

Implementasi Algoritma RSA Untuk Aplikasi Enkripsi Dan Dekripsi Citra Dua Dimensi Berbasis Web (Studi Kasus: PT. Intigarmindo Persada)

Deshinta Ariani^{1*}, Dimas Abisono Pungkastyo¹

¹Fakultas Ilmu Komputer, Teknik Informatika, Universitas Pamulang, Jl. Raya Puspipetek No. 46, Kel. Buaran, Kec. Serpong, Kota Tangerang Selatan, Banten 15310, Indonesia

Email: ^{1*}deshintaarn@email.com, ²dosen006752@unpam.ac.id

(* : coressponding author)

Abstrak—Data citra *sample design* adalah ajuan desain pakaian atau aksesoris yang dibuat oleh tim pendesain PT Intigarmindo Persada yang berisikan informasi mengenai ukuran, pola, warna, dan bahan yang akan dibutuhkan pada produksi. Guna mengamankan data citra *sample design* dari kebocoran informasi, maka dibutuhkan sistem yang dapat menyandikan data citra *sample design* agar kerahasiaannya terjaga. Penelitian ini mengimplementasikan algoritma kriptografi *rivest shamir adleman* (RSA) untuk perancangan aplikasi enkripsi dan dekripsi data citra dua dimensi yang berbasis web dengan menggunakan metode pengembangan *waterfall*. Penelitian ini menghasilkan aplikasi enkripsi dan dekripsi data citra dua dimensi yang dapat meminimalisir kebocoran informasi dari data citra *sample design*. Hasil pengujian menunjukkan bahwa algoritma RSA dapat mengamankan data citra menjadi tidak dapat terbaca dan mengembalikannya ke dalam bentuk semula.

Kata Kunci: Data Citra, *Rivest Shamir Adleman*, Enkripsi, Dekripsi

Abstract—*Sample design image data is a design proposal for clothes or accessories made by the design team of PT Intigarmindo Persada which contains information about the size, pattern, color, and materials that will be needed in production. In order to secure sample design image data from information leakage, a system is needed that can encode sample design image data so that confidentiality is maintained. This study will implement the rivest shamir adleman (RSA) cryptographic algorithm for the design of encryption and decryption applications of web-based two-dimensional image data using waterfall development methods. This research resulted in two-dimensional encryption and decryption application of image data that can minimize information leakage from sample design image data. The test results show that the RSA algorithm can secure image data into unreadability and return it to its original form.*

Keywords: *Imagery Data, Rivest Shamir Adleman, Encryption, Decryption*

1. PENDAHULUAN

PT Intigarmindo Persada merupakan perusahaan yang bergerak di bidang industri tekstil yang memproduksi pakaian jadi dibawah naungan brand *Lois Jeans* yang dibentuk pada tahun 1978. Hingga saat ini PT Intigarmindo Persada terus memproduksi pakaian dan aksesoris dengan bahan dasar denim hingga *leather*. Pada kegiatan produksinya, terdapat proses pengiriman data *sample design* oleh pendesain kepada tim produksi. Data *sample design* adalah data ajuan desain pakaian atau aksesoris yang dibuat oleh tim pendesain PT Intigarmindo Persada guna menambah model pakaian dan aksesoris yang diproduksi. Pada data *sample design* berisi ukuran, pola, warna, dan bahan yang akan dibutuhkan pada produksi pakaian atau aksesoris tersebut. Karena itu, perlindungan pada data *sample design* ini sangat penting guna meminimalisir kebocoran informasi kepada pihak yang tidak berwenang. Data *sample design* ini berbentuk data citra atau gambar dua dimensi.

Citra adalah gambar dua dimensi yang bisa ditampilkan pada layar komputer sebagai himpunan atau diskrit nilai digital yang disebut *pixel* atau elemen gambar (Marleny, 2022:6). Penyimpanan data citra *sample design* pada PT Intigarmindo Persada masih menggunakan sistem penyimpanan pada server lokal yang *ter-sharing* keseluruhan divisi kerja perusahaan. Cara kerja ini dapat menimbulkan masalah dalam hal keamanan *karena multi user* yang saling berbagi ruang penyimpanan dimana menyebabkan kebocoran informasi dari data citra *sample design* oleh pihak yang tidak bertanggung jawab. Dengan ruang penyimpanan yang mudah di akses oleh siapapun membuat tidak adanya keamanan yang terjamin dalam perlindungan data citra *sample design*

sehingga pengguna server dari divisi kerja lain dapat mengakses dan membahayakan keaslian data dalam aspek modifikasi.

