# Penerapan Enkripsi dan Tanda Tangan Digital untuk Keamanan dan Integritas Citra Medis

Eiffel Aqila Amarendra - 13520074
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jalan Ganesha 10 Bandung
E-mail: 13520074@std.stei.itb.ac.id

***Abstract*—Dalam dunia medis modern, citra digital medis merupakan aspek yang tidak dapat terpisahkan. Pada citra tersebut, tersimpan informasi sensitif mengenai kondisi kesehatan dan struktur internal dari tubuh pasien yang esensial pada proses medis. Oleh karena itu, keamanan dan integritas medis menjadi prioritas utama dalam sistem medis. Makalah ini akan membahas mengenai penerapan enkripsi dan tanda tangan digital pada citra medis untuk menjaga keamanan dan integritas citra tersebut. Dalam implementasinya, digunakan algoritma enkripsi *hybrid* yang mengombinasikan algoritma AES dan RSA serta algoritma ECDSA yang menggunakan kurva SECP256k1 dan fungsi *hash* SHA256. Berdasarkan hasil pengujian, terbukti bahwa program berhasil melakukan pengenkripsian dan pendekripsian citra medis tanpa menurunkan akurasi dari citra hasil dekripsi. Selain itu, program juga berhasil melakukan penandatanganan digital dan pemvalidasian keaslian citra melalui verifikasi tanda tangan digital.**

***Keywords—citra digital medis; enkripsi data; tanda tangan digital***

## I. PENDAHULUAN

Dalam dunia medis modern, citra digital medis merupakan aspek yang tidak dapat terpisahkan. Citra medis, seperti *magnetic resonance imaging* (MRI) dan *computed tomography* (CT) *scan* menyimpan informasi mengenai kondisi kesehatan dan struktur internal dari tubuh pasien sehingga esensial dalam proses diagnosis, perencanaan pengobatan dan perawatan, serta pemantauan kondisi kesehatan pasien. Namun, data pada citra medis merupakan hal yang bersifat sensitif sehingga membutuhkan perlindungan untuk dijaga keamanan dan integritasnya. Oleh karena itu, keamanan data medis menjadi prioritas utama dalam sistem medis, terutama jika data tersebut dikelola dan didistribusikan melalui jaringan publik.

Pengelolaan dan pengiriman citra medis melalui jaringan digital menghadapi risiko besar terkait keamanan data. Risiko ini mencakup privasi pasien, pengaksesan data secara ilegal, serta potensi manipulasi data sehingga menimbulkan kesalahan diagnosis, pengobatan, dan perawatan. Untuk mengatasi persoalan tersebut, teknik enkripsi serta tanda tangan digital perlu digunakan dalam sistem medis.

Enkripsi merupakan sebuah proses pengonversian data citra medis menjadi format yang tidak dapat dibaca oleh pihak yang tidak berwenang. Dengan memanfaatkan enkripsi data, seperti algoritma RSA dan AES, kerahasiaan data citra dapat dijaga kerahasiaannya sehingga hanya dapat dibaca oleh pihak yang berwenang. Selain enkripsi, tanda tangan digital juga berperan penting dalam memastikan integritas dan otentikasi data citra medis. Adapun algoritma yang mengimplementasikan tanda tangan digital adalah ECDSA. Dengan mengintegrasikan enkripsi dan tanda tangan digital, keamanan dan integritas citra medis dapat semakin terjaga.

Makalah ini akan membahas penerapan enkripsi dan tanda tangan digital pada citra medis untuk menjaga keamanan dan integritas citra tersebut. Selain itu, makalah ini juga membahas konsep dasar mengenai enkripsi data, tanda tangan digital, dan algoritma yang berkorelasi dengan kedua teknik tersebut.

## II. DASAR TEORI

### A. Citra Digital Medis

Citra digital merupakan sebuah representasi diskrit visual dari satu atau beberapa objek yang dapat menyimpan informasi krusial dalam berbagai bidang, salah satunya bidang medis. Citra digital medis merupakan sebuah representasi visual dari struktur internal dari tubuh pasien. Citra ini umumnya dihasilkan melalui teknologi *X-rays*, *computed tomography* (CT), *magnetic resonance imaging* (MRI), dan ultrasonik. Di samping itu, citra ini memiliki peran krusial pada proses medis, antara lain diagnosis, perawatan, dan pengamatan kondisi medis dari seorang pasien. Salah satu contoh dari citra medis ditunjukkan pada Fig 1.

