dengan *r* atau n = *length*(P) / *r*. Selanjutnya pesan tersebut dibagi menjadi blok-blok P_i berukuran r-bit.

Untuk memulai proses penyerapan, sebuah *b*-bit dari peubah status (*state*) diinisiasikan menggunakan bit nol dengan *b* = *r* + c. Berikutnya *b*-bit ini akan dioperasikan pada blok-blok pesan P_i secara berurutan. Blok-blok pesan P_i akan dilakukan operasi XOR dengan *r*-bit sebelum dimasukkan kedalam fungsi *f*. Hasil dari fungsi *f* pada status (*state*) ini akan digunakan sebagai input pada status berikutnya.

Pada fase pemerasan, blok *r* dari output fase sebelumnya akan diambil sebagai sub bagian dari pesan ringkas Z_i. Proses ini dilakukan hingga total panjang dari pesan ringkas sama dengan panjang pesan ringkas yang diinginkan (224, 256, 384, atau 512 bits).

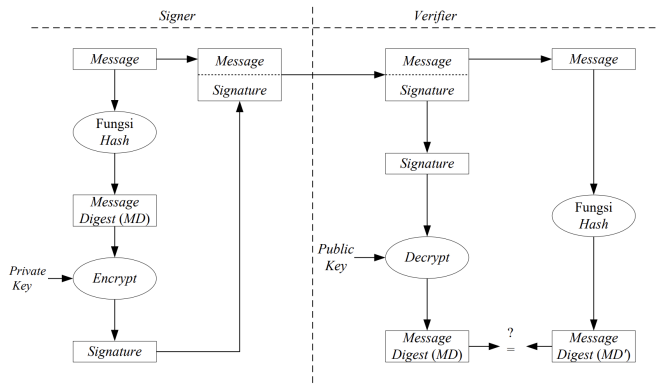
E. Tanda Tangan Digital

Tanda tangan digital adalah proses pembubuhan tanda tangan yang dilakukan sebagai bukti keabsahan dokumen secara digital menggunakan bantuan komputasi komputer. Pada proses pembuatan tanda tangan digital, terdapat 2 konsep kriptografi yang digunakan, yaitu konsep algoritma Kunci-Publik dan konsep fungsi hash.

Pada algoritma Kunci-Publik, kunci publik digunakan untuk mengenkripsi pesan untuk dikirim kepada sang pemilik kunci privat. Walaupun konsep algoritma ini dapat menjaga pesan yang dikirimkan kepada seseorang dengan baik, konsep ini tidak dapat mengidentifikasi identitas sang pengirim pesan karena kunci publik yang sama diketahui oleh banyak orang (diketahui publik). Oleh karena itu, cara lain dibutuhkan agar identitas sang pengirim pesan dapat diketahui.

Konsep algoritma Kunci-Publik digunakan secara terbalik untuk dapat membuat tanda tangan digital. Hal ini dilakukan agar penerima pesan dapat mengidentifikasi sang pengirim pesan. Kunci privat sang pengirim pesan akan digunakan untuk mengenkripsi pesan. Selanjutnya hasil enkripsi ini akan dikirim kepada sang penerima dan didekripsi menggunakan kunci publik sang pengirim pesan.

Pada proses penandatanganan suatu dokumen, umumnya pesan yang ditandatangani tidak bersifat rahasia. Selain itu, untuk mengenkripsi seluruh dokumen menggunakan algoritma Kunci-Publik umumnya tidak efisien karena waktu komputasi yang relatif lama. Oleh karena itu, fungsi hash digunakan untuk mengatasi masalah tersebut.



Gambar 4. Alur Kerja Proses Penandatanganan dan Verifikasi Suatu Pesan Dengan Tanda Tangan Digital

Pesan awal yang ingin ditandatangani sebelumnya dimasukkan ke dalam fungsi hash sehingga memiliki panjang yang lebih pendek. Selanjutnya pesan ringkas dari hasil fungsi hash dienkripsi menggunakan kunci privat dari pengirim pesan untuk dihasilkan tanda tangan digital. Tanda tangan digital yang sudah dibuat dapat ditempelkan pada bagian akhir pesan awal.