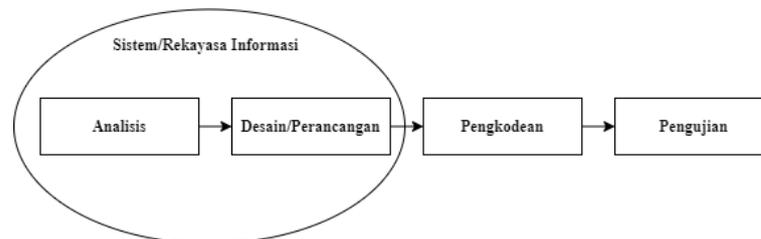
Pada kasus ini ilmu kriptografi dapat diterapkan guna mengatasi masalah keamanan pada data citra *sample design*. Kriptografi merupakan suatu teknik menyembunyikan pesan dimana pesan tersebut hanya dapat diketahui oleh orang tertentu dimana pesan tersebut sering disebut enkripsi (Kurniawan, Dedih & Supriyadi, 2017:102). Dunia kriptografi saat ini sudah menerapkan metode penyandian data berbentuk multimedia salah satunya pada citra dua dimensi. Keamanan dan keakuratan penyediaan informasi menjadi sangat penting bagi segala kalangan dan dengan bertambahnya citra dua dimensi dalam penggunaan penyediaan informasi, melindungi kerahasiaan, keaslian dan keutuhan gambar menjadi masalah mendasar yang harus diperhatikan.

Kriptografi memiliki beberapa algoritma diantaranya terdapat algoritma simetris dan algoritma asimetris. Algoritma simetris merupakan algoritma kriptografi yang menggunakan kunci yang sama baik untuk proses enkripsi maupun dekripsi (Meko, 2018:8). Sedangkan Algoritma asimetris merupakan pasangan kunci kriptografi yang salah satunya digunakan untuk proses enkripsi dan satu lagi dekripsi (Yusfrizal, 2019:32). Algoritma asimetris memiliki keunggulan pada tingkat keamanan karena memerlukan dua kunci berbeda pada proses enkripsi dan dekripsinya. Pada algoritma asimetris terdapat banyak metode dengan salah satunya adalah metode RSA (*Rivest Shamir Adleman*). RSA adalah metode yang menggunakan perhitungan matematika yang rumit dan disertai dengan kunci pengaman awal dengan *private key* maupun *public key* sehingga amat sulit untuk ditembus oleh *hacker* (Sahara, Prastiawan & Rohman, 2017:119). Dengan itu dapat diketahui bahwa algoritma kunci RSA memiliki tingkat keamanan yang terjamin. Penulis memilih algoritma RSA sebagai pendekatan guna mengetahui pengaruh keamanannya pada kerahasiaan data citra *sample design*. RSA adalah algoritma kriptografi asimetris yang menggunakan kunci berbeda untuk proses enkripsi dan dekripsinya. Kunci publik digunakan untuk mengenkripsi dan kunci privat untuk mendekripsi.

2. METODOLOGI PENELITIAN

2.1 Metode Pengembangan Sistem

Pada proses perancangan sistem informasi ini penulis menggunakan *System Development Live Cycle* (SDLC) dengan metode *waterfall* atau metode air terjun karena metode ini memiliki tahapan sistem yang terstruktur. Metode Waterfall adalah suatu proses pengembangan perangkat lunak berurutan, di mana kemajuan dipandang sebagai terus mengalir ke bawah (seperti air terjun) melewati fase-fase perencanaan, pemodelan, implementasi (konstruksi), dan pengujian (Trisianto, 2018:12). Pada metode ini, setiap tahapannya harus diselesaikan terlebih dahulu agar semua proses dari tahap awal sampai akhir dapat terselesaikan dengan baik.



Gambar 1. Pemodelan Metode *Waterfall*

2.2 Metode Pengumpulan Data

Melakukan pengumpulan data penunjang melalui sumber yang berkaitan dengan penelitian. Pengumpulan data dilakukan dengan beberapa metode yaitu metode observasi, metode wawancara dan studi pustaka.

a. Metode Observasi

Pada metode ini, penulis melakukan pengamatan langsung ke divisi produksi PT Intigarmino Persada yang ber alamat di Jl. Pualam Raya 31, Kemayoran, Jakarta Pusat.