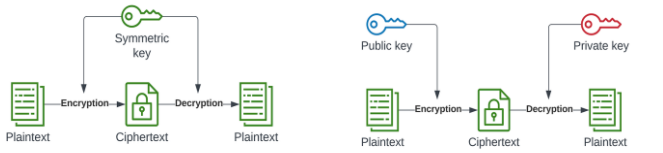
Pengelolaan dan pengiriman citra medis melalui jaringan digital menghadapi risiko besar terkait keamanan data. Risiko ini mencakup privasi pasien, pengaksesan data secara ilegal, serta potensi manipulasi data sehingga menimbulkan kesalahan diagnosis, pengobatan, dan perawatan. Dengan demikian, perlindungan terhadap citra medis merupakan hal yang esensial untuk mempertahankan kerahassiaan, keamanan, dan integritas dari citra tersebut.

Fig. 1. Contoh citra medis (sumber: *Medical Imaging* - Wikipedia)

## B. *Enkripsi Data*

Enkripsi data merupakan sebuah proses pengonversian data mentah menjadi sebuah data *cipher* yang tidak dapat terbaca untuk memberikan perlindungan terhadap data tersebut dari akses ilegal. Proses pengenkripsian data dilakukan dengan menggunakan serangkaian algoritma untuk mengubah data menjadi bentuk yang terenkripsi. Pengenkripsian data umumnya digunakan untuk melindungi informasi rahasia atau sensitif, seperti dokumen rahasia, sandi, dan data sensitif. Enkripsi citra merupakan salah satu cabang dari enkripsi data yang berfokus pada perlindungan data visual, seperti citra, untuk melindungi data tersebut dari pengaksesan dan pengubahan secara ilegal. Hal ini merupakan proses yang esensial dalam berbagai bidang, salah satunya bidang medis yang menyimpan informasi pasien ke dalam sebuah citra.

Pada proses pengenkripsian data, kunci merupakan sebuah komponen nilai rahasia yang digunakan sebagai parameter masukan dalam algoritma enkripsi. Enkripsi memanfaatkan kunci enkripsi untuk mengonversi data menjadi bentuk yang terenkripsi, sedangkan dekripsi memanfaatkan kunci dekripsi untuk mengonversi data yang terenkripsi menjadi bentuk semula. Berdasarkan jenis kuncinya, enkripsi dibagi menjadi dua, yaitu enkripsi simetris dan asimetris.




(a) (b)

Fig. 2. Enkripsi (a) simetris dan (b) asimetris (sumber: *Hybrid Encryption in Python*)

Pada enkripsi simetris, seperti yang ditunjukkan pada Fig 2(a), proses enkripsi dan dekripsi data menggunakan sebuah kunci yang sama. Dengan menggunakan kunci yang sama, teknik ini menjadi lebih cepat dan efisien dibandingkan dengan teknik enkripsi asimetris. Meskipun demikian, algoritma ini menjadi kurang aman karena hanya menggunakan satu buah kunci. Adapun algoritma yang menggunakan enkripsi simetris, antara lain *Data Encryption Standard* (DES) dan *Advanced Encryption Standard* (AES).

Pada enkripsi asimetris, seperti yang ditunjukkan pada Fig 2(b), proses enkripsi dan dekripsi data menggunakan sebuah kunci yang berbeda. Proses enkripsi menggunakan kunci publik, sedangkan proses dekripsi menggunakan kunci privat yang hanya diketahui oleh pemilik kunci privat tersebut. Dengan menggunakan dua buah kunci yang berbeda, teknik ini menjadi lebih aman dibandingkan dengan teknik enkripsi simetris. Meskipun demikian, algoritma ini menjadi cukup lambat. Adapun algoritma yang menggunakan enkripsi simetris, antara lain Diffie-Hellman, ElGamal, dan Rivest-Shamir-Adleman (RSA).

Di samping itu, terdapat teknik enkripsi *hybrid*, yaitu teknik enkripsi yang mengombinasikan teknik enkripsi simetris dengan teknik enkripsi asimetris. Pada teknik ini, data yang terenkripsi dengan kunci simetris dikirimkan bersamaan dengan kunci simetris yang telah dienkripsi dengan kunci publik. Sementara itu, data dapat didekripsi dengan menggunakan kunci simetris yang telah didekripsi terlebih dahulu menggunakan kunci privat. Proses ini dapat dilihat pada Fig 3. Dengan demikian, teknik ini mampu mengombinasikan efisiensi dari proses enkripsi simetris dan keamanan dari proses enkripsi asimetris.

