J-SISKO TECH (Jurnal Teknologi Sistem Informasi dan Sistem Komputer TGD)
Vol.4. No.2, Juli 2021, pp. 180~190
E-ISSN: 2615-5133

Penerapan Algoritma OTP dan Algoritma RSA CRT dalam Pengamanan Citra

Rani Lestari*, Relita Buaton, Imeldawaty Gultom****
*Teknik Informatika,STMIK Kaputama
**Teknik Informatika,STMIK Kaputama

Article Info
Article history:
Received Juli 1 th, 2021
Revised Juli 28 th, 2021
Accepted Juli 31 th, 2021

Keyword:
Citra
Kriptografi
One Time Pad
RSA CRT

ABSTRAK
Perkembangan teknologi seperti saat ini memungkinkan setiap orang untuk saling bertukar informasi tanpa ada batasan waktu dan jarak. Kemungkinan yang akan terjadi adanya kebocoran data pada saat proses pertukaran informasi yang dilakukan, oleh karena itu dalam pengiriman data khususnya citra, aspek keamanan, kerahasiaan dan efisiensi penyimpanan data sangat diperlukan. Citra ada yang bersifat rahasia ada yang tidak. Citra yang bersifat rahasia perlu mendapatkan pengamanan agar kerahasiaan gambar tidak diketahui oleh pihak yang tidak berwenang. Salah satu cara untuk melakukan pengamanan citra adalah dengan teknik kriptografi. Kriptografi citra merupakan ilmu dan seni untu menjaga keamanan citra dengan cara penyandian terhadap citra yang akan dikirim dari satu tempat ke tempat lain sehingga bentuk citra tidak dimengerti lagi maknanya. Dalam proses kriptografi banyak algoritma dan metode yang dapat digunakan untuk mengamankan suatu citra, yaitu seperti algoritma *One Time Pad* dan algoritma *RSA CRT* enkripsi citra dapat dilakukan dan semua citra berhasil dikembalikan ke bentuk citra asli. Dari penelitian ini dapat disimpulkan algoritma *one-time pad* dan *rsa crt* dapat digunakan untuk kriptografi citra dengan efektif.

Corresponding Author:
Nama : Rani Lestari
Teknik Informatika
STMIK Kaputama
Email: ranilestari678@gmail.com

1. PENDAHULUAN

Teknologi yang makin berkembang semakin memudahkan manusia untuk memenuhi kebutuhannya dalam hal komunikasi. Dahulu kala manusia harus melakukan perjalanan untuk berkomunikasi dengan orang lain di tempat yang berbeda. Namun pada masa kini manusia bisa dengan mudah berkomunikasi dengan orang lain melalui internet. Dengan hadirnya internet, informasi dapat dengan mudahnya menyebar ke seluruh penjuru dunia hanya dalam hitungan detik. Internet sebagai jalan raya informasi *(the information highway)* telah banyak dirasakan membawa perubahan pada banyak aspek dalam kehidupan manusia.

Pengamanan citra dengan menggunakan algoritma OTP dimana citra yang digunakan adalah citra yang berwarna (*color*) dan citra hitam putih (*grayscale*) dimana penelitian ini mempunyai kelemahan citra yang diamankan hanya berekstensi bmp saja [1]. Penelitian ini membahas tentang mengenkripsi pesan di hp android dengan menggunkan algoritma RSA CRT dimana mempunyai kelemahan proses mengenkrip pesan akan lama jika spesifikasi rendah [2]. Penyisipan pesan dan ektraksi, pesan data tersebut sulit dihitung secara manual sehingga dibutuhkan perhitungan secara komputasi melalui program namun memiliki kelemahan yaitu Untuk pembangkitan bilangan acak perlu dikembangkan dengan metode lain agar pengacakannya lebih baik tanpa harus berulang pada periode tertentu [3].