Observasi ini cukup efektif bagi penulis dalam mengetahui proses transaksi data *sample design* pada tim produksi.

b. Metode Wawancara

Pada penelitian ini penulis melakukan wawancara kepada tim produksi guna mengetahui teknis penyimpanan data *sample design* dan juga masalah yang terjadi dalam proses transaksi sehingga penulis dapat mengambil kesimpulan yang pada akhirnya dapat diperoleh sebuah data penelitian.

c. Studi Pustaka

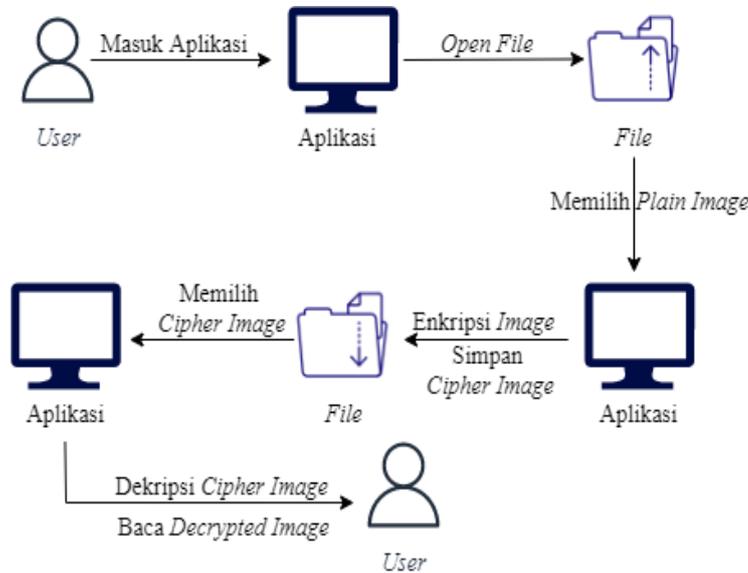
Pada metode ini penulis mengumpulkan data dan informasi yang diperoleh dari berbagai media seperti buku, jurnal, maupun *website*. Adapun sumber-sumber buku, jurnal dan *website* yang digunakan pada penelitian ini dapat dilihat pada bagian *references*.

3. ANALISA DAN PEMBAHASAN

3.1 Analisa

3.1.1 Analisa Rancangan Program

Program atau aplikasi yang akan dibuat terdiri dari empat buah halaman, yaitu *home page*, menu *help*, menu enkripsi dan menu dekripsi. Untuk melakukan enkripsi, *user* dapat memilih tombol enkripsi pada *home page*, begitupun saat ingin melakukan dekripsi. Menu *help* berguna untuk memberi tahu fungsi - fungsi pada aplikasi dan tata cara melakukan proses enkripsi dan dekripsi pada aplikasi. Saat ingin mengenkripsi data citra *sample design*, *user* bisa langsung menuju ke menu enkripsi dan memilih data citra mana yang ingin di enkripsi. Sedangkan untuk mengembalikan data citra yang sudah terenkripsi (*cipher image*) *user* dapat memilih halaman menu dekripsi dan memilih *cipher image* mana yang ingin dipulihkan.



Gambar 2. Analisa Rancangan Program

3.1.2 Analisa Kebutuhan

Pada tahapan perancangan terdapat proses analisis kebutuhan perangkat lunak. Pada tahap ini dibagi lagi menjadi dua jenis kebutuhan yaitu kebutuhan fungsional dan kebutuhan non fungsional. Kebutuhan fungsional mencakup layanan atau proses apa saja yang akan tersedia pada sistem, sedangkan kebutuhan non fungsional mencakup kebutuhan yang berfokus pada perilaku yang dimiliki sistem atau batasan fungsi yang ada pada sistem. Adapun kebutuhan-kebutuhan utama pada sistem ini sebagai berikut:

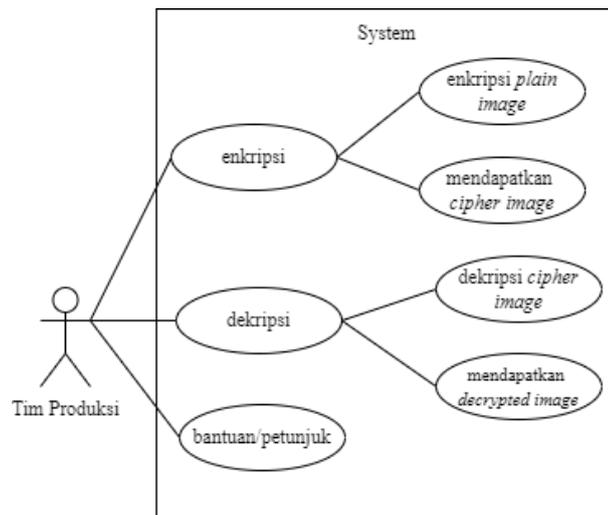
- a. Kebutuhan fungsional:
 1. Sistem dapat melakukan penyandian data citra (enkripsi)
 2. Sistem dapat mengembalikan data citra yang sudah terenkripsi ke bentuk semula (dekripsi)
 3. Sistem memerlukan *public key* dan *private key* untuk proses enkripsi dan dekripsi RSA.
- b. Kebutuhan non fungsional:
 1. Aplikasi dapat dijalankan oleh beberapa web browser diantaranya *google chrome*, *mozilla firefox* dan *internet explore*.
 2. Aplikasi memiliki tampilan antarmuka yang mudah dipahami (*user friendly*).
 3. Aplikasi dapat dijalankan pada komputer dengan kapasitas memori minimum 2GB RAM.

3.1.3 Analisa Perancangan *Unified Modeling Language* (UML)

Tahapan ini dilakukan untuk menggambarkan secara umum tentang sistem yang dirancang dan mengidentifikasi komponen-komponen terkait dengan terperinci. UML merupakan sebuah model perancangan sistem yang mempunyai kelebihan dapat memudahkan *developer* sistem dalam merancang sistem yang akan dibuat karena sifatnya yang berorientasikan pada objek (Prihandoyo, 2018:126).

a. *Use Case Diagram*

Use case diagram digunakan untuk mendeskripsikan apa yang seharusnya dilakukan oleh sistem (Handayani, 2018:185). Diagram ini menggambarkan interaksi yang terjadi antara pengguna dengan komponen yang ada pada sistem.



Gambar 3. *Use Case Diagram* Aplikasi

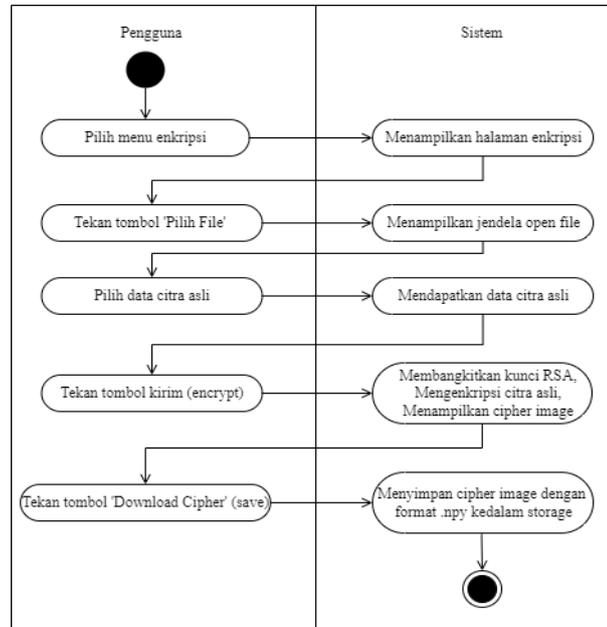
Dekripsi pendefinisian aktor pada aplikasi enkripsi dan dekripsi data citra dua dimensi ini dapat dilihat pada tabel 1.

Tabel 1. Definisi Aktor

No.	Aktor	Dekripsi
1.	Tim Produksi	<ul style="list-style-type: none"> • Tim Produksi dapat mengenkripsi data citra <i>sample design</i>. • Tim Produksi dapat menyimpan <i>cipher image</i> dari data citra <i>sample design</i>. • Tim produksi dapat mengembalikan <i>cipher image</i> dari data citra <i>sample design</i>. • Tim produksi dapat melihat dan menyimpan citra asli hasil dekripsi. • Tim produksi dapat melihat petunjuk terkait cara kerja aplikasi.