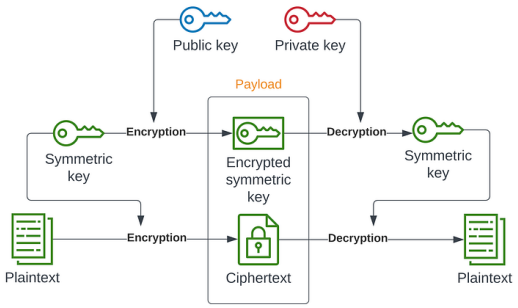



Fig. 3. Enkripsi (a) simetris dan (b) asimetris (sumber: *Hybrid Encryption in Python*)

## C. *Tanda Tangan Digital*

Tanda tangan digital (*digital signature*) merupakan salah satu teknik kriptografi dengan tujuan yang ekivalen dengan tanda tangan yang ditulis tangan, yaitu untuk memvalidasi keotentikan dan integritas dari sebuah data, pesan, atau dokumen digital. Teknik ini digunakan untuk memastikan bahwa pengirim pesan sesuai dengan klaim serta pesan belum mengalami pengubahan selama pentransmisiannya. Selain itu, dengan menggunakan tanda tangan digital, aspek *authentication* dan *nonrepudiation* pada layanan keamanan kriptografi dapat dipenuhi.

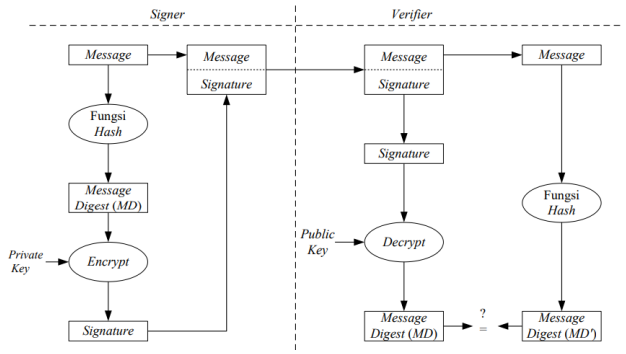



Fig. 4. Proses *Digital Signature* (sumber: Slide Perkuliahan)

Proses tanda tangan digital dapat dibagi menjadi dua buah proses, yaitu *signing* atau penandatangan pesan serta *verification* atau pemverifikasian pesan yang telah dibubuhi tanda tangan digital. Terdapat beberapa teknik tanda tangan digital, seperti penandatanganan dengan cara mengenkripsi pesan dengan kunci simetris, mengenkripsi pesan dengan kunci asimetris, dan mengombinasikan kunci asimetris dan fungsi *hash*, seperti yang ditunjukkan pada Fig 4. Dengan mengombinasikan kunci asimetris dan fungsi *hash*, tanda tangan digital mampu memenuhi pula aspek *integrity* pada layanan keamanan kriptografi. Adapun algoritma tanda tangan

digital yang umum digunakan, antara lain *Digital Signature Algorithm* (DSA) dan *Elliptic Curve Digital Signature Algorithm* (ECDSA).

### *D. Algoritma Advanced Encryption Standard (AES)*

Algoritma enkripsi *Advanced Encryption Standard* (AES) merupakan algoritma enkripsi blok yang dirancang untuk menggantikan *Data Encryption Standard* (DES). Pada algoritma AES, pengenkripsian data dilakukan dalam blok-blok berukuran 128 bit dengan kunci yang memiliki panjang 128, 192, atau 256 bit. Proses enkripsi dan dekripsi dalam AES melibatkan serangkaian operasi meliputi operasi *AddRoundKey* pada putaran awal, operasi *SubBytes*, *ShiftRows*, *MixColumns*, dan *AddRoundKey* pada beberapa putaran sebanyak $N_r - 1$, dan *SubBytes*, *ShiftRows*, dan *AddRoundKey* untuk putaran terakhir, seperti yang ditunjukkan pada Fig 5. Melalui serangkaian operasi ini, data dapat dipastikan terlindungi secara menyeluruh dari berbagai jenis serangan kriptografi.