Setelah pesan dengan tanda tangan digital tersebut sampai kepada penerima pesan, sang penerima pesan dapat melakukan verifikasi terhadap pesan apakah benar dikirim oleh pengirim yang valid menggunakan kunci publik sang pengirim pesan. Tanda tangan digital pada pesan diambil dan didekripsi menggunakan kunci publik tersebut. Selanjutnya pesan yang diterima juga dimasukkan ke dalam fungsi hash. Jika kedua hasil tersebut sama, maka pesan yang diterima adalah valid dari sang pengirim. Namun jika berbeda, maka terdapat indikasi penggantian isi dari dokumen ataupun pengirim yang tidak valid.

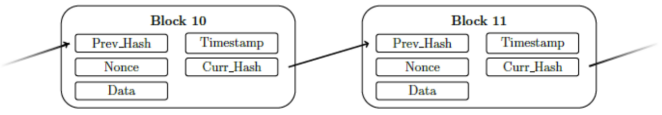
F. Blockchain

Blockchain merupakan sebuah konsep yang terinspirasi dari konsep buku besar (*ledger*) pada bidang akuntansi yang dapat dikelola secara kolektif dan terdesentralisasi. Dengan sistem yang terdesentralisasi, setiap orang yang berkontribusi di dalam *blockchain* memiliki catatan sendiri sehingga tidak membutuhkan adanya pihak ketiga seperti bank.

Konsep blockchain memiliki karakteristik seperti berikut:

1. menghilangkan ketergantungan dengan pihak ketiga sebagai pihak penengah,
2. melibatkan banyak pihak yang tidak perlu saling percaya satu sama lain,
3. menggunakan sistem konsensus untuk melakukan validasi dari transaksi yang dicatat,
4. setiap transaksi dapat dicatat menggunakan *timestamp* (*traceable*), serta
5. immutable sehingga transaksi yang telah dibuat tidak dapat dihapus kembali.

Setiap transaksi baru ingin ditambahkan ke dalam *blockchain*, transaksi tersebut akan dicatat menggunakan arsitektur *peer-to-peer* dengan sesama pengguna *blockchain* tersebut. Pada transaksi baru tersebut, nilai hash dari transaksi sebelumnya akan disematkan. Selanjutnya nilai dari transaksi baru ini juga dimasukkan ke dalam fungsi hash dan dicatat hasil pesan ringkasnya untuk transaksi berikutnya.



Gambar 5. Ilustrasi dari Transaksi yang Dicatat pada *Blockchain*

Seiring bertambahnya transaksi yang masuk, transaksi-transaksi tersebut akan membentuk sebuah rantai yang terhubung satu sama lain. Oleh karena hal itu, transaksi yang telah dimasukkan ke dalam *blockchain* tidak dapat dihapus kembali (*immutable*).

III. Rancangan Solusi dan Implementasi

Untuk menyelesaikan masalah yang telah dijabarkan pada bab sebelumnya, penyelesaian solusi dibagi menjadi beberapa bagian, yaitu Deskripsi Umum, Rancangan, dan Implementasi Solusi.

A. Deskripsi Umum Solusi

Penggabungan beberapa konsep dari kriptografi akan diterapkan sebagai solusi untuk dapat menyimpan dokumen rekam medis dengan baik dan aman. Hal ini dilakukan agar masing-masing masalah yang telah dijabarkan sebelumnya dapat ditangani oleh masing-masing teknik kriptografi yang sesuai.

