# Implementasi Tanda Tangan Digital pada Laporan Hasil *Medical Check Up*

Yudi Alfayat - 13519051
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jalan Ganesha 10 Bandung
E-mail : 13519051@std.stei.itb.ac.id

***Abstract*—Penerapan laporan *medical check up* elektronik menjadi kebutuhan di Indonesia guna meningkatkan kualitas pelayanan kesehatan, efisiensi biaya, dan berperan penting dalam keamanan pelayanan medis pasien. Dalam laporan *medical check up* dibutuhkan tanda tangan digital sebagai alat untuk autentikasi dan verifikasi atas identitas penandatangan, keutuhan serta keotentikan informasi elektronik. Pada makalah ini akan dibahas implementasi tanda tangan digital pada laporan hasil *medical check up* dengan menggunakan kriptografi kunci publik RSA dan SHA-256.**

***Keywords—Medical Check Up*, Tanda Tangan digital, *Algoritma RSA, Fungsi Hash, SHA-256***

## I. PENDAHULUAN

Laporan *medical check up* Elektronik merupakan suatu sistem informasi kesehatan terkomputerisasi yang berisi laporan pemeriksaan kesehatan secara menyeluruh berupa pemeriksaan laboratorium, fisik, dan penunjang yang dibutuhkan guna mengetahui kondisi kesehatan seseorang dan dapat dilengkapi dengan sistem pendukung keputusan. Upaya dalam meningkatkan kualitas pelayanan, kepuasan pasien, akurasi pendokumentasian, dan pengurangan *clinical error*s, bisa diwujudkan dengan penggunaan laporan *medical check up* elektronik.

Penerapan laporan *medical check up* elektronik yang terintegrasi menjadi kebutuhan di Indonesia guna meningkatkan kualitas pelayanan kesehatan, efisiensi biaya, serta memiliki peran penting dalam keamanan pelayanan medis pasien. Setiap pencatatan laporan *medical check up* elektronik harus dibubuhi nama, waktu dan tanda tangan dokter, dokter gigi atau tenaga kesehatan tertentu yang memberikan pelayanan kesehatan. Tanda tangan merupakan suatu kebiasaan formil untuk menyatakan persetujuan seseorang dan memastikan identitas (*authentication*) orang tersebut bertanda tangan. Dalam transaksi elektronik, penggunaan tanda tangan digital berguna sebagai alat untuk autentikasi dan verifikasi atas identitas penandatangan dan keutuhan dan keotentikan informasi elektronik. Salah satu contoh pemanfaatan tanda tangan digital adalah untuk legalisasi dokumen elektronik seperti laporan *medical check up* elektronik.

Dengan demikian, makalah ini membahas terkait implementasi tanda tangan digital sebagai salah satu metode untuk meningkatkan keamanan pada laporan hasil *medical check up*. Penggunaan tanda tangan digital ini bertujuan agar setiap laporan *medical check up* terjamin autentik dan tidak bisa diduplikasi sesuai dengan prinsip dari tanda tangan digital.

## II. DASAR TEORI

### A. *Medical Check Up*

M*edical check up* adalah tindakan bersifat rutin yang dilakukan mencakup didalamnya pemeriksaan untuk layanan pencegahan klinis, hal ini adalah proses dari pemeriksaan kesehatan secara rutin. *Medical check up* terdiri dari serangkaian wawancara dan pemeriksaan kesehatan. Lingkup pemeriksaan kesehatan dalam *medical check up* bervariasi, tergantung keperluan dan permintaanya. Contoh pemeriksaan *medical check up* yaitu foto *thorax* (pemeriksaan jantung), cek laboratorium dan *scanning*.

### B. Tanda tangan Digital

Tanda tangan digital merupakan tanda tangan yang terdiri dari informasi yang dilekatkan, terasosiasi ataupun terkait dengan informasi elektronik lainnya yang digunakan sebagai alat verifikasi dan autentikasi. Tujuan tanda tangan digital yaitu memastikan otensitas dari sebuah dokumen, menerima atau menyetujui secara menyakinkan isi dari sebuat tulisan.

Tanda tangan digital bersifat autentik, aman, interoperabilitas dari perangkat lunak maupun jaringan dari penyedia jasa, dan konfidensialitas. Dalam menandatangani pesan, terdapat dua metode yang dapat dilakukan yaitu dengan cara mengenkripsi pesan dan menggunakan kombinasi fungsi hash dan kriptografi kunci publik.