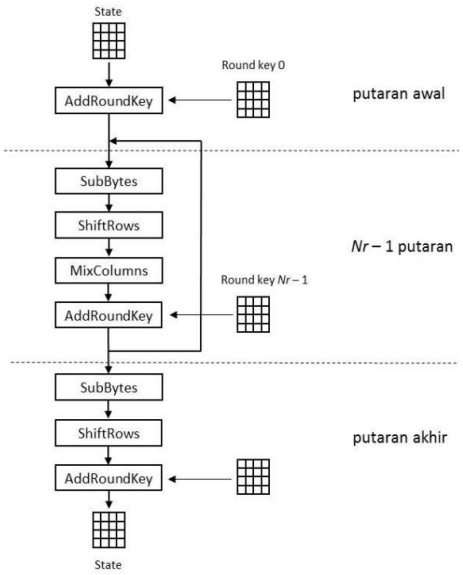



Fig. 5. Algoritma *AES* (sumber: Slide Perkuliahan)

### *E. Algoritma Rivest-Shamir-Adleman (RSA)*

*Rivest-Shamir-Adleman* (RSA) merupakan algoritma asimetris yang didasarkan pada prinsip-prinsip teori bilangan, seperti pemfaktoran bilangan besar. Algoritma ini menggunakaan sepasang kunci, yaitu kunci publik untuk mengenkripsi data *plaintext* menjadi *ciphertext* dan kunci privat untuk mendekripsi data *ciphertext* menjadi *plaintext*. RSA. Data yang dienkripsi oleh kunci publik hanya dapat didekripsi dengan kunci privat yang sesuai sehingga hanya pihak yang memiliki kunci privat tersebut yang mampu mengakses informasi rahasia tersebut.

Dalam konteks keamanan data, RSA digunakan untuk memastikan kerahasiaan dan otentikasi sebuah data. RSA menawarkan tingkat keamanan yang sangat kuat karena memanfaatkan kompleksitas faktorisasi bilangan besar sehingga membutuhkan waktu yang sangat lama untuk memecahkan hasil pengenkripsian RSA. Meskipun RSA sangat aman, proses enkripsi dan dekripsinya cenderung lebih lambat dibandingkan dengan algoritma enkripsi simetris, seperti AES. Dengan demikian, pengombinasian RSA dengan algoritma enkripsi simetris menjadi pilihan yang baik untuk mempercepat waktu enkripsi dan dekripsi tanpa mengurangi keamanan dari data tersebut.

### *F. Elliptic Curve Digital Signature Algorithm (ECDSA)*

*Elliptic curve digital signature algorithm* (ECDSA) merupakan algoritma tanda tangan digital yang mengombinasikan *elliptic curve cryptography* (ECC) dan *Digital Signature Algorithm* (DSA). Penggunaan ECC pada algoritma ini memberikan peluan keamanan tinggi dengan ukuran kunci yang lebih kecil dibandingkan dengan algoritma RSA. Proses pembuatan tanda tangan ECDSA melibatkan penggunaan kunci privat untuk menghasilkan tanda tangan unik dari pesan yang telah di-*hash*, atau disebut dengan proses *signing*. Sementara itu, proses verifikasi tanda tangan digital tersebut menggunakan kunci publik yang sesuai.

Dalam konteks keamanan data, ECDSA digunakan untuk memastikan integritas, otentikasi, dan aspek *nonrepudiation* dari sebuah data. Tanda tangan digital yang dihasilkan ECDSA dapat diverifikasi penerima untuk memastikan bahwa pesan tidak mengalami perubahan sejak dilakukan penandatanganan oleh pengirim yang sah. Hal ini merupakan aspek yang sangat penting dalam sistem medis karena keakuratan dan integritas pada sebuah data merupakan hal yang krusial. Dengan demikian, dengan memanfaatkan ECDSA, data citra medis dapat terlindungi dari proses manipulasi dan pengubahan dengan tingkat keamanan yang tinggi dan efisien.

## III. RANCANGAN SOLUSI DAN IMPLEMENTASI

Pada bagian ini, akan dibahas terkait rancangan solusi yang akan dibangun dan implementasi dari rancangan solusi terseut untuk menyelesaikan permasalahan yang diberikan.

### *A. Rancangan Solusi*

Untuk mengatasi permasalahan keamanan dan integritas konten pada citra medis, penulis mengusulkan solusi berupa penerapan enkripsi dan tanda tangan digital terhadap citra medis. Enkripsi bertujuan untuk mengonversi citra medis menjadi bentuk yang tidak dapat terbaca sehingga terjaga keamanan dan kerahasiaan data terhadap akses ilegal. Sementara itu, tanda tangan digital bertujuan untuk memastikan integritas dan keaslian suatu data serta memastikan bahwa pengirim pesan tidak dapat menyangkal data tersebut.