Namun internet juga merupakan salah satu jaringan publik yang tidak aman. Kegiatan-kegiatan transaksi informasi tersebut tentu saja akan menimbulkan resiko apabila informasi yang sensitif dan berharga tersebut diaksesoleh orang-orang yang tidak berhak *(unauthorized persons)*, misalnya pesan berupa data teks atau citra yang besifat pribadi dan rahasia. Setiap orang yang mengirimkan pesan tentu berkeinginan pesan yang dikirimkan akan aman. Aman dalam artian aman dari ancaman orang yang tidak berhak. Berbagai ancaman yang mungkin terjadi antara lain tidak sampainya citra, tersadapnya citra, citra yang dimanipulasi,

hingga penyamaran dan penyangkalan karena ada pihak yang mengirimkan citra dengan identitas orang lain. Tanpa fasilitas keamanan yang baik, sang penerima akan menerima citra tersebut tanpa mencurigai adanya perubahan yang dapat merugikan baik bagi pengirim maupun penerima. Untuk itu diperlukan sistem pengamanan yang dapat melindungi citra yang ditransmisikan melalui suatu jaringan komunikasi.
Algoritma RSA CRT merupakan algoritma kriptografi kunci publik yangterkenal aman karena sulitnya memecahkan fungsi matematis yang dipakaisebagai dasar pembuatan algoritmanya. Sedangkan algoritma OTP merupakan suatu metode yang sangat kuat, kunci yang digunakan adalah *session key*,dimana kunci hanya berlaku untuk satu kali proses enkripsi. Metode ini sangat baik untuk mengirim citra karena akan semakin sulit untuk mengetahui kunci yang digunakan.

Berdasarkan latar belakang di atas, maka rumusan masalah yang dibahas pada penelitian ini adalah bagaimana menerapkan teknik penyandian citra menggunakan kombinasi metode algoritma OTP dan algoritma RSA CRT dalam pengamanan citra. Tujuan Penelitian ini adalah untuk menerapkan penyandian citra menggunakan kombinasi metode algoritma OTP dan algoritma RSA CRT, sehingga dapat mengamankan citra dari pihak-pihak yang tidak bertanggung jawab.

2. METODE PENELITIAN

2.1. Pengertian Kriptografi

Kriptografi (*cryptography*) berasal dari bahasa Yunani yang terdiri dari dua suku kata, yaitu *cryptós* yang berarti rahasia dan *gráphein* yang berarti kata tulisan. Karena itu secara umum kriptografi diartikan sebagai tulisan rahasia.Terdapat beberapa definisi kriptografi dalam berbagai literatur. Definisi pada tahun 80-anmenyatakan kriptografi adalah ilmu dan seni untuk menjaga keamanan pesan. Kata seni dalam definisi ini berasal dari fakta sejarah bahwa pada awal sejarah kriptografi, setiap orang mempunyai cara yang unik untuk merahasiakan pesan[4].

Sedangkan definisi dalam buku-buku terbaru menyatakan kriptografi merupakan ilmu mengenai metode untuk mengirimkan pesan secara rahasia sehingga hanya penerima yang dimaksud yang dapat menghapus dan membaca pesan tersebut atau memahaminya. Pengertian lain kriptografi yaitu ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan, integritas data, serta otentikasi. Kata *graphy* dalam kata *cryptography* itu sendiri sudah menyiratkan sebuah seni.

Jadi, kriptografi adalah suatu ilmu sekaligus seni yang bertujuan untuk menjaga keamanan suatu pesan (*cryptography is the art and science of keeping messages secure*). Secara umum, kriptografi adalah teknik pengamanan informasi dimana informasi diubah dengan kunci tertentu melalui enkripsi sehingga menjadi informasi baru yang tidak dapat dimengerti oleh orang yang tidak berhak menerimanya, dan informasi tersebut hanya dapat di ubah kembali oleh orang yang berhak menerimanya melalui dekripsi.