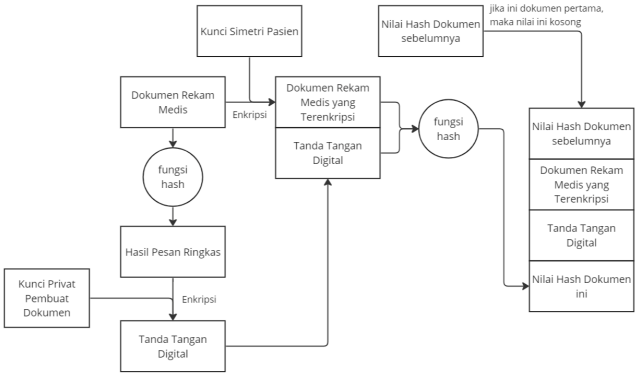
Pertama, pada setiap dokumen rekam medis yang ingin disimpan perlu ditandatangani secara digital oleh pembuat dokumen (seperti dokter, perawat, atau tenaga medis) terlebih dahulu. Tanda tangan digital akan dibuat dengan bantuan algoritma Kunci-Publik RSA dan fungsi hash SHA-3 (Keccak).

Kedua, isi dari dokumen rekam medis perlu dienkripsi menggunakan algoritma cipher simetri sebelum disimpan untuk menjaga kerahasiaan isi dokumen dari pihak ketiga. Algoritma cipher simetri yang diimplementasikan adalah algoritma cipher simetri DES.

Ketiga, dokumen rekam medis masing-masing pasien akan disimpan dalam bentuk *blockchain* tersendiri sehingga rekam medis akan tersimpan berurutan secara historis. Hal ini dilakukan agar kelengkapan dan keterurutan dari rekam medis masing-masing pasien dapat terjaga.

B. Rancangan Solusi

Solusi yang dirancang dibagi menjadi 2 bagian, yaitu tahap memasukkan rekam medis ke dalam *blockchain* serta tahap verifikasi dokumen rekam medis yang sudah tersimpan. Pada tahap memasukkan rekam medis, terdapat 3 hal yang perlu dilakukan, yaitu menandatangani dokumen, mengenkripsi isi dokumen, serta membuat dokumen ke dalam format *blockchain*. Pada tahap verifikasi rekam medis, tanda tangan digital dapat didekripsi dan dicek kesamaannya dengan isi dokumen.

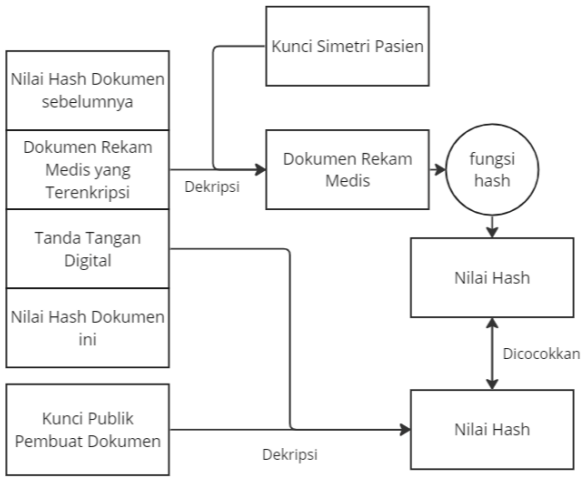


Gambar 6. Alur Kerja Penambahan Dokumen Rekam Medis Baru

Sebelum sebuah dokumen rekam medis yang baru ditambahkan ke dalam *blockchain* pasien terkait, pembuat dokumen (seperti dokter, perawat, atau tenaga medis) perlu mencantumkan tanda-tangan digital ke dalam dokumen rekam medis. Tanda tangan digital akan dibuat menggunakan fungsi hash SHA-3 (Keccak) dengan isi dokumen sebagai inputnya. Pesan ringkas yang dihasilkan berikutnya akan dienkripsi dengan kunci privat dari algoritma Kunci-Publik RSA sebagai hasil tanda tangan digital.

Isi dari dokumen rekam medis yang sudah memiliki tanda tangan digital akan dienkripsi menggunakan algoritma cipher simetri DES. Kunci enkripsi yang digunakan dapat dibedakan untuk setiap pasien dan disimpan pada repositori terpisah. Perlu dicatat bahwa dokumen harus dienkripsi setelah ditandatangani. Hal ini dilakukan agar hanya orang yang memiliki akses kunci simetri pasien dapat melakukan verifikasi dari tanda tangan digital.

