**IJCIT (Indonesian Journal on Computer and Information Technology)**
Vol.3, No.2, November 2018, pp. 243~252
p-ISSN: 2527-449X, e-ISSN**:** 2549-7421

Diterima Oktober 23, 2018; Revisi November 1, 2018; Disetujui November 5, 2018

# Komparasi Algoritma Kriptografi Elgamal Dan Caesar Cipher Untuk Enkripsi Dan Dekripsi Pesan

**Ai Ilah Warnilah[1], Siti Nurhasanah Nugraha[2]**

[1]Universitas Bina Sarana Informatika PSDKU Tasikmalaya
ai.aiw@bsi.ac.id

[2] Universitas Bina Sarana Informatika PSDKU Tasikmalaya
sitinurh1711@bsi.ac.id

**Abstrak**

Pesatnya perkembangan teknologi informasi telah menjadikan informasi sebagai kebutuhan pokok bagi setiap orang. Seiring berkembangnya teknologi, keamanan terhadap kerahasiaan akan data dan informasi yang dipertukarkan akan semakin meningkat. Saat ini keamanan dalam pertukaran informasi masih kurang terjaga. Permasalahan yang terjadi pada proses pertukaran informasi yang bersifat rahasia, seringkali infromasi tersebut tersebar luas karena adanya penyadapan, pencurian, dan pemalsuan informasi, yang akan menyebabkan kerugian bagi pemilik informasi. Penerapan algoritma kriptografi ElGamal dan caesar cipher adalah salah satu cara efektif dalam pertukaran informasi agar tetap terjaga kerahasiaannya. Keamanan algoritma ini terletak pada sulitnya menghitung logaritma diskrit. Algoritma caesar cipper merupakan sistem persandian klasik berbasis subtitusi yang sederhana pada enkripsi dan dekripsi sebuah sistem persandian caesar menggunakan operasi shift. Adapun hasil dari penelitian ini adalah terciptanya sebuah aplikasi untuk proses enkripsi pesan asli menjadi pesan yang tidak dapat terbaca agar pesan yang akan dikirim tetap terjaga kerahasiaannya dan mengembalikannya dengan proses dekripsi untuk proses penerimaan atau pembacaan pesan oleh penerima.
**Kata Kunci**: caesar cipher, dekripsi, elgamal, enkripsi, kriptografi

***Abstract***

*The rapid development of information technology has made information as a basic need for everyone. As technology develops, security for confidentiality of data and information exchanged will increase. At present security in information exchange is still not maintained. The problems that occur in the process of exchanging information that are confidential, often the information is widespread because of wiretapping, theft, and falsification of information, which will cause harm to the information owner. The application of ElGamal cryptographic algorithm and caesarean cipher is one of the effective ways to exchange information to maintain its confidentiality. The security of this algorithm lies in the difficulty of calculating discrete logarithms. The cipper caesar algorithm is a simple substitution based coding system for encryption and decryption of a cesarean coding system using shift operations. The results of this study are the creation of an application for the encryption process of the original message into an unreadable message so that the message to be sent is kept confidential and returns it with the decryption process for receiving or reading the message by the recipient.*
***Keywords****: caesar cipher, cryptographic, decryption, elgamal, encryption*

## 1. Pendahuluan

Pesatnya perkembangan teknologi informasi telah menjadikan informasi sebagai kebutuhan pokok bagi setiap orang, sehingga keamanan terhadap kerahasiaan akan data dan informasi yang dipertukarkan akan semakin meningkat. Kerahasiaan pesan atau data yang dimiliki oleh seseorang merupakan hal penting dalam pengiriman pesan agar pesan tersebut hanya dapat diberikan oleh orang tertentu saja yang dapat mengakses informasi tersebut.

Di jaman yang serba canggih seperti ini alat untuk mengirim pesan sudah banyak termasuk medianya seperti: facebook dan twitter sehingga kita bisa mengirim pesan dengan cepat begitu pun

sebaliknya kita bisa menerima pesan dengan cepat pula. Dari semua kemudahan itu tentu akan sangat berpengaruh ketika kita akan mengirim pesan yang isinya hanya orang-orang tertentu saja yang boleh mengetahui isinya. Salah satu yang harus benar-benar dijaga adalah pesan yang bersifat rahasia karena jika pesan itu tersebar maka akan berdampak buruk pada kita.