### C. Algoritma Kunci Publik RSA

RSA adalah algoritma kunci-publik yang paling terkenal dan paling banyak aplikasinya. Algoritma RSA merupakan algoritma yang ditemukan tiga peneliti MIT yaitu Adi Shamir, Ronald Rivest, dan Len Adleman di tahun 1976. Keamanan algoritma RSA terletak pada sulitnya memfaktorkan bilangan bulat yang besar menjadi faktor prima. Pada Algoritma RSA terdapat persamaan enkripsi seperti ditunjukan pada persamaan (2) dan persamaan dekripsi seperti ditunjukkan pada persamaan (3).

Enkripsi: $E_e(m) = c = m^e \bmod n$ (2)

Dekripsi : $D_d(c) = m = c^d \bmod n$ (3)

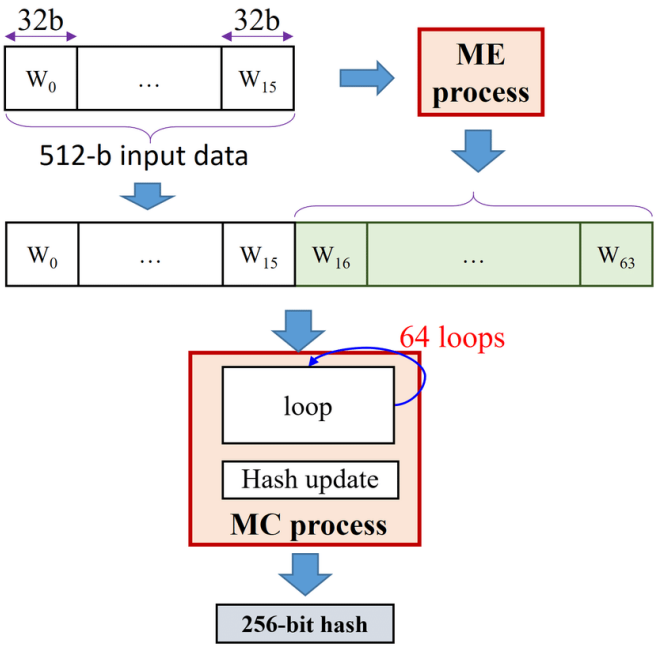
Pada makalah ini, algoritma RSA digunakan untuk melakukan enkripsi nilai hash dari dokumen laporan *Medical Check Up* untuk kemudian menjadi tanda tangan digital.

D. Fungsi Hash SHA-256

*Secure Hash Algorithm* 2 (SHA-2) adalah sebuah himpunan dari fungsi hash yang dirancang oleh United States National Security Agency (NSA) pada tahun 2001. Fungsi SHA-2 banyak digunakan untuk aplikasi dan protokol keamanan, seperti TLS dan SSL, PGP, SSH, S/MIME dan IPsec. SHA-2 terdiri dari SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/224, SHA-512/256. Umumnya, algoritma SHA-256 yaitu sebagai berikut,

1. L : panjang pesan
2. Inisialisasi hash values (h) berisi 32 bit pertama dari pecahan akar dari 8 prima pertama (2…19)
3. Inisialisasi array berisi konstanta bilangan bulat yang berisi 32 bit pertama dari pecahan akar kubik dari 64 prima pertama (2…311)
4. Melakukan padding dengan menambahkan satu ‘1’ bit.
5. Melakukan padding dengan menambahkan ‘0’ bit sebanyak K dimana K merupakan angka minimum >=0 yang memenuhi L + 1 + K + 64 % 512 = 0
6. Melakukan padding dengan menambahkan L sebagai 64-bit big-endian dimana total pesan yang telah ditambahkan padding menjadi kelipatan 512.
7. Membagi pesan yang telah di-padding menjadi blok berukuran 512
8. Untuk setiap blok, melakukan right rotate dan right shift untuk setiap karakter . Selanjutnya melakukan compression secara looping
9. Nilai yang sudah terkompresi kemudian akan dimodifikasi menjadi 32 bit untuk setiap nilai h dari h0 sampai h7 untuk menghasilkan hash value yang final.

Pada makalah ini, algoritma SHA-256 untuk melakukan hashing terhadap dokumen laporan *Medical Check Up* untuk kemudian dijadikan tanda tangan digital.




Gambar II.1. Gambaran umum algoritma SHA-256

## III. RANCANGAN SOLUSI DAN IMPLEMENTASI

Dalam menyelesaikan permasalahan, dilakukan beberapa langkah yaitu Rancangan, dan Implementasi Solusi

A. Rancangan Solusi

Dalam menyelesaikan permasalahan kecurangan dalam bentuk pemalsuan dokumen laporan *medical check u*p, pada makalah ini akan digunakan perpaduan antara algoritma hashing SHA-256 dan kriptografi kunci publik RSA untuk menjaga kebenaran dari dokumen. Dengan menggunakan tanda tangan digital, dapat dicapai aspek-aspek keamanan seperti otentik, asli, dan anti-penyangkalan pada dokumen *medical check up*.