Proses enkripsi dan dekripsi data citra medis dilakukan dengan menggunakan teknik enkripsi *hybrid* yang mengombinasikan algoritma AES dan RSA dengan ukuran *private key* sebesar 2048bit. Algoritma RSA digunakan untuk mengenkripsi kunci simetris AES, sedangkan AES digunakan untuk mengenkripsi data. Sementara itu, proses tanda tangan digital dilakukan dengan menggunakan algoritma ECDSA yang menggunakan kurva SECP256k1 dan fungsi *hash* SHA256. Berikut adalah penjelasan alur/proses yang dilakukan pada proses enkripsi dan penandatanganan citra digital.

*1)* Pertama-tama, pengirim dan penerima terlebih dahulu membangkitkan pasangan kunci baik untuk kunci enkripsi asimetris RSA maupun kunci tanda tangan digital ECDSA.

*2)* Selanjutnya, pengirim memasukan citra medis yang hendak dikirimkan ke penerima. Citra medis masukan selanjutnya dikonversi menjadi kumpulan *bytes*.

*3)* Nilai *hash* selanjutnya dihitung dari kumpulan *bytes* tersebut dengan menggunakan algoritma SHA256. Hasil dari *hash* tersebut selanjutnya dilakukan *signing* dengan menggunakan *private key* ECDSA sehingga dihasilkan tanda tangan digital (*signature*).

*4) Signature* tersebut selanjutnya disisipkan ke akhir *bytes* citra untuk dilakukan proses enkripsi.

*5)* Selanjutnya, *bytes* citra medis yang telah disisipi signature dilakukan proses pengenkripsian dengan menggunakan enkripsi *hybrid* yang mengombinasikan AES untuk mengenkripsi data *bytes* tersebut serta RSA untuk mengenkripsi kunci simetris yang digunakan AES dengan menggunakan *public key* RSA penerima.

*6)* Terakhir, pasangan *bytes* citra beserta kunci simetris yang telah dienkripsi dikirimkan ke penerima.

Berikut adalah penjelasan alur/proses yang dilakukan pada proses dekripsi dan pemverifikasian tanda citra digital.

*1)* Pertama-tama, penerima yang telah menerima pasangan *bytes* citra beserta kunci simetris yang telah dienkripsi melakukan pendekripsian kunci simetris terlebih dahulu dengan menggunakan *private key* RSA penerima.

*2)* Kunci simetris AES yang telah didekripsi selanjutnya digunakan untuk mendekripsi *bytes* citra yang telah terenkripsi sehingga diperoleh hasil dekripsi berupa gabungan *bytes* citra dan tanda tangan digital (*signature*).

*3)* Selanjutnya, penerima melakukan verifikasi *bytes* citra dengan *signature* tersebut dengan *public key* ECDSA pengirim. Apabila hasil verifikasi sesuai, penerima dapat memvalidasi bahwa dokumen terjamin keasliannya serta pengirim juga terjamin keasliannya dan nirpenyangkalan.

### *B. Implementasi*

Program penerapan enkripsi dan tanda tangan digital pada citra medis diimplementasikan dengan menggunakan algoritma enkripsi *hybrid* yang mengombinasikan algoritma AES dan RSA serta algoritma ECDSA yang menggunakan kurva SECP256k1 dan fungsi *hash* SHA256. Pada algoritma RSA, ukuran *private key* yang digunakan adalah 2048bit. Program dibuat dalam bahasa Python dengan menggunakan kakas *pycryptodome* serta *ecdsa* untuk algoritma kriptografi. Terdapat beberapa menu yang diimplementasikan pada program, antara lain.

*1)* Pembangkitan pasangan kunci privat dan kunci publik untuk algoritma RSA.

*2)* Pembangkitan pasangan kunci privat dan kunci publik untuk algoritma ECDSA.

*3)* Pengenkripsian dan penandatanganan citra medis.

*4)* Pendekripsian dan pemverifikasian tanda tangan citra medis.

*5)* Pembandingan citra hasil dekripsi dengan citra asli dengan menggunakan metrik *peak signal-to-noise ratio* (PSNR)

## IV. PENGUJIAN DAN ANALISIS

Program penerapan enkripsi dan tanda tangan 6igital menyediakan 6 menu, seperti yang dapat dilihat pada Fig 8.

```
Available commands:
1.      Generate RSA Key Pairs
2.      Generate ECDSA Key Pairs
3.      Encrypt and Sign Image
4.      Decrypt and Verify Encrypted Image
5.      Compare Two Images (PSNR)
6.      Exit
Enter command:
```

Fig. 6. Tampilan Menu Program

Pertama-tama, sebelum melakukan pengenkripsian dan penandatanganan citra medis, pengirim dan penerima harus terlebih dahulu membangkitkan kunci privat dan kunci publik RSA dan ECDSA. Proses ini dapat dilakukan berturut-turut dengan memilih menu nomor 1 dan 2. Pada saat menjalankan menu 1 dan 2, pengguna perlu memasukan nama *file private key* dan *public key* untuk disimpan pada komputer, seperti yang ditunjukkan pada Fig 7. Selanjutnya, pengirim dan penerima perlu untuk melakukan pembagian *file* kunci publik masing-masing ke satu sama lain.