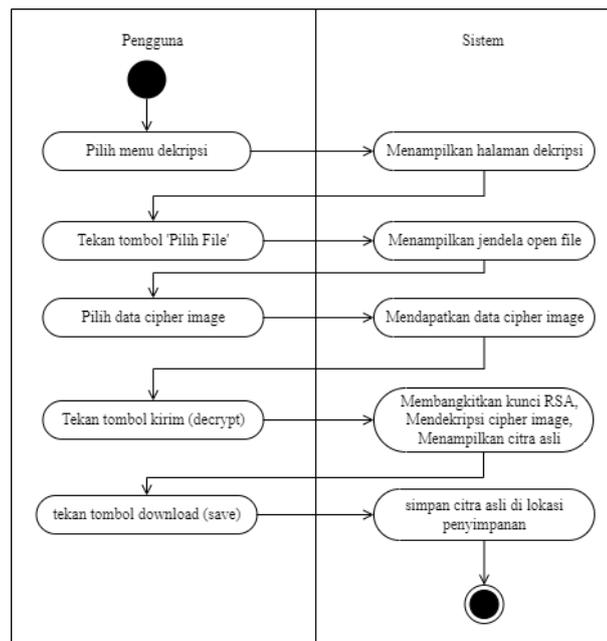
b. Activity Diagram

Activity diagram digunakan untuk menggambarkan berbagai aktivitas dalam sistem yang dirancang, bagaimana masing-masing fungsionalitas bekerja, dan bagaimana suatu fungsionalitas berakhir (Sari dkk, 2021:67). Diagram ini akan menggambarkan aliran suatu aktivitas ke aktivitas lainnya di dalam sistem yang dibangun.



Gambar 4. Activity Diagram Enkripsi

Diagram pada gambar 4 mendefinisikan aktivitas pengguna dalam mengenkripsi data citra dengan cara memilih menu enkripsi yang ada pada *home page* dan memilih data citra yang ingin dienkripsi. Selanjutnya klik tombol kirim untuk memproses enkripsi, setelah proses enkripsi berhasil pengguna dapat menyimpan *cipher image* yang sudah dihasilkan dari proses enkripsi.

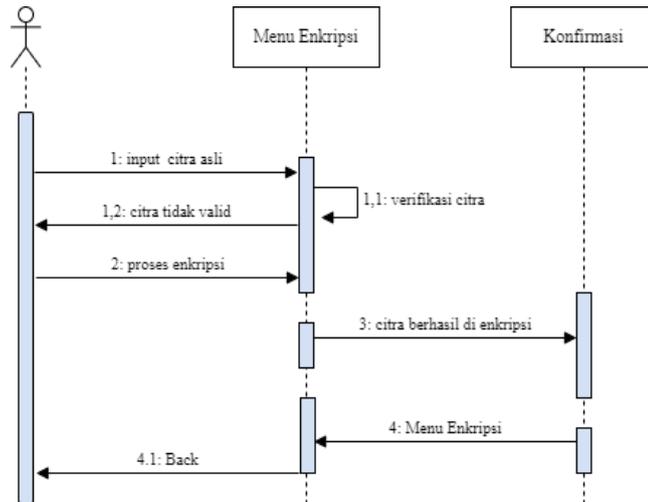


Gambar 5. Activity Diagram Deskripsi

:Diagram pada gambar 5 mendefinisikan aktivitas pengguna dalam mendekripsi *cipher image* dengan cara memilih menu dekripsi yang ada pada *home page* dan memilih *cipher image* yang ingin dipulihkan dengan dekripsi. Selanjutnya klik tombol *decrypt* untuk memproses dekripsi, setelah proses dekripsi berhasil akan muncul data citra asli dan pengguna dapat melihat maupun menyimpan data citra *sample design* yang sudah bisa terbaca.

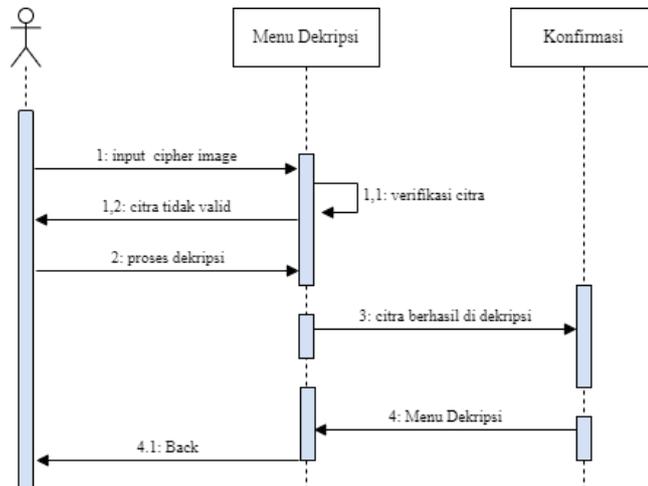
c. Sequence Diagram

Sequence diagram adalah suatu diagram yang menggambarkan interaksi antara objek dan mengidentifikasi komunikasi antara objek tersebut (Alita dkk, 2021:20). Diagram ini akan menggambarkan interaksi pesan dalam rangkaian waktu yang terjadi pada suatu sistem.