2.2. Algoritma One Time Pad

One Time Pad merupakan salah satu algoritma yang populer dan sering digunakan dalam teknik kriptografi. OTP termasuk kelompok algoritma yang simetris dalam kriptografi dimana kunci enkripsi dan dekripsi dalam bentuk dan panjang yang sama, serta menggunakan operasi XOR. Keunggulan OTP adalah sangat sulit untuk dipecahkan tapi memiliki kekurangan dimana kunci yang digunakan kadang terlalu panjang karena harus menyesuaikan jumlah karakter yang akan dienkripsi.Dari semua metode kriptografi yang telah dirancang, OTP adalah metode yang telah terbukti benar-benar aman secara matematis.One Time Pad bisa dikatakan jika memenuhi kondisi berikut kunci harus sepanjang plainteks, kunci harus acak seluruhnya atau sepenuhnya berbeda, kunci hanya sekali digunakan setiap melakukan enkripsi, danhanya terdapat dua salinan dari kunci: satu untuk pengirim dan satu untuk penerima [1].

Algoritma *One Time Pad* mempunyai cara kerja dimana penerima pesanmempunya salinan kunci yang sama dan kuncitersebut hanya dipakai satu kali (*one time*)untuk enkripsi dan dekripsi dan setelahdigunakan maka pad (kertas *blocknot*)harussegera dihancurkan agar tidak bisa dipakai lagi untuk enkripsi dan dekripsi pesan yanglain.Pengirim dan penerima harus sama sama memiliki satu set materi kunci yang besar dan juga acak, selama kombinasi dari semua pesan yang pernah dikirimkan [5].

Jadi secara teori alasan OTP tidak dapat dipecahkan jika kuncinya secara sempurna diacak, dirahasiakan dan hanya dipakai sekali saja. Pada algoritma OTP mempunyai panjang kunci yang sama dengan panjang *plaintext.*Sehingga tidak ada kebutuhan untuk mengulang penggunaaan kunci selama proses enkripsi. Pada algoritma OTP mempunyai panjang kunci yang sama dengan panjang *plaintext.* Sehingga tidak ada kebutuhan untuk mengulang penggunaaan kunci selama proses enkripsi [5].

Teknik Enkripsi pada Algoritma One Time Pad

$Ci = (Pi + Ki) \bmod 256$

Keterangan :

Ci = Cipherteks (Ciphertext)

Pi = Plainteks (Plaintext)

Ki = kunci (Key)

Teknik Dekripsi Pada Algoritma One Time Pad

Ci=(Pi – Ki) mod 256

Keterangan :

Ci = Cipherteks (Ciphertext)

Pi = Plainteks (Plaintext)

Ki = kunci (Key)

2.3. Algoritma RSA CRT (Chinese Remainder Theorem)

Algoritma RSA with CRT adalah algoritma kunci asimetris yang diusulkan oleh Quisquarter & Couvreur pada tahun 1982. Algoritma ini merupakan varian dari RSA berdasarkan *Chinese Remainder Theorem* (CRT). Pada teknik ini dua kunci rahasia yang sangat kecil (dP, dQ) menghitung dari kunci rahasia asli (d), dekripsi dilakukan dengan dua buah kunci dan hasilnya digabungkan dengan bantuan dari *Chinese Remainder Theorem* (CRT). Algoritma kriptografi RSA with CRT dapat mempercepat kerja kunci dekripsi, untuk meningkatkan kinerja dari algoritma dekripsi dasar RSA [6].

Chinese Remainder Theorem (CRT)

Chinese Remainder Theorem adalah teorema mengenai kekongruenan lanjar dalam teori bilangan bulat yaitu aritmatika modulo. Teorema ini pertama kali di temukan oleh Sun Tze. Misalkan $m_1, m_2, ..., m_n$ adalah bilangan bulat positif sedemikian sehingga FPB(m_i, m_j)= 1 untuk i ≠ j. Maka sistem kongeruen lanjar $x = a_k \pmod{m_k}$ mempunyai solusi untuk modulo $m= m_1.m_2. ... .m_n$[3].