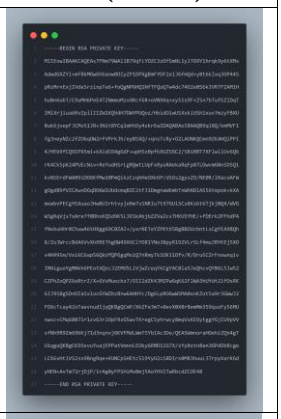
```
Available commands:
1.      Generate RSA Key Pairs
2.      Generate ECDSA Key Pairs
3.      Encrypt and Sign Image
4.      Decrypt and Verify Encrypted Image
5.      Compare two images (PSNR)
6.      Exit
Enter command: 1
Enter RSA private key filename: alice_rsa_sk.pem
Enter RSA public key filename: alice_rsa_pk.pem
RSA private key file is written successfully: alice_rsa_sk.pem
RSA public key file is written successfully: alice_rsa_pk.pem

Available commands:
1.      Generate RSA Key Pairs
2.      Generate ECDSA Key Pairs
3.      Encrypt and Sign Image
4.      Decrypt and Verify Encrypted Image
5.      Compare Two Images (PSNR)
6.      Exit
Enter command: 2
Enter ECDSA private key filename: alice_ecdsa_sk.pem
Enter ECDSA public key filename: alice_ecdsa_pk.pem
ECDSA private key file is written successfully: alice_ecdsa_sk.pem
ECDSA public key file is written successfully: alice_ecdsa_pk.pem
```

Fig. 7. Tampilan Menu 1 dan 2

Adapun pasangan kunci RSA dan ECDSA ditunjukkan pada Table I.

TABLE I. PASANGAN KUNCI RSA DAN ECDSA

| ***Jenis Kunci*** | ***Pengguna*** | |
|---|---|---|
| | ***Alice* (Pengirim)** | ***Bob* (Penerima)** |

| *Jenis Kunci* | *Pengguna* | |
|---|---|---|
| | ***Alice* (Pengirim)** | ***Bob* (Penerima)** |
| *Private Key* RSA |  |  |
| *Public Key* RSA |  |  |
| *Private Key* ECDSA | □/<□□C□ □□4□E□□<br>ɔ□9□'S□h□Uj□□□□ | eY7□□?iT□ \mW□□.LT<br>W□□xh□$□□□□ |
| *Public Key* ECDSA | □□`r□□h ou□H-<br>V!G□□□□=74□ □-<br>9□□□ IZI□□□□&o<br>□□X!9□□□<br>+-P { | m□□<□Ṇt淹x V□5h□Qa<br>□w□□<br>P□□!□□[□~ □ΨK<br>□□"Z廋+-<br>□[!z>□□u |

Selanjutnya, setelah membangkitkan kunci, pengirim dapat melakukan pengenkripsian dan penandatanganan citra medis dengan menggunakan menu 3. Pada menu 3, terdapat beberapa *input* yang perlu dimasukan oleh pengirim pesan, antara lain *public key* RSA penerima, *private key* ECDSA pengirim, nama *file* citra medis masukan, dan nama *file* citra medis hasil enkripsi dan penandatanganan, seperti yang ditunjukkan pada Fig 8. Pada gambar tersebut, pengirim (Alice) memasukan *public key* RSA penerima (Bob) dan *private key* ECDSA miliknya.

```
Available commands:
1.      Generate RSA Key Pairs
2.      Generate ECDSA Key Pairs
3.      Encrypt and Sign Image
4.      Decrypt and Verify Encrypted Image
5.      Compare two images (PSNR)
6.      Exit
Enter command: 3
Enter other RSA public key path: bob_rsa_pk.pem
Enter ECDSA private key path: alice_ecdsa_sk.pem
Enter image path: test_image_1.jpg
Signing data...
Concating signature to data...
Encrypting data...
Encrypting symmetric key...
Enter encrypted image path: enc_image_1.jpg
Encrypted image is successfully saved to enc_image_1.jpg
```