Berikutnya, seluruh isi dokumen yang sudah dienkripsi beserta tanda tangan digitalnya akan dimasukkan ke dalam fungsi hash untuk menghasilkan nilai ringkas yang berperan sebagai *pointer* antar dokumen rekam medis. Nilai ringkas ini beserta nilai ringkas dari dokumen sebelumnya akan digabung dengan isi dokumen yang sudah dienkripsi beserta tanda tangan digitalnya untuk membentuk sebuah blok baru di *blockchain* tersebut. Jika dokumen yang dimasukkan merupakan dokumen pertama, maka nilai hash dokumen sebelumnya dapat dikosongkan.



Gambar 7. Alur Kerja Verifikasi Dokumen Rekam Medis

Pada tahap verifikasi dokumen medis, tanda tangan digital dan isi dokumen yang terenkripsi akan diambil dari blok pada *blockchain*. Isi dokumen didekripsi terlebih dahulu menggunakan kunci simetri pasien, kemudian hasil dekripsi tersebut digunakan sebagai input fungsi hash untuk menghasilkan pesan ringkas A. Selanjutnya, tanda tangan digital didekripsi menggunakan kunci publik penulis dokumen menghasilkan output B. Jika hasil dari pesan ringkas A dan output B sama, maka dokumen rekam medis tersebut valid, sedangkan jika berbeda maka terdapat pergantian isi dokumen atau kunci publik yang tidak cocok.

C. Implementasi Solusi

Pertama, dokumen rekam medis yang ingin disimpan harus ditandatangani terlebih dahulu. Dokumen tersebut akan dimasukkan ke dalam fungsi hash SHA-3 (Keccak) untuk menghasilkan pesan ringkas sepanjang 256-bits. Selanjutnya pesan dienkripsi dengan kunci privat menggunakan algoritma RSA dengan panjang kunci 1024-bits untuk menghasilkan tanda tangan digital.

Tabel 1. Proses Pembentukan Tanda Tangan Digital

Contoh Isi Dokumen Rekam Medis	
Nama Pasien: Ahmad Kasim Umur: 32 tahun Tanggal dan waktu: 22 Mei 2023, 11:07 Keluhan: sesak nafas Riwayat penyakit: asma Hasil pemeriksaan fisik dan penunjang medik Diagnosis: sesak nafas, lemas Pengobatan dan/atau tindakan: Pemberian oksigen Pelayanan lain yang diberikan kepada pasien: -	
Hasil hash	31e1dfcf3db25ae4712e0ff531f2ae13053deec5d1396e7066ee58c71b393ff4