Terdapat tiga tahap utama dalam proses tanda tangan digital pada laporan medical check up ini,

1. Tahap *Key Generation*

Pada tahap ini akan dibentuk pasangan kunci yaitu private dan public key yang akan digunakan untuk meng-enkripsi nilai hash dari dokumen *medical check up*. Pasangan kunci akan dimiliki oleh dokter atau pihak rumah sakit yang melakukan pemeriksaan terhadap pasien. *Private key* akan dirahasiakan atau hanya dapat diketahui oleh pemilik tersebut. Sedangkan *public key* dapat diketahui oleh siapa pun atau *public*.

2. Tahap Penandatangani Dokumen

Pada tahap ini akan dilakukan penandatangan terhadap dokumen laporan medical check up. Nilai hash dari dokumen akan dihitung dengan menggunakan algoritma SHA-256. Nilai hash dari dokumen akan sama dengan nilai hash dokumen yang diberikan ke pasien jika tidak ada dilakukan perubahan terhadap dokumen. Nilai hash ini akan dienkripsi dengan menggunakan algoritma RSA dan *private key* yang sudah dibentuk pada tahap pertama. Enkripsi ini akan menghasilkan

sebuah digital signature yang akan di-*embed* ke dalam dokumen laporan pada halaman yang dapat dipisahkan dengan konten asli laporan.

3. Tahap Verifikasi

Pada tahap ini akan dilakukan verifikasi terhadap dokumen laporan *medical check up* untuk mengetahui keaslian dari dokumen tersebut. Tanda tangan digital yang di-embed di dalam dokumen akan dipisahkan dengan konten utama. Tanda tangan digital akan di-dekripsi kembali menjadi nilai hash dari dokumen original dengan menggunakan algoritma RSA dan public key yang sudah dibentuk pada tahap pertama. Lalu nilai hash ini akan dibandingkan dengan nilai konten utama. Jika nilai dari tanda tangan digital dan konten dokumen sama maka dokumen masih sama dengan dokumen original. Sedangkan jika terdapat perbedaan maka dapat dipastikan bahwa sudah dilakukan modifikasi terhadap dokumen.

B. Implementasi

Implementasi tanda tangan digital pada makalah ini menggunakan bahasa pemrograman *JavaScript* dengan *crypto* dan *pdf library*.

```
const arguments = process.argv.slice(2);
if (arguments.length === 0) {
 console.log('Commands:');
 console.log('1. generate-key');
 console.log('2. sign <pdf-filename>');
 console.log('3. verify <pdf-filename>');
 console.log();
 console.log('ex: node index.js sign
surat1.pdf');
 return;
}

const cmd = arguments[0];

if (cmd === 'generate-key') {
 generateKey();
 return;
}

if (cmd === 'sign') {
 const filename = arguments[1];
 if (!filename) {
   console.log('Please input pdf file name');
   return;
 }
 sign(filename);
}

if (cmd === 'verify') {
 const filename = arguments[1];
 if (!filename) {
   console.log('Please input pdf file name');
   return;
 }
 verify(filename);
}
```

Berdasarkan rancangan solusi yang sudah dibuat, terhadap tiga bagian utama dalam program yang dibuat yaitu *key generation, signing, dan verifying*. User dapat memilih aksi yang ingin dilakukan.

```
const generateKey = () => {
 // Generate RSA key pair
 const { privateKey, publicKey } =
crypto.generateKeyPairSync('rsa', {
   modulusLength: 2048,
 });

 // Convert keys to PEM format
 const privateKeyPem = privateKey.export({ type:
'pkcs1', format: 'pem' });
 const publicKeyPem = publicKey.export({ type:
'pkcs1', format: 'pem' });

 // Save keys to files
 fs.writeFileSync('private_key.pem',
privateKeyPem);
 fs.writeFileSync('public_key.pem',
publicKeyPem);

 console.log('Private and public keys saved to
private_key.pem & public_key.pem');
};
```