Pembangkit Kunci RSA-CRT

Pada Pembangkitan kunci RSA-CRT eksponen deskripsi *d* tidak secara langsung diberikan pada kunci privat namun dapat dihitung melalui parameter dP, dQ, dan qInv yang memiliki ukuran setengah dari panjang *n* bit *d*. Algoritma pembangkit kunci RSA-CRT adalah sebagai berikut :

1. Pilih dua buah bilangan prima yang berbeda *p* dan *q*
2. Hitung n = p.q (Sebaiknya p ≠ q, sebab jika p = q maka $n = p^2$ sehingga p dapat diperoleh dengan menarik akar pangkat dua dari n)
3. Hitung Øn = (p − 1)(q − 1)
4. Pilih bilangan integer *e* dimana $1 < e < \phi(N)$ dan $\gcd(e,\ \phi(N)) = 1$
5. Yaitu e dan $\phi(N)$ adalah relatif prima
6. Tentukan *d* sebagai $d^{-1} \equiv e\ (mod\ \phi(N))$, yaitu d adalah perkalian inverse dari $e\ (modulo\ \phi(N))$
7. dP = d mod (p - 1)
8. dQ = d mod (q – 1)
9. qInv = q^{-1} pada Z_p

K_{publik} = (e,n), K_{privat} = (dP, dQ, qInv,p,q)

Teknik Enkripsi Pada Algoritma RSA-CRT

Kunci publik RSA-CRT sama dengan sistem RSA yaitu (e) sehingga algoritma enkripsi tidak mengalami perubahan yaitu dengan menggunakan fungsi eksponensial modular yaitu seperti terlihat pada rumus berikut :

$c_i = m_i^e \bmod n$

Dimana :

- $\boldsymbol{c_i}$ = chipertext
- $\boldsymbol{m_i}$ = plaintext
- $\boldsymbol{e}$,$\boldsymbol{n}$ = kunci publik

Teknik Dekripsi Pada Algoritma RSA-CRT

Pada proses dekripsi berdasarkan penyelesaian persoalan CRT, d dapat dihitung kembali sehinggamemulihkan teks sandi untuk mendapatkan kembali teks asli. dengan menggunakan fungsi sebagai berikut :

$m_1 = c_i^{dP} \bmod p$
$m_2 = c_i^{dQ} \bmod q$
$h = qlnv.(m_1 - m_2) mod\ p$
$m_1 = m_2 + h\,.q$

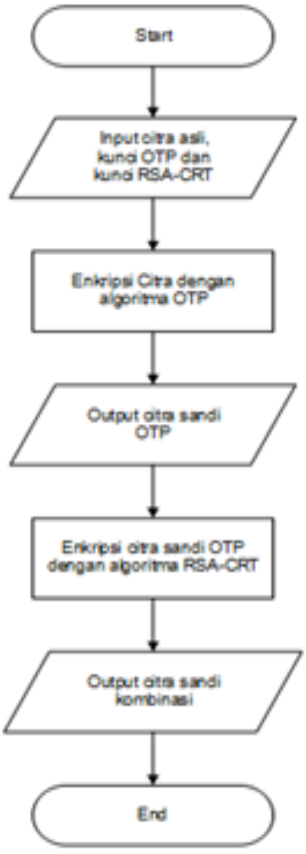
Dimana :

$- m_i = plaintext$
$- c_i = chipertxt$
$- \boldsymbol{dp, dQ, p, q,}$ **dan qlnv = kunci privat**

3. ANALISA DAN HASIL

3.1. Flowchart Sistem Enkripsi OTP dan RSA CRT

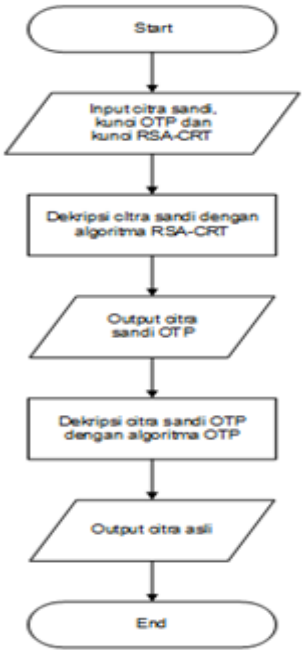
Berikut ini gambar dari *flowchart* sistem enkripsi OTP dan RSA CRT.