Gambar 6. Sequence Diagram Enkripsi

Pada gambar 6 dijelaskan tahapan mulai dari penginputan data citra asli sampai dengan proses enkripsi. Hanya citra dengan format jpg yang dapat di enkripsi.



Gambar 7. Sequence Diagram Deskripsi

Pada gambar 7 dijelaskan tahapan mulai dari penginputan *cipher image* sampai dengan proses dekripsi. Hanya format npy yang dapat di dekripsi

3.1.4 Analisa Penerapan Rivest Shamir Adleman

Pada algoritma RSA, perlu dilakukan pembangkitan kunci terlebih dahulu sebelum dilakukannya proses enkripsi dan dekripsi. Berikut penjelasan algoritma pembangkitan kunci:

- a. Memilih dua bilangan prima secara acak (p dan q) dengan $p \neq q$. Nilai p dan q bersifat rahasia.
- b. Menghitung nilai n dengan persamaan $n = p * q$. nilai n tidak harus dirahasiakan.
- c. Menghitung nilai m dengan persamaan $\Phi(n) = (p-1) * (q-1)$.
- d. Memilih nilai e dengan syarat $e > 1$, dan FPB ($e, \Phi(n)$) = 1
- e. Memilih nilai d dengan ketentuan $(d.e) \bmod \Phi(n) = 1$

Dari pembangkitan kunci diatas dapat diperoleh *public key* yaitu pasangan (e, n) dan *private key* yaitu pasangan (d, n). Setelah mendapatkan masing - masing kunci privat dan publik, maka dapat dilakukan proses enkripsi dan dekripsi. Proses enkripsi menggunakan persamaan $C_i = P_i^e \bmod n$ sedangkan proses dekripsi menggunakan persamaan $P_i = C_i^d \bmod n$ dengan C untuk *Cipherkey* dan P untuk *Plainkey* (kunci asli). Perhitungann manual algoritma RSA dapat digunakan sebagai gambaran kasar dari cara kerja algoritma ini. Berikut perhitungan manual untuk algoritma *Rivest Shamir Adleman*:

Langkah I: Memilih dua bilangan prima untuk p dan q dimana $p \neq q$.

$$p = 37$$

$$q = 7$$

Langkah II: Menghitung nilai $n = p * q$

$$n = 37 * 7$$

$$n = 259$$

Langkah III: Menghitung $\Phi(n) = (p-1) * (q-1)$

$$\Phi(n) = (37 - 1) (7 - 1)$$

$$\Phi(n) = (36) (6)$$

$$\Phi(n) = 216$$

Langkah IV: Memilih nilai e dimana $\text{fpb}(e, 216) = 1$. Misal $e = 3$, apakah $\text{gcd}(3, 216) = 1$?

$$3 \bmod 216 = 3$$

$$216 \bmod 3 = 0$$

Karena $\text{gcd}(3, 216) \neq 1$ maka 3 tidak bisa mengisi nilai e .

Maka pilih nilai lain, misal $e = 5$, apakah $\text{gcd}(5, 216) = 1$?

$$5 \bmod 216 = 5$$

$$216 \bmod 5 = 1$$

Karena $\text{gcd}(5, 216) = 1$ maka 5 dapat mengisi nilai e .

Langkah V: Memilih nilai d dengan rumus $d = 1 + (k \Phi(n)) / e$

misal $k = 1$, maka $d = 43,4$ (tidak bulat)

misal $k = 2$, maka $d = 86,6$ (tidak bulat)

misal $k = 3$, maka $d = 129,8$ (tidak bulat)

misal $k = 4$, maka $d = 173$ (bulat)

Selanjutnya dipilih $d = 173$ dengan syarat $(d.e) \bmod \Phi(n) = 1$, maka:

$$(173 \times 5) \bmod 216$$

$$865 \bmod 216 = 1$$

Karena $(d.e) \bmod \Phi(n) = 1$, Maka 173 dapat mengisi nilai e .

Setelah mendapatkan pasangan (e, n) yaitu (5, 259) sebagai kunci publik dan pasangan (d, n) yaitu (865, 259) seagai kunci privat, selanjutnya adalah proses enkripsi dengan rumus enkripsi $C_i = P_i^e \bmod n$. Menggunakan perumpamaan M adalah nilai desimal 115, 118, 116.