Pada tahap *key generation*, pasangan kunci dibuat dengan menggunakan *library crypto* yang sudah disediakan oleh *node-js*. Setelah itu, pasangan kunci akan dikonversi ke format PEM (Privacy Enhanced Mail) dan disimpan ke dalam file yang bernama private_key.pem dan public_key.pem.

```
const sign = async (filename) => {
 // hash
 const data = await getPdfText(filename);
 const hash = crypto.createHash('sha256');
 hash.update(data);
```

```
 const hashDigest = hash.digest('base64');

 console.log('Digest:', hashDigest);
 console.log();

 // Encrypt
 const privateKey =
fs.readFileSync('private_key.pem', 'utf8');
 const buff = Buffer.from(hashDigest, 'base64');
 const encrypted =
crypto.privateEncrypt(privateKey, buff);
 const encryptedBase64 =
encrypted.toString('base64');
 console.log('Encrypted Digest:',
encryptedBase64);
 console.log();

 // Embed
 await writeToPdf(filename, encryptedBase64);
 console.log(`Success!! Please check
signed_${filename}`);
};
```

Tahap selanjutnya merupakan proses memberikan tanda tangan digital pada dokumen. Terdapat tiga proses utama dalam tahap ini. Pertama yaitu menghitung nilai hash dari dokumen laporan medical check up. Setelah itu akan dienkripsi pada nilai hash dengan menggunakan algoritma RSA dan *private key* yang sudah dibuat. Enkripsi ini menggunakan bantuan *library crypto* dari node-js. proses terakhir yaitu memasang tanda tangan hasil enkripsi ke dokumen laporan.

```
const verify = async (filename) => {
 const ds = await readDs(filename);
 if (ds === '') {
   console.log('Digital signature is not found
in the document');
   console.log('=== DOCUMENT IS NOT VALID ===');
   return;
 }
 console.log('Get Digital Signature:', ds);
 console.log();

 const digestFromDs = decryptDs(ds);

 // Load the PDF document
 const pdfBytes = fs.readFileSync(filename);
 const pdfDoc = await
PDFDocument.load(pdfBytes);

 // Get the total number of pages in the
document
 const pageCount = pdfDoc.getPageCount();

 // Remove the last page
 pdfDoc.removePage(pageCount - 1);

 // Serialize the modified PDF document
 const modifiedPdfBytes = await pdfDoc.save();

 const PDFParser = require('pdf-parse');
 const pdf = await PDFParser(modifiedPdfBytes);
 const data = pdf.text;
 const hash = crypto.createHash('sha256');
 hash.update(data);
 const hashDigest = hash.digest('base64');

 console.log();
 if (hashDigest === digestFromDs) {
   console.log('=== DOCUMENT IS VALID ===');
 } else {
   console.log('=== DOCUMENT IS NOT VALID ===');
 }
 console.log();
};
```

Tahap terakhir yaitu verifikasi. Terdapat beberapa proses dalam melakukan verifikasi dokumen. Pertama, membaca tanda tangan digital yang di-embed ke dokumen laporan. Lalu tanda tangan ini akan didekripsi dengan menggunakan kunci publik untuk mendapatkan nilai hash dari dokumen. Lalu konten utama dari laporan akan dihitung nilai hashnya dan dibandingkan dengan nilai hash yang didapat dari tanda tangan digital.

## IV. PENGUJIAN DAN PEMBAHASAN

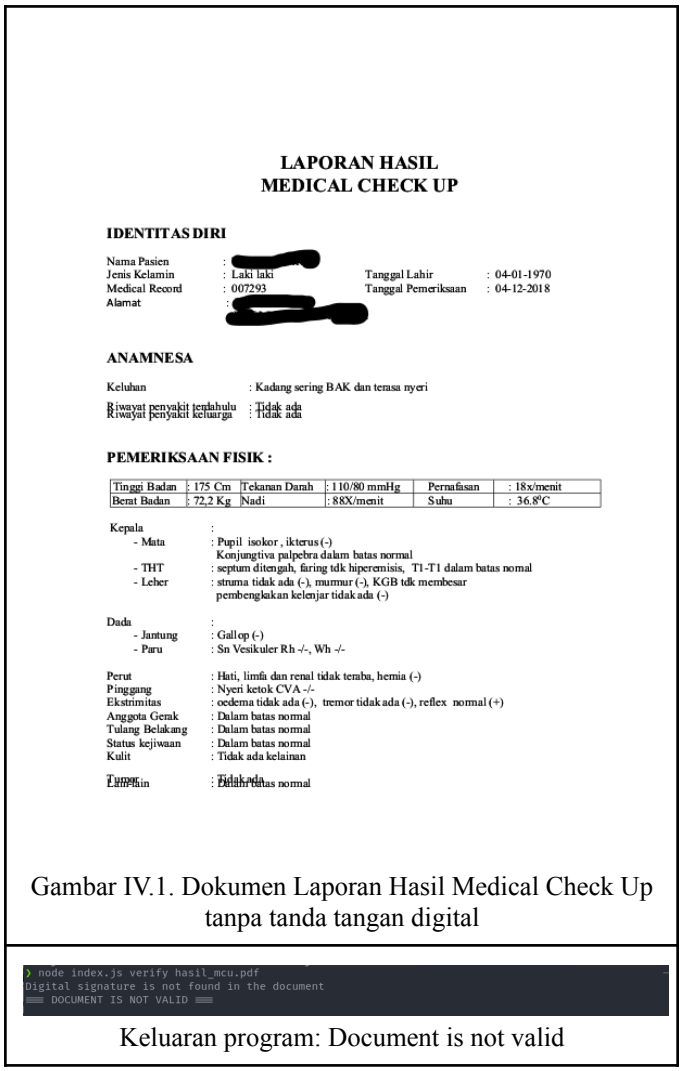
Setelah dilakukan implementasi akan dilakukan tahap pengujian dan pembahasan dari implementasi.