Gambar 1. Flowchart Sistem Enkripsi OTP Dan RSA CRT

3.2. Flowchart Sistem Dekripsi OTP dan RSA CRT

Berikut ini gambar dari *flowchart* sistem Dekripsi OTP dan RSA CRT.



Gambar 2. Flowchart Sistem Dekripsi OTP Dan RSA CRT

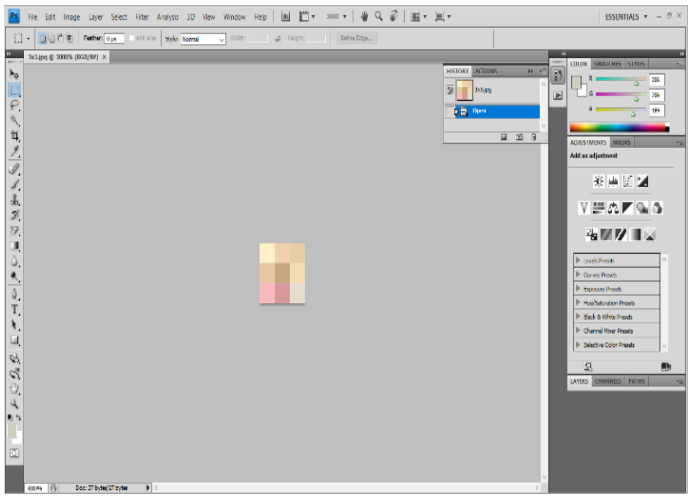
3.3. Perhitungan Enkripsi Citra Algoritma OTP

Pada Analisis perhitungan algoritma OTP akan dimulai dengan proses mengkonversikan citra Selanjutnya analisis perhitungan algoritma OTP akan dimulai dengan proses enkripsi sehingga citra yang diinginkan diamankan menjadi tidak diketahui isinya, kemudian akan di dekripsikan kembali untuk mengembalikan citra menjadi bentuk asli, sehingga kembali dapat dilihat isinya.

Adapun gambar yang dipilih untuk mengambil nilai matriks sebagai berikut :

Gambar 3. Citra Format jpg

Gambar 3 merupakan gambar yang akan dilakukan enkripsi, untuk mencari nilai dari pixelnya dengan cara menggunakan software tambahan photoshop ukuran foto tersebut 3x3



Gambar 4. Ukuran 3X3

Dari piksel-piksel citra asli dilakukan perhitungan dengan algoritma OTP dengan mengggunakan :

Kunci = nH3c8

Dimana mencari Enkripsi adalah dengan rumus :

Ci = (Pi + Ki) mod 256

Maka proses enkripsi citra dengan algoritma OTP Sebagai Berikut :