Kunci Publik Dokter	MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDLlWeKowErvEOFyffPTE6a8H+zzxD6sr0/6YcKE3LQ1Juq1Wja72z+5lScoTdq9KcZflMs/n6V8NPm7Uq30sRkNGIUUiwK8I8bDZkBlQjE9EaXT0dI+O/4S5wy4FXTWNKX2rIo8cgVFZPNXlUvbw8MN4NM4vDhQaEb9QRbqSy5qIDAQAB
Kunci Privat Dokter	MIICeAIBADANBgkqhkiG9w0BAQEFAASCAmIwggJeAgEAAoGBAMuVZ4qjASu8Q4XJ989MTprwf7PPEPqyvT/phwoTctDUm6rVaNrvbP7mVJyhN2r0pxl+Uyz+fpXw0+btSrfSxGQ0YhRSLArwjxsNmQGVCMT0RpdPR0j47/hLnDLgVdNY0pfasijxyBUVk81eVS9vDww3g0zi8OFBoRv1BFupLLmpAgMBAAECgYEAtBVxBd2zB3D9ebdykdi6H6xmCjQ8nMbHSWXVokAZ7EhlevRUUHZCQCiW6AZj8yR/O7nW8ZIdf50MlNWKppi2RyblBi5XsYc4FgVjn/hE8OCQcItWOd/L6feTGWx/vB5FGMzfGsVP23dvtJtkiy5stAogqBgJ4ewhpiU+GH4NmNECQQD/pzJn4lsCgWHNMvlAm34/vn60isQQL4oM3CDS2VY0fNQjWQrOY+t0TmNAdDXvpGp/ScQzhSbjjelBS+4aThMzAkEAy9we7avGOe4DBryqv3uGlpFz9kr0MwCBuv31r8HwlUDxcFconGlMn/e6uFxGBXwJiMttIHWzBzTxfhelMrV/swJBAMwEVclpbk+ViMMExry0Wg/sqZjSlJyGE5knolohbxX7+B8tU95ZBvGODM7G7rQLdaGW8Khcvigie97MBXugitkCQQCFhdZoG0NJfCBVUEuSAWlEw14tqihKI4HVJTO/e4qFZ7T7vMqnr7x1Zj/RMvbV7skb5QnD4fNxu/aUfQ5BqWlLAkAkWprY8O3kGmYW3rKcVo+hjHQddkrqQHunym09nNFdaXn1XUrS/Q4vWBHq8V4ksP7k1JI3vBJo1S436RgvaKNe
Hasil Enkripsi Kunci Privat (tanda tangan digital)	V3YYf+TJ5ODlNiJoxEpLWSbQZfSYZCaJY8xjckp9quozZZb0O6MwmIA4qU6KbLDkPPX55llwbnSlJdFY0olEG8uA3H/CnDuZE0CVJriljUt8H9NnI4s9UFWN9emnUxAix9EAXE/EH+rxWWqZWPNUsl9nH/MACPiXIj2BdZRao1o=

Setelah tanda tangan digital berhasil dibuat, isi dari dokumen rekam medis akan dienkripsi menggunakan algoritma cipher simetri DES.

Tabel 2. Proses Enkripsi Isi Dokumen Rekam Medis Menggunakan Cipher Simetri

Kunci simetri	pasien07
Hasil enkripsi isi rekam medis menggunakan DES	/jj4P9A5QUgq4D84mfhnhuuQ/+NhHO19TPTuD6eeWVUFOCsCGIJSTlJjIo9staWNoFnim72Vwmd7ataznJWD11rGiiOelCqRMOLu1/8HE95ZHLrf4b43rMuzuOjbkTqWfOltVvqIfQyiBnZUqf3wTaTp5+5L6TBWmqtzre6ZbRlggQ8/OoxabWVHVPfH1LJMa0So/q+zLXEN1p/yHvUWwkOuJTOhHBx+XCAFh3B2DyDeNal8Nl7k2sKV0WQIYxtMdtjyfK8J2+OvjEf8hjLnHKF3yfW2XKZmB84+PfkSv4eFaGwew/+eE1w31gKEDOALtg3cVKpjwTXxsS0juD0JB9gcThmbep05tZbB47wETxRFp0pwlW+J4OmJCgPj4cB+w3igldQB1KB65iafbiEDg==

Hasil enkripsi rekam medis digabung dengan hasil tanda tangan digital sebelumnya untuk membentuk sebuah blok baru. Blok ini kemudian dimasukkan kembali ke dalam fungsi hash untuk menghasilkan pesan ringkas blok ini. Jika blok tersebut bukan merupakan blok pertama, masukkan juga pesan ringkas blok sebelumnya pada blok sekarang sebagai *pointer*.

Tabel 3. Proses Pembentukan blok baru pada *blockchain*

Isi Dokumen Rekam Medis yang sudah dienkripsi beserta tanda tangan digitalnya	/jj4P9A5QUgq4D84mfhnhuuQ/+NhHO19TPTuD6eeWVUFOCsCGIJSTlJjIo9staWNoFnim72Vwmd7ataznJWD11rGiiOelCqRMOLu1/8HE95ZHLrf4b43rMuzuOjbkTqWfOltVvqIfQyiBnZUqf3wTaTp5+5L6TBWmqtzre6ZbRlggQ8/OoxabWVHVPfH1LJMa0So/q+zLXEN1p/yHvUWwkOuJTOhHBx+XCAFh3B2DyDeNal8Nl7k2sKV0WQIYxtMdtjyfK8J2+OvjEf8hjLnHKF3yfW2XKZmB84+PfkSv4eFaGwew/+eE1w31gKEDOALtg3cVKpjwTXxsS0juD0JB9gcThmbep05tZbB47wETxRFp0pwlW+J4OmJCgPj4cB+w3igldQB1KB65iafbiEDg== V3YYf+TJ5ODlNiJoxEpLWSbQZfSYZCaJY8xjckp9quozZZb0O6MwmIA4qU6KbLDkPPX55llwbnSlJdFY0olEG8uA3H/CnDuZE0CVJriljUt8H9NnI4s9UFWN9emnUxAix9EAXE/EH+rxWWqZWPNUsl9nH/MACPiXIj2BdZRao1o=