### A. Pengujian

Pengujian akan dilakukan dengan menggunakan tiga skema yaitu pengecekan dokumen laporan yang tidak diberi tanda tangan digital, pengecekan dokumen laporan yang diberi tanda tangan digital dan tidak dilakukan modifikasi terhadap dokumen, dan pengecheckan dokumen laporan yang diberi tanda tangan digital tapi dilakukan modifikasi terhadap dokumen.

1. Pengujian dokumen tanpa tanda tangan digital

Pada pengujian ini, dokumen laporan hasil *medical check up* tidak diberi tanda tangan digital seperti yang dilihat pada gambar IV.1.



**LAPORAN HASIL**
**MEDICAL CHECK UP**

**IDENTITAS DIRI**

Nama Pasien : [redacted]
Jenis Kelamin : Laki laki
Medical Record : 007293
Alamat : [redacted]
Tanggal Lahir : 04-01-1970
Tanggal Pemeriksaan : 04-12-2018

**ANAMNESA**

Keluhan : Kadang sering BAK dan terasa nyeri
Riwayat penyakit terdahulu : Tidak ada
Riwayat penyakit keluarga : Tidak ada

**PEMERIKSAAN FISIK :**

| | | | | | |
|---|---|---|---|---|---|
| Tinggi Badan | : 175 Cm | Tekanan Darah | : 110/80 mmHg | Pernafasan | : 18x/menit |
| Berat Badan | : 72,2 Kg | Nadi | : 88X/menit | Suhu | : 36.8°C |

Kepala :
- Mata : Pupil isokor , ikterus (-)
  Konjungtiva palpebra dalam batas normal
- THT : septum ditengah, faring tdk hiperemisis, T1-T1 dalam batas normal
- Leher : struma tidak ada (-), murmur (-), KGB tdk membesar
  pembenglakan kelenjar tidak ada (-)

Dada :
- Jantung : Gallop (-)
- Paru : Sn Vesikuler Rh -/-, Wh -/-

Perut : Hati, limfa dan renal tidak teraba, hemia (-)
Pinggang : Nyeri ketok CVA -/-
Ekstrimitas : oedema tidak ada (-), tremor tidak ada (-), reflex normal (+)
Anggota Gerak : Dalam batas normal
Tulang Belakang : Dalam batas normal
Status kejiwaan : Dalam batas normal
Kulit : Tidak ada kelainan
Tumor : Tidak ada
Lain-lain : Dalam batas normal