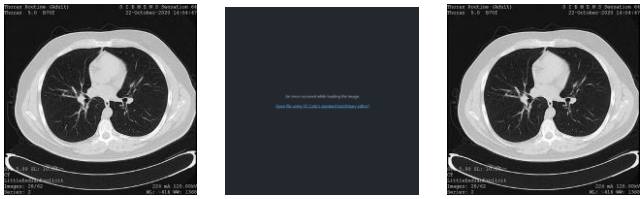
Fig. 8. Tampilan Menu 3

Selanjutnya, setelah menerima citra medis yang telah dienkripsi, penerima dapat melakukan pendekripsian dan pemverifikasian tanda tangan digital citra medis dengan menggunakan menu 4. Pada menu 4, terdapat beberapa *input* yang perlu dimasukan oleh penerima pesan, antara lain *private key* RSA penerima, *public key* ECDSA pengirim, nama *file* citra medis yang telah terenkripsi, dan nama *file* citra medis hasil dekripsi, seperti yang ditunjukkan pada Fig 9. Pada gambar tersebut, penerima (Bob) memasukan *private key* RSA miliknya dan *public key* ECDSA pengirim (Alice).

```
Available commands:
1.      Generate RSA Key Pairs
2.      Generate ECDSA Key Pairs
3.      Encrypt and Sign Image
4.      Decrypt and Verify Encrypted Image
5.      Compare Two Images (PSNR)
6.      Exit
Enter command: 4
Enter RSA private key path: bob_rsa_sk.pem
Enter other ECDSA public key path: alice_ecdsa_pk.pem
Enter encrypted image path: enc_image_1.jpg
Decrypting symmetric key...
Decrypting data...
Verifying signature...
Signature is valid!
Enter decrypted image path: dec_image_1.jpg
Decrypted image is successfully saved to dec_image_1.jpg
```

Fig. 9. Tampilan Menu 4

Dengan melakukan pendekripsian dan pemverifikasian tanda tangan digital, diperoleh citra hasil dekripsi, seperti yang ditunjukkan pada Fig 10(c). Adapun perbandingan antara citra orisinal, hasil enkripsi, dan hasil dekripsi secara berturut-turut dapat dilihat pada Fig 10(a), Fig 10(b), dan Fig 10(c). Namun, karena pengenkripsian terjadi pada tingkat *bytes*, citra hasil enkripsi tidak dapat terbuka.



(a) (b) (c)

Fig. 10. Perbandingan (a) citra orisinal, (b) hasil enkripsi, dan (c) hasil dekripsi

Selain itu, akurasi hasil citra hasil dekripsi pada citra medis merupakan hal yang esensial untuk mencegah terjadinya kesalahan diagnosis. Dengan demikian, perlu dilakukan pengujian akurasi hasil dekripsi terhadap citra masukan. Untuk menguji akurasi hasil dekripsi terhadap citra medis masukan, kedua citra tersebut dilakukan pengujian terhadap metrik PSNR untuk memeriksa apakah ada perubahan pada hasil dekripsi sehingga menimbulkan *noise*. Adapun pengujian dilakukan dengan menggunakan menu 5, seperti yang ditunjukkan pada Fig 11. Pada pengujian tersebut, hasil PSNR yang diperoleh bernilai *infinity* sehingga dapat disimpulkan bahwa citra hasil dekripsi tidak mengalami perubahan sama sekali.

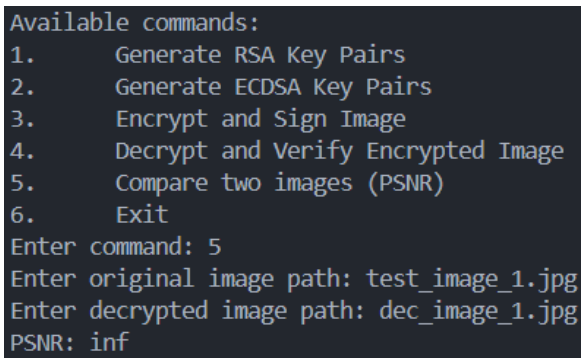



Fig. 11. Tampilan Menu 5

Di samping itu, pengujian terhadap keamanan data juga perlu dilakukan. Untuk menangani hal tersebut, pengujian pengaksesan ilegal dengan menggunakan *private key* RSA pihak ketiga (Charlie) dilakukan, seperti yang ditunjukkan pada Fig 12. Pada pengujian tersebut, terbukti bahwa pihak ketiga yang tidak memiliki *private key* RSA penerima tidak dapat mendekripsi citra medis tersebut.