Kunci = nH3c8

pixel (0,0) =

Red = (255 + 110) Mod 256 = 109

Green = (240 + 72) Mod 256 = 56

Blue = (202 + 51) Mod 256 = 253

pixel (0,1) =

Red = (232 + 99) Mod 256 = 75

Green = (200 + 56) Mod 256 = 0

Blue = (162 + 110) Mod 256 = 16

pixel (0,2) =

Red = (248 + 72) Mod 256 = 64

Green = (186 + 51) Mod 256 = 237

Blue = (189 + 99) Mod 256 = 32

pixel (1,0) =

Red = (241 + 56) Mod 256 = 41

Green = (209 + 110) Mod 256 = 63

Blue = (171 + 72) Mod 256 = 243

pixel (1,1) =

Red = (198 + 51) Mod 256 = 249

Green = (166 + 99) Mod 256 = 9

Blue = (128 + 56) Mod 256 = 184

pixel (1,2) =

Red = (214 + 110) Mod 256 = 68

Green = (152 + 72) Mod 256 = 224

Blue = (155 + 51) Mod 256 = 206

pixel (2,0) =

Red = (231 + 99) Mod 256 = 74

Green = (206 + 56) Mod 256 = 6

Blue = (166 + 110) Mod 256 = 20

pixel (2,1) =

Red = (243 + 72) Mod 256 = 59

Green = (218 + 51) Mod 256 = 13

Blue = (178 + 99) Mod 256 = 21

pixel (2,2) =

Red = (227 + 56) Mod 256 = 27

Green = (221 + 110) Mod 256 = 75

Blue = (205 + 72) Mod 256 = 21

3.4. Perhitungan Enkripsi Citra Algoritma RSA CRT

Dari hasil enkripsi citra dengan algoritma OTPdilakukan kembali perhitungan dengan algoritma RSA-CRT:

p = 29
q = 17
n = p x q = 29 x 17 = 493
t(n) = (p - 1) x (q - 1) = (29 - 1) x (17 - 1) = 448
dp = 71
dq = 79
Cari nilai e =
e x d mod t(n) = 1
e x 15 mod 448 = 1
239 x 15 mod 448 = 1
3585 mod 448 = 1
1 = 1
maka e = 239
Cari nilai d =
d mod (p-1) = dp mod (p-1) dan d mod (q-1) = dq mod (q-1)
d mod (29-1) = 71 mod (29-1) dan d mod (17-1) = 79 mod (17-1)
15 mod (28) = 71 mod (28) dan 15 mod (16) = 79 mod (16)
15 = 15 dan 15 = 15
maka d = 15
Kunci Public yaitu : E = 239 N = 493
Kunci Private yaitu : D = 15 N = 493
Dimana mencari Enkripsi adalah dengan rumus :

$$Ci = Pi^{E} \bmod N$$

Maka proses enkripsi citra dengan algoritma RSA-CRT Sebagai Berikut :
pixel (0,0) =
Red = (109 ^ 239) mod 493 = 22
Green = (56 ^ 239) mod 493 = 466

Blue = (253 ^ 239) mod 493 = 8
pixel (0,1) =
Red = (75 ^ 239) mod 493 = 447
Green = (0 ^ 239) mod 493 = 0
Blue = (16 ^ 239) mod 493 = 16
pixel (0,2) =
Red = (64 ^ 239) mod 493 = 412
Green = (237 ^ 239) mod 493 = 237
Blue = (32 ^ 239) mod 493 = 229
pixel (1,0) =
Red = (41 ^ 239) mod 493 = 481
Green = (63 ^ 239) mod 493 = 469
Blue = (243 ^ 239) mod 493 = 279
pixel (1,1) =
Red = (249 ^ 239) mod 493 = 99
Green = (9 ^ 239) mod 493 = 444
Blue = (184 ^ 239) mod 493 = 164
pixel (1,2) =
Red = (68 ^ 239) mod 493 = 425
Green = (224 ^ 239) mod 493 = 414
Blue = (206 ^ 239) mod 493 = 26
pixel (2,0) =
Red = (74 ^ 239) mod 493 = 190
Green = (6 ^ 239) mod 493 = 122
Blue = (20 ^ 239) mod 493 = 397
pixel (2,1) =
Red = (59 ^ 239) mod 493 = 117
Green = (13 ^ 239) mod 493 = 361
Blue = (21 ^ 239) mod 493 = 472
pixel (2,2) =
Red = (27 ^ 239) mod 493 = 437
Green = (75 ^ 239) mod 493 = 447
Blue = (21 ^ 239) mod 493 = 472