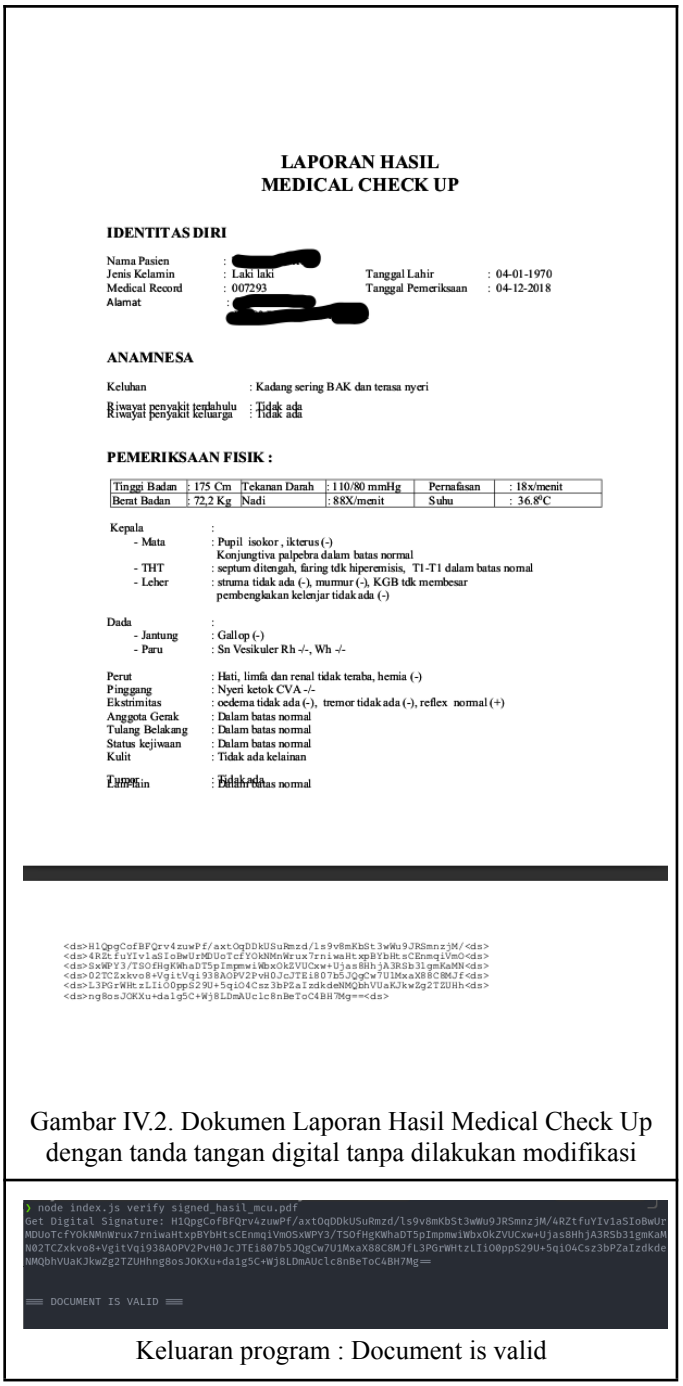
Gambar IV.1. Dokumen Laporan Hasil Medical Check Up tanpa tanda tangan digital




Keluaran program: Document is not valid

2. Pengujian dokumen laporan dengan menggunakan tanda tangan digital dan tidak dimodifikasi

Tanda tangan digital disisipkan pada bagian akhir dokumen yang dapat dilihat pada gambar IV.2.



**LAPORAN HASIL**
**MEDICAL CHECK UP**

**IDENTITAS DIRI**

Nama Pasien : [redacted]
Jenis Kelamin : Laki laki
Medical Record : 007293
Alamat : [redacted]
Tanggal Lahir : 04-01-1970
Tanggal Pemeriksaan : 04-12-2018

**ANAMNESA**

Keluhan : Kadang sering BAK dan terasa nyeri
Riwayat penyakit terdahulu : Tidak ada
Riwayat penyakit keluarga : Tidak ada

**PEMERIKSAAN FISIK :**

| | | | | | |
|---|---|---|---|---|---|
| Tinggi Badan | : 175 Cm | Tekanan Darah | : 110/80 mmHg | Pernafasan | : 18x/menit |
| Berat Badan | : 72,2 Kg | Nadi | : 88X/menit | Suhu | : 36.8°C |

Kepala :
- Mata : Pupil isokor , ikterus (-)
  Konjungtiva palpebra dalam batas normal
- THT : septum ditengah, faring tdk hiperemisis, T1-T1 dalam batas normal
- Leher : struma tidak ada (-), murmur (-), KGB tdk membesar
  pembenglakan kelenjar tidak ada (-)

Dada :
- Jantung : Gallop (-)
- Paru : Sn Vesikuler Rh -/-, Wh -/-

Perut : Hati, limfa dan renal tidak teraba, hemia (-)
Pinggang : Nyeri ketok CVA -/-
Ekstrimitas : oedema tidak ada (-), tremor tidak ada (-), reflex normal (+)
Anggota Gerak : Dalam batas normal
Tulang Belakang : Dalam batas normal
Status kejiwaan : Dalam batas normal
Kulit : Tidak ada kelainan
Tumor : Tidak ada
Lain-lain : Dalam batas normal