Hasil hash blok ini	db739678a1f3201310f165f496b86249e43cc8505b8337b3334e62cd191d2b14
Hasil hash blok sebelumnya (asumsi ini adalah blok pertama)	-

Untuk melakukan verifikasi pada isi dokumen rekam medis, isi dokumen yang terenkripsi dan tanda tangan digital dipisahkan kembali. Setelah itu, isi dokumen didekripsi menggunakan cipher simetri dengan kunci pasien dan dimasukkan hasilnya sebagai input dari fungi hash. Berikutnya tanda tangan digital didekripsi menggunakan kunci publik pembuat dokumen. Setelah itu, hasil dari fungsi hash dan hasil dari dekripsi kunci publik dicocokkan.

Tabel 4. Proses Validasi Isi Dokumen terhadap Tanda Tangan Digital

Isi Dokumen Rekam Medis yang terenkripsi	/jj4P9A5QUgq4D84mfhnhuuQ/+NhHO19TPTuD6eeWVUFOCsCGIJSTlJjIo9staWNoFnim72Vwmd7ataznJWD11rGiiOelCqRMOLu1/8HE95ZHLrf4b43rMuzuOjbkTqWfOltVvqIfQyiBnZUqf3wTaTp5+5L6TBWmqtzre6ZbRlggQ8/OoxabWVHVPfH1LJMa0So/q+zLXEN1p/yHvUWwkOuJTOhHBx+XCAFh3B2DyDeNal8Nl7k2sKV0WQIYxtMdtjyfK8J2+OvjEf8hjLnHKF3yfW2XKZmB84+PfkSv4eFaGwew/+eE1w31gKEDOALtg3cVKpjwTXxsS0juD0JB9gcThmbep05tZbB47wETxRFp0pwlW+J4OmJCgPj4cB+w3igIddQB1KB65iafbiEDg==
Tanda tangan digital	V3YYf+TJ5ODlNiJoxEpLWSbQZfSYZCaJY8xjckp9quozZZb0O6MwmIA4qU6KbLDkPPX55llwbnSlJdFY0olEG8uA3H/CnDuZE0CVJriljUt8H9NnI4s9UFWN9emnUxAix9EAXE/EH+rxWWqZWPNUsl9nH/MACPiXIj2BdZRao1o=
Kunci publik dokter	MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDLlWeKowErvEOFyffPTE6a8H+zzxD6sr0/6YcKE3LQ1Juq1Wja72z+5lScoTdq9KcZflMs/n6V8NPm7Uq30sRkNGIUUiwK8I8bDZkBlQjE9EaXT0dI+O/4S5wy4FXTWNKX2rIo8cgVFZPNXlUvbw8MN4NM4vDhQaEb9QRbqSy5qQIDAQAB

Hasil dekripsi isi dokumen	
Nama Pasien: Ahmad Kasim Umur: 32 tahun Tanggal dan waktu: 22 Mei 2023, 11:07 Keluhan: sesak nafas Riwayat penyakit: asma Hasil pemeriksaan fisik dan penunjang medik Diagnosis: sesak nafas, lemas Pengobatan dan/atau tindakan: Pemberian oksigen Pelayanan lain yang diberikan kepada pasien: -	
Hasil pesan ringkas dari hash isi dokumen	31e1dfcf3db25ae4712e0ff531f2ae13053deec5d1396e7066ee58c71b393ff4
Hasil dekripsi tanda tangan digital dengan kunci publik	31e1dfcf3db25ae4712e0ff531f2ae13053deec5d1396e7066ee58c71b393ff4

Pada contoh Tabel 4, isi dokumen tersebut lolos tahap verifikasi karena hasil dari fungsi hash dan hasil dari dekripsi kunci publik cocok. Jika pada isi dokumen ada yang diubah setelah proses pembentukkan tanda tangan, maka hasil hash tidak akan sama dengan hasil dekripsi tanda tangan digital.