Fig. 12. Kasus Pendekripsian dengan *Private Key* RSA yang Tidak Sesuai

Terakhir, pengujian terhadap integritas data juga perlu dilakukan. Untuk menangani hal tersebut, pengujian pemodifikasian data setelah dilakukan penandatanganan dilakukan. Adapun citra hasil modifikasi ditunjukkan pada Fig 13.

Fig. 13. Citra Medis Hasil Modifikasi

Seperti pada Fig 14, pada pengujian tersebut, terbukti bahwa tanda tangan digital menjadi tidak valid akibat pemodifikasian pada citra pascapenandatanganan. Dengan demikian, terbukti bahwa terdapat pemodifikasian terhadap citra asli.


Fig. 14. Kasus Pemverifikasian Tanda Tangan Citra yang Telah Dimodifikasi

Berdasarkan pengujian yang dilakukan, penerapan enkripsi dan tanda tangan digital pada citra medis dengan menggunakan algoritma enkripsi *hybrid* yang mengombinasikan algoritma AES dan RSA serta algoritma ECDSA yang menggunakan kurva SECP256k1 dan fungsi *hash* SHA256 telah diimplementasikan dengan baik.

## V. KESIMPULAN DAN SARAN

Pengenkripsian dengan menggunakan algoritma enkripsi *hybrid* yang mengombinasikan algoritma AES dan RSA serta penandatanganan digital dengan menggunakan algoritma ECDSA yang menggunakan kurva SECP256k1 dan fungsi *hash* SHA256 berhasil diimplementasikan dengan baik. Penerapan enkripsi dan tanda tangan digital pada citra medis terbukti mampu menjaga keamanan dan integritas citra tersebut sehingga tidak dapat diakses dan dimodifikasi oleh pihak yang bertanggung jawab. Berdasarkan pengujian yang telah dilakukan, program berhasil melakukan pengenkripsian dan pendekripsian citra medis tanpa menurunkan akurasi dari citra hasil dekripsi. Selain itu, program juga berhasil melakukan penandatanganan digital dan pemvalidasian keaslian citra melalui verifikasi tanda tangan digital.

Program yang diimplementasikan hanya dijalankan sebatas pada komputer secara lokal saja tanpa adanya pengiriman citra melalui jaringan. Untuk membangun program yang lebih aplikatif, penulis menyarankan untuk membangun sistem pengiriman citra medis yang juga terenkripsi antara pengirim dan penerima.

## TAUTAN SOURCE CODE

Kode algoritma yang digunakan pada makalah ini dapat dilihat pada tautan GitHub berikut.

https://github.com/eiffelaqila/Makalah_IF4020_Kriptografi

## UCAPAN TERIMA KASIH

Pertama, penulis mengucap syukur kepada Tuhan karena atas rahmatnya penulis dapat menyelesaikan makalah ini dengan baik. Penulis juga mengucapkan terima kasih kepada semua pihak yang telah berkontribusi dalam makalah ini. Penulis juga mengucapkan terima kasih yang sebesar-besarnya kepada bapak Dr. Ir. Rinaldi Munir, M.T. selaku dosen pengajar Mata Kuliah IF4020 Kriptografi Tahun Ajaran 2023/2024 yang telah mengajarkan berbagai pengetahuan sehingga penulis mampu menyelesaikan makalah ini.

## REFERENSI


[1] Castro, F., Impedovo, D., & Pirlo, G. (2022). *A Medical Image Encryption Scheme for Secure Fingerprint-Based Authenticated Transmission*. Applied Sciences, 13(10), 6099. https://doi.org/10.3390/app13106099

[2] Munir, Rinaldi. 2024. *01-Pengantar Kriptografi*. Diakses dari https://informatika.stei.itb.ac.id/~rinaldi.munir/Kriptografi/2023-2024/01-Pengantar-Kriptografi-(2024).pdf

[3] Munir, Rinaldi. 2024. *15-Beberapa cipher blok (Bagian 2: AES)*. Diakses dari https://informatika.stei.itb.ac.id/~rinaldi.munir/Kriptografi/2023-2024/15-Beberapa-block-cipher-bagian2-2024.pdf

[4] Munir, Rinaldi. 2024. *18-Algoritma RSA*. Diakses dari https://informatika.stei.itb.ac.id/~rinaldi.munir/Kriptografi/2023-2024/18-Algoritma-RSA-2024.pdf

[5] Munir, Rinaldi. 2024. *Elliptic Curve Cryptography - Bagian 2*. Diakses dari https://informatika.stei.itb.ac.id/~rinaldi.munir/Kriptografi/2023-2024/23-ECC-Bagian2-2024.pdf


## 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, 12 Juni 2024

Eiffel Aqila Amarendra
13520074