<ds>H1QpgCofBFQrv4zuwPf/axtOqDDkUSuRmzd/1s9v8mKbSt3wWu9JRSmnzjM/</ds>
<ds>4RZtfuYIv1aSIoBwUrMDUoTcfYOkNMnWrux7rniwaHtxpBYbHtsCEnmqiVmO</ds>
<ds>SxWPY3/TSOfHgKWhaDT5pImpmwiWbxOkZVUCxw+Ujas8HhjA3RSb3lgmKaMN</ds>
<ds>02TCZxkvo8+VgitVqi938AOPV2PvH0JcJTEi807b5JQgCw7U1MxaX88C8MJf</ds>
<ds>L3PGrWHtzLIi0OppS29U+5qiO4Csz3bPZaIzdkdeNMQbhVUaKJkwZg2TZUHh</ds>
<ds>ng8osJOKXu+da1g5C+Wj8LDmAUclc8nBeToC4BH7Mg==</ds>

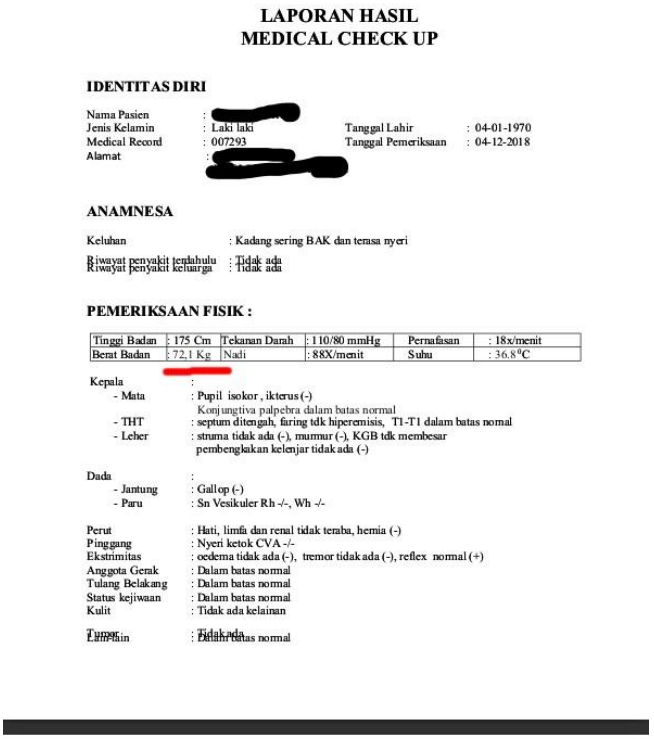

Gambar IV.2. Dokumen Laporan Hasil Medical Check Up dengan tanda tangan digital tanpa dilakukan modifikasi




Keluaran program : Document is valid

3. Pengujian dokumen laporan dengan menggunakan tanda tangan digital dan dilakukan modifikasi pada dokumen

Tanda tangan digital disisipkan pada bagian akhir dokumen. Lalu dilakukan modifikasi pada dokumen yaitu dengan mengganti berat badan dari 72.2 kg menjadi 72.1 kg seperti yang dapat dilihat pada gambar IV.3.



**LAPORAN HASIL**
**MEDICAL CHECK UP**

**IDENTITAS DIRI**

Nama Pasien : [redacted]
Jenis Kelamin : Laki laki — Tanggal Lahir : 04-01-1970
Medical Record : 007293 — Tanggal Pemeriksaan : 04-12-2018
Alamat : [redacted]

**ANAMNESA**

Keluhan : Kadang sering BAK dan terasa nyeri
Riwayat penyakit terdahulu : Tidak ada
Riwayat penyakit keluarga : Tidak ada

**PEMERIKSAAN FISIK :**

| | | | | | |
|---|---|---|---|---|---|
| Tinggi Badan | : 175 Cm | Tekanan Darah | : 110/80 mmHg | Pernafasan | : 18x/menit |
| Berat Badan | : 72,1 Kg | Nadi | : 88X/menit | Suhu | : 36.8°C |

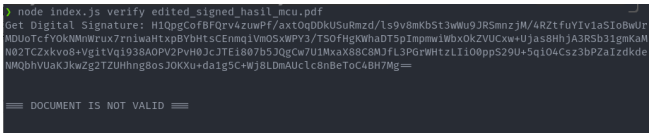
Kepala :
- Mata : Pupil isokor , ikterus (-)
  Konjungtiva palpebra dalam batas normal
- THT : septum ditengah, faring tdk hiperemisis, T1-T1 dalam batas normal
- Leher : struma tidak ada (-), murmur (-), KGB tdk membesar
  pembengkakan kelenjar tidak ada (-)

Dada :
- Jantung : Gallop (-)
- Paru : Sn Vesikuler Rh -/-, Wh -/-

Perut : Hati, limfa dan renal tidak teraba, hernia (-)
Pinggang : Nyeri ketok CVA -/-
Ekstremitas : oedema tidak ada (-), tremor tidak ada (-), reflex normal (+)
Anggota Gerak : Dalam batas normal
Tulang Belakang : Dalam batas normal
Status kejiwaan : Dalam batas normal
Kulit : Tidak ada kelainan
Tumor : Tidak ada
Lain-lain : Dalam batas normal