3.5. Perhitungan Dekripsi Citra Algoritma RSA CRT

Selanjutnya mendekripsikan dengan algoritma RSA-CRT dengan melakukan perhitungan dengan rumus sebagai berikut :

$$\mathbf{Pi = Ci^{D} \bmod N}$$

Maka proses dekripsi citra dengan algoritma RSA-CRT Sebagai Berikut :

Kunci Private yaitu : D = 15 N = 493

pixel (0,0) =

Red = (22 ^ 15) mod 493 = 109

Green = (466 ^ 15) mod 493 = 56

Blue = (8 ^ 15) mod 493 = 253

pixel (0,1) =

Red = (447 ^ 15) mod 493 = 75

Green = (0 ^ 15) mod 493 = 0

Blue = (16 ^ 15) mod 493 = 16

pixel (0,2) =

Red = (412 ^ 15) mod 493 = 64

Green = (237 ^ 15) mod 493 = 237

Blue = (229 ^ 15) mod 493 = 32

pixel (1,0) =

Red = (481 ^ 15) mod 493 = 41

Green = (469 ^ 15) mod 493 = 63

Blue = (279 ^ 15) mod 493 = 243

pixel (1,1) =

Red = (99 ^ 15) mod 493 = 249

Green = (444 ^ 15) mod 493 = 9

Blue = (164 ^ 15) mod 493 = 184

pixel (1,2) =

Red = (425 ^ 15) mod 493 = 68

Green = (414 ^ 15) mod 493 = 224

Blue = (26 ^ 15) mod 493 = 206

pixel (2,0) =

Red = (190 ^ 15) mod 493 = 74

Green = (122 ^ 15) mod 493 = 6

Blue = (397 ^ 15) mod 493 = 20

pixel (2,1) =

Red = (117 ^ 15) mod 493 = 59

Green = (361 ^ 15) mod 493 = 13

Blue = (472 ^ 15) mod 493 = 21

pixel (2,2) =

Red = (437 ^ 15) mod 493 = 27

Green = (447 ^ 15) mod 493 = 75

Blue = (472 ^ 15) mod 493 = 21

3.6. Perhitungan Dekripsi Citra Algoritma OTP

Selanjutnya mendekripsikan dengan algoritma RSA-CRT dengan melakukan perhitungan dengan rumus sebagai berikut :

$$\mathbf{Pi = Ci^{D} \bmod N}$$

Maka proses dekripsi citra dengan algoritma RSA-CRT Sebagai Berikut :

Kunci Private yaitu : D = 15 N = 493

Kunci = nH3c8

pixel (0,0) =

Red = (109 - 110) Mod 256 = 255

Green = (56 - 72) Mod 256 = 240

Blue = (253 - 51) Mod 256 = 202

pixel (0,1) =

Red = (75 - 99) Mod 256 = 232

Green = (0 - 56) Mod 256 = 200

Blue = (16 - 110) Mod 256 = 162

pixel (0,2) =

Red = (64 - 72) Mod 256 = 248

Green = (237 - 51) Mod 256 = 186

Blue = (32 - 99) Mod 256 = 189

pixel (1,0) =

Red = (41 - 56) Mod 256 = 241

Green = (63 - 110) Mod 256 = 209

Blue = (243 - 72) Mod 256 = 171

pixel (1,1) =

Red = (249 - 51) Mod 256 = 198

Green = (9 - 99) Mod 256 = 166

Blue = (184 - 56) Mod 256 = 128

pixel (1,2) =

Red = (68 - 110) Mod 256 = 214

Green = (224 - 72) Mod 256 = 152

Blue = (206 - 51) Mod 256 = 155

pixel (2,0) =

Red = (74 - 99) Mod 256 = 231

Green = (6 - 56) Mod 256 = 206

Blue = (20 - 110) Mod 256 = 166

pixel (2,1) =

Red = (59 - 72) Mod 256 = 243

Green = (13 - 51) Mod 256 = 218

Blue = (21 - 99) Mod 256 = 178

pixel (2,2) =

Red = (27 - 56) Mod 256 = 227

Green = (75 - 110) Mod 256 = 221

Blue = (21 - 72) Mod 256 = 205

4. KESIMPULAN

Berdasarkan hasil perancangan dan pembuatan program aplikasi kriptografi menggunakan metode OTPdan RSA-CRTini dapat di ambil kesimpulan sebagai berikut :