Langkah VI: Proses enkripsi dengan rumus $C_i = P_i^e \bmod n$, maka:

$$C_1 = 115^5 \bmod 259 = 173$$

$$C_2 = 118^5 \bmod 259 = 83$$

$$C_3 = 116^5 \bmod 259 = 128$$

Ciphertext: 173, 83, 128.

Langkah VI: Setelah mendapatkan ciphertext, untuk mengembalikannya menjadi *plaintext* atau teks asli diperlukan proses dekripsi dengan rumus $P_i = C_i^d \bmod n$, maka:

$$M_1 = 173^{173} \bmod 259 = 115$$

$$M_2 = 83^{173} \bmod 259 = 118$$

$$M_3 = 128^{173} \bmod 259 = 116$$

Maka *plainkey* hasil dekripsi adalah P (115, 118, 116) yang mana kembali ke nilai semula.

4. IMPLEMENTASI

Setelah proses perancangan selesai, maka langkah selanjutnya adalah tahap implementasi. Pada bab ini akan dijelaskan implementasi dari rancangan yang sudah dibuat.

4.1 Tampilan Program

a. Tampilan Halaman *Home Page*

Halaman ini menampilkan pilihan - pilihan yang ingin dituju seperti menu enkripsi, dekripsi atau *help*.

Aplikasi Enkripsi Dan Dekripsi Data Citra Sample Design



PT. Intigarmindo Persada LoisJeans

Gambar 8. Tampilan Halaman *Home Page*

b. Tampilan Halaman Menu *Help*

Halaman ini berisikan panduan atau petunjuk penggunaan fungsi - fungsi yang terdapat pada aplikasi.

Aplikasi Enkripsi Dan Dekripsi Data Citra Sample Design



PT. Intigarmindo Persada LoisJeans

Gambar 9. Tampilan Halaman Menu *Help*

c. Tampilan Halaman Menu Enkripsi

Menu ini merupakan halaman untuk memproses enkripsi pada data citra. Pada menu ini terdapat tahapan pemilihan data citra asli yang kemudian akan di proses untuk dijadikan data citra terenkripsi. Hasil dari enkripsi data citra tersebut dapat disimpan dalam format npy yang berisikan indeks warna yang sudah teracak.

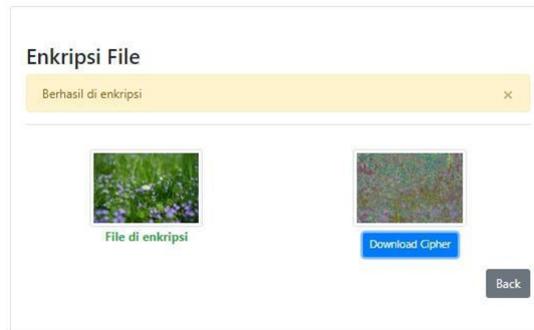
Aplikasi Enkripsi Dan Dekripsi Data Citra Sample Design



PT. Intigarmindo Persada LoisJeans

Gambar 10. Tampilan Halaman Menu Enkripsi Input

Aplikasi Enkripsi Dan Dekripsi Data Citra Sample Design

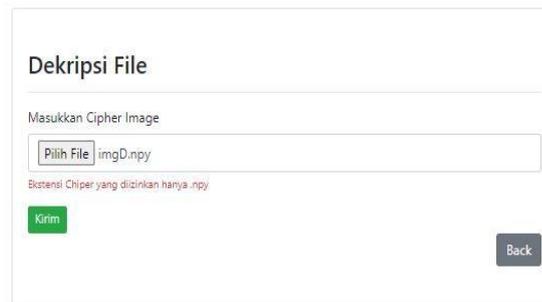


PT. Intigarmindo Persada LoisJeans

Gambar 11. Tampilan Halaman Menu Enkripsi

- d. Tampilan Halaman Menu Deskripsi
Menu ini merupakan halaman untuk mengembalikan *cipher image* ke bentuk semula (dekripsi) pada data citra.