<ds>H1QpgCofBFQrv4zuwPf/axtOqDDkUSuRmzd/ls9v8mKbSt3wWu9JRSmnzjM/<ds>
<ds>4RZtfuYIv1aSIoBwUrMOUoTcfYOkNMnWrux7rniwaHtxpBYbHtsCEnmqiVmO<ds>
<ds>SxWPY3/TSOfHgKWhaDT5pImpmwiWbxOkZVUCxw+UjasBHhjA3R5b31gmKaMN<ds>
<ds>D2TC2xkvo8+VgitVqi93BAOPV2PvH0JcJTE1807b5JQgCw7U1MxaX8SC8MJfL3PGrWHtzLIiO0ppS29U+5qiO4Csz3bPZaIzdkdeNMQbhVUaKJkwZg2TZUHhng8osJOKXu+da1g5C+Wj8LDmAUclc8nBeToC4BH7Mg==<ds>


Gambar IV.3. Dokumen Laporan Medical Check Up dengan tanda digital dan dimodifikasi




Keluaran Program : Document is not valid

B. Pembahasan

Berdasarkan pengujian yang telah dilakukan, didapatkan hasil sebagai berikut,

1. Pengujian dokumen laporan tanpa tanda tangan digital

Dokumen laporan *medical check up* yang tidak memiliki tanda tangan digital akan dianggap sebagai dokumen yang tidak valid secara otomatis oleh program.

2. Pengujian dokumen laporan dengan menggunakan tanda tangan digital dan tidak dilakukan modifikasi

Tanda tangan digital disisipkan pada bagian akhir dokumen. Program akan memisahkan tanda tangan dan konten dari laporan. Setelah melakukan pengecekan, program menghasilkan keluaran dokumen adalah valid. Hal ini karena nilai hash yang didapat dari dokumen laporan sama dengan nilai hash yang berada di tanda tangan digital.

3. Pengujian dokumen laporan dengan menggunakan tanda tangan digital dan dilakukan modifikasi pada dokumen

Sama seperti pengujian sebelumnya, tanda tangan disisipkan pada bagian akhir dokumen. Lalu dilakukan modifikasi pada bagian berat badan dari 72.2 kg menjadi 72.1 kg. Program menghasilkan keluaran bahwa dokumen sudah tidak valid atau sudah dilakukan modifikasi. Nilai hash yang didapatkan dari dokumen tidak sama dengan nilai hash yang berada di tanda tangan digital.

## V. KESIMPULAN DAN SARAN PENGEMBANGAN

Solusi yang diimplementasikan berhasil untuk menjaga keaslian dan keotentikan dari laporan *medical check up*. Hal ini memfasilitasi pihak penerima laporan *medical check up* untuk memverifikasi keaslian dan keotentikan laporan tanpa melakukan pengecekan langsung kepada pihak pemberi baik dokter, dokter gigi, ataupun tenaga medis pemberi laporan *medical check up* tersebut.

Kedepannya, solusi dapat dikembangkan lebih lanjut pada beberapa bagian, seperti penempatan tanda tangan digital berada pada halaman dari dokumen laporan.


## UCAPAN TERIMA KASIH

Ucapan terima kasih penulis berikan kepada Tuhan Yang Maha Esa, atas karunia-Nya penulis dapat menyelesaikan dan memberikan kontribusi nyata untuk memberikan ide yang dituangkan pada makalah ini. Penulis juga mengucapkan banyak terima kasih kepada Dr. Rinaldi Munir atas dedikasinya dalam memberikan ilmu pengetahuan terkait mata kuliah kriptografi kepada penulis.


## REFERENSI


[1] Munir, Rinaldi. 2023. Slide Kuliah IF4020 Kriptografi: Fungsi hash

[2] Munir, Rinaldi. 2023. Slide Kuliah IF4020 Kriptografi: Fungsi hash SHA-1

[3] Munir, Rinaldi. 2023. Slide Kuliah IF4020 Kriptografi: Algoritma RSA

[4] Munir, Rinaldi. 2023. Slide Kuliah IF4020 Kriptografi: Tanda tangan digital (digital signature)

[5] Gunawan, Indra, dkk. (2020). Perancangan Sistem Informasi Medical Check Up Guna Mempercepat Pelayanan MCU di RSUD Brebes


## 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, 22 Mei 2023

Yudi Alfayat
13519051