Tabel 5. Contoh Kasus Isi Dokumen yang telah Diganti

Isi Dokumen yang diganti (teks yang diubah diberi warna merah)	
Nama Pasien: Ahmad Kasim Umur: 32 tahun Tanggal dan waktu: 22 Mei 2023, 11:07 Keluhan: sesak nafas Riwayat penyakit: penyakit jantung Hasil pemeriksaan fisik dan penunjang medik Diagnosis: sesak nafas, lemas Pengobatan dan/atau tindakan: Pemberian oksigen Pelayanan lain yang diberikan kepada pasien: -	
Hasil pesan ringkas dari hash isi dokumen	f6e5d96fa5664f89ae8e0bc8c1f6bfe54a4d85558a7caf4ab8c197cbfdea9cbe
Hasil dekripsi tanda tangan digital dengan kunci publik	31e1dfcf3db25ae4712e0ff531f2ae13053deec5d1396e7066ee58c71b393ff4

IV. KESIMPULAN

Implementasi beberapa konsep kriptografi seperti konsep cipher simetri, konsep tanda tangan digital, dan konsep penyimpanan *blockchain* terhadap penyimpanan dokumen rekam medis pasien dapat diintegrasikan dengan baik. Dengan

adanya bantuan kriptografi, informasi yang terdapat pada isi dokumen rekam medis dapat lebih terjaga dibandingkan dengan sistem penyimpanan berbasis kertas. Selain itu, konsep kriptografi juga membantu mengidentifikasi keaslian isi dokumen serta autentikasi pembuat dokumen.

Dengan disimpan menggunakan konsep *blockchain*, dokumen-dokumen rekam medis setiap pasien dapat disimpan secara berurutan secara historis. Konsep *blockchain* dapat memastikan kelengkapan dan keterurutan dari rekam medis masing-masing pasien dapat terjaga dengan baik.

Referensi

[1] https://informatika.stei.itb.ac.id/~rinaldi.munir/Kriptografi/2022-2023/15-Beberapa-block-cipher-bagian1-2023.pdf, diakses pada 18 Mei 2023.

[2] Kriptografi Kunci-Publik, diakses pada 18 Mei 2023.

[3] https://informatika.stei.itb.ac.id/~rinaldi.munir/Kriptografi/2022-2023/27-SHA-3-2023.pdf, diakses pada 18 Mei 2023.

[4] https://informatika.stei.itb.ac.id/~rinaldi.munir/Kriptografi/2022-2023/28-Tanda-tangan-digital-2023.pdf, diakses pada 18 Mei 2023.

[5] https://informatika.stei.itb.ac.id/~rinaldi.munir/Kriptografi/2022-2023/40-Penggunaan-kriptografi-di-dalam-blockchain.pdf, diakses pada 18 Mei 2023.

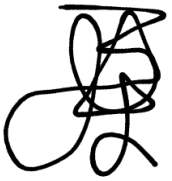
[6] Contoh Rekam Medis Pasien dan yang Harus Ada di Dalamnya, diakses pada 18 Mei 2023.

[7] Rekam Medik Rawat Jalan Puskesmas | PDF, diakses pada 18 Mei 2023.

Pernyataan

Dengan ini saya menyatakan bahwa makalah yang saya tulis ini adalah tulisan saya sendiri, bukan saduran, atau terjemahan dari makalah orang lain, dan bukan plagiasi.

Bandung, 18 Mei 2023



Nicholas Chen

13519029