1. Aplikasi pengamanan citramenggunakan algoritma OTP dan RSA-CRT mempunyai dua teknik pembacaan yaitu teknik enkripsi mengubah *file* asli menjadi *file* yang tidak dapat dibaca dan teknik dekripsi mengubah *file* yang tidak dapat dibaca menjadi *file*asli.
2. Aplikasi pengamanan mempunyai kalmiat sandi atau *passphare* yang harus diingat dan bersifat sensitif, maksudnya huruf besar dan kecil dibedakan,agar *passphare* sulit ditebak oleh siapapun.

3. Pengamanan citra dengan menggunakan algoritma OTP dan RSA-CRT untuk merahasiakan citra berjalan dengan baik. citra berhasil di enkripsi dan di dekripsi, percobaan yang dilakukan pada algoritma OTP dan RSA-CRT waktu proses yang di hasilkan dekripsi lebih cepat dibandingkan hasil enkripsi.

REFERENSI

[1] D. R. I. M. Setiadi, E. H. Rachmawanto, and C. A. Sari, "Implementasi One Time Pad Kriptografi Pada Gambar Grayscale Dan Gambar Berwarna," *Pros. Semin. Nas. Multi Disiplin Ilmu Call Pap. Unisbank Ke-3(Sendi_U 3)*, pp. 50–56, 2017.

[2] R. Herteno, "Steganografi Untuk Pesan Terenskripsi Menggunakan Agoritma," 2019.

[3] N. R. Nasution, "Kombinasi RSA-CRT dengan Random LSB untuk Keamanan Data," vol. 5341, no. April, pp. 32–42, 2017.

[4] A. P. N. Nurdin, "Analisa Dan Implementasi Kriptografi Pada Pesan Rahasia," *Jesik*, vol. 3, no. 1, pp. 1–11, 2017, [Online]. Available: nnurdin69@gmail.com.

[5] A. Fauzi, Y. Maulita, and Novriyenni, "Perancangan Aplikasi Keamanan Pesan Menggunakan Algoritma Elgamal Denganmemanfaatkan Algoritma One Time Pad Sebagai Pembangkit Kunci," *J. Tek. Inform. Kaputana*, vol. 1, no. 1, pp. 1–9, 2017.

[6] D. Garg and S. Verma, "Improvement over public key cryptographic algorithm," *2009 IEEE Int. Adv. Comput. Conf. IACC 2009*, pp. 734–739, 2009, doi: 10.1109/IADCC.2009.4809104.

BIBLIOGRAFI PENULIS

	Rani Lestari, dilahirkan di Kabupaten Langkat tepatnya di Dusun Teladan Desa Pantai Cermin Kecamatan Tanjung Pura pada hari Selasa tanggal 27 Januari 1998. Putrid dari pasanga Parino dan Sri Wati dan merupakan anak pertama dari dua bersaudara. Penulis memulai pendidikan formal di SD Negeri 056020 Pematang Rambai pada tahun 2004 hingga 2010 dan melanjutkan pendidikan di SMP Negeri 3 Tanjung Pura pada tahun 2010 hingga 2013, kemudian penulis melanjutkan pendidikan di SMK Negeri 1 Tanjung Pura pada tahun 2013 dan tamat pada tahun 2016. Ditahun yang sama penulis terdaftar sebagai mahasiswi pada program studi Teknik Informatika, program Strata Satu (S1) di STMIK Kaputama Binjai.
Second author's photo(3x4cm)	Relita Buaton, ST., M.Kom
Thirth author's photo(3x4cm)	Imeldawaty Gultom, S.Kom.,M.Pd