Aplikasi Enkripsi Dan Dekripsi Data Citra Sample Design



PT. Intigarmindo Persada LoisJeans

Gambar 12. Tampilan Halaman Menu Deskripsi Input

Aplikasi Enkripsi Dan Dekripsi Data Citra Sample Design

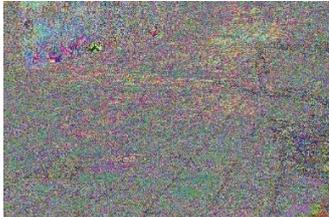


PT. Intigarmindo Persada LoisJeans

Gambar 13. Tampilan Halaman Menu Deskripsi

4.2 Pengujian Citra Asli Dengan Citra Setelah Dekripsi

Tabel 2. Pengujian Citra Asli Dengan Citra Setelah Dekripsi

Data Citra Asli	Cipher Image	Citra Setelah Dekripsi
   imgA; 61,819 bytes Cipher-imgA; 106,916 bytes imgA_decrypted; 54,751 bytes		
   imgB; 36,972 bytes Cipher-imgB; 99,094 bytes imgB_decrypted; 39,290 bytes		
   imgC; 35,877 bytes Cipher-imgC; 105,070 bytes imgC_decrypted; 54,751 bytes		

5. KESIMPULAN

Berdasarkan analisa, perancangan, implementasi dan pengujian pada penelitian ini maka dapat di ambil kesimpulan bahwa:

- citra yang dihasilkan dari proses enkripsi memiliki pola yang acak sehingga informasi visualnya tidak dapat dilihat maupun ditebak.
- Penerapan algoritma RSA pada aplikasi enkripsi dan dekripsi data citra dua dimensi dapat menjaga keaslian data citra dikarenakan data citra hasil enkripsi memiliki format npy. Format ini tidak berbentuk data visual melainkan hanya barisan acak sehingga membuatnya sulit terbaca dan dimodifikasi. Dekripsi yang dilakukan pada *cipher image* pun dapat mengembalikan data format npy ke bentuk citra semula.

REFERENCES

- Debby Alita, I. S. (2021). PENERAPAN NAÏVE BAYES CLASSIFIER UNTUK PENDUKUNG KEPUTUSAN PENERIMA BEASISWA. *JDMSI, Vol. 2*, No. 1, 17-23.
- Handayani, S. (2018). PERANCANGAN SISTEM INFORMASI PENJUALAN BERBASIS E-COMMERCE STUDI KASUS TOKO KUN JAKARTA. *ILKOM Jurnal Ilmiah Volume 10* Nomor 2, 182-189.
- Marleny, F. D. (2022). *Pengolahan Citra Digital Menggunakan Python*. Purwokerto Selatan: PENERBIT CV. PENA PERSADA.
- Meko, D. A. (2018). Perbandingan Algoritma DES, AES, IDEA Dan Blowfish dalam Enkripsi dan Dekripsi Data. *Jurnal Teknologi Terpadu, Vol. 4*, No. 1, 8-15.



- Prihandoyo, M. T. (2018). Unified Modeling Language (UML) Model Untuk Pengembangan Sistem Informasi Akademik Berbasis Web. *Jurnal Informatika: Jurnal Pengembangan IT (JPIT)*, Vol.03, No.01, 126-129.
- Ratna Sari, F. H. (2021). SISTEM INFORMASI AKUNTANSI PERHITUNGAN HARGA POKOK PRODUKSI PADA KONVEKSI SJM BANDAR LAMPUNG. *Jurnal Teknologi dan Sistem Informasi (JTSI)*, Vol. 2, No. 1, 65-73.
- Riad Sahara, H. P. (2017). Implementasi Keamanan SMS Dengan Algoritma RSA Pada Smartphone Android. *JURNAL ILMIAH FIFO, Volume IX*, No.2, 118-122.
- Satriya Tri Cahya Kurniawan, D. S. (2017). Implementasi Kriptografi Algoritma Rivest Shamir Adleman dengan Playfair Cipher pada Pesan Teks Berbasis Android. *JOIN (Jurnal Online Informatika)*, Volume 2 No. 2, 102-109.
- Trisianto, C. (2018). PENGGUNAAN METODE WATERFALL UNTUK PENGEMBANGAN SISTEM MONITORING DAN EVALUASI PEMBANGUNAN PEDESAAN. *Jurnal Teknologi Informasi ESIT Vol. XII* No. 01, 7-21.
- Yusfrizal. (2019). RANCANG BANGUN APLIKASI KRIPTOGRAFI PADA TEKS MENGGUNAKAN METODE REVERSE CHIPER DAN RSA BERBASIS ANDROID. *Jurnal Teknik Informatika Kaputama (JTIK)* Vol. 3, No. 2, 29-37.