Salah satu cara untuk mengamankan data atau informasi dari tindak kejahatan adalah menggunakan konsep kriptografi. Kriptografi adalah suatu ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamana informasi, integritas suatu data, serta autentikasi data. Algoritma kripografi yang akan digunakan untuk menyelesaikan masalah pengamanan informasi atau data yaitu dengan menggunakan metode kriptografi ElGamal dan metode kriptografi caesar cipher.

Algoritma ElGamal merupakan algoritma dalam kriptografi yang termasuk dalam kategori algoritma asimetris (kunci enkripsi dan dekripsinya berbeda). Algoritma Elgamal dipilih dalam teknik kriptografi untuk pengamanan informasi atau data ini karena algoritma elgamal dalam mengamankan pesan rahasia membutuhkan pembentukan kunci dengan menggunakan bilangan prima dan pemecahan masalahnya menggunakan logaritma diskrit yang cukup sulit untuk diselesaikan.

Algoritma *caesar chiper* adalah teknik kriptografi yang dilakukan dengan mensubtitusi setiap abjad dari pesan yang akan dienkripsi melalui pergeseran susunan sebagai kuncinya. *Caesar Cipher* merupakan salah satu algoritma *cipher* tertua dan paling diketahui dalam perkembangan ilmu kriptografi. *Caesar cipher* merupakan salah satu jenis *cipher* substitusi yang membentuk *cipher* dengan cara melakukan penukaran karakter pada *plainteks* menjadi tepat satu karakter pada *chiperteks*.

## 2. Metode Penelitian

Metode penelitian yang digunakan untuk pemecahan masalah pengamanan pesan yaitu metode kriptografi elgamal dan metode caesar cipher.

### A. Algoritma Kriptografi ElGamal

Algoritma ElGamal ditemukan pada tahun 1985 oleh ilmuwan Mesir yaitu Taher ElGamal. Algoritma ElGamal merupakan algoritma berdasarkan konsep kunci publik. Algoritma ini pada umumnya digunakan untuk digital signature, namun kemudian dimodifikasi sehingga bisa digunakan untuk enkripsi dan dekripsi.

Algoritma kriptografi kunci publik ElGamal merupakan algoritma blok chipper yaitu algoritma yang melakukan proses enkripsi pada blok-blok plainteks yang kemudian menghasilkan blok-blok chipertext, yang nantinya blok-blok chipertext tersebut akan didekripsi kembali dan hasilnya kemudian digabungkan menjadi plainteks semula.

Keamanan algoritma ElGamal terletak pada kesulitan perhitungan logaritma diskrit pada modulo prima yang besar, sehingga upaya untuk menyelesaikan masalah logaritma ini menjadi sulit untuk dipecahkan.

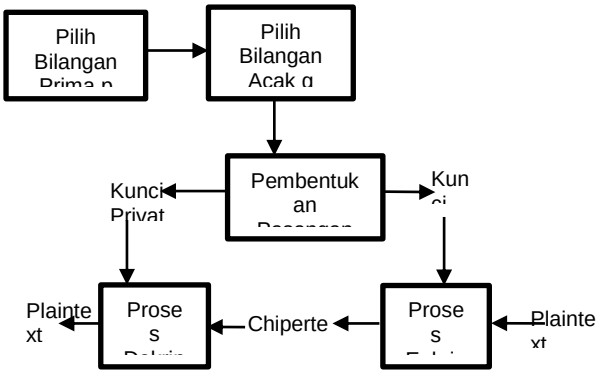
Algoritma ini memiliki kelebihan yaitu pembangkitan kunci yang menggunakan logaritma diskrit dan metode enkripsi dekripsi yang menggunakan proses komputasi yang besar sehingga hasil enkripsinya berukuran dua kali dari ukuran semula. Kekurangan algoritma ini adalah membutuhkan resource yang besar karena chipertext yang dihasilkan dua kali panjang plaintext serta membutuhkan processor yang mampu untuk melakukan komputasi yang besar untuk perhitungan logaritma perpangkatan besar.

Untuk proses dekripsi, algoritma ini membutuhkan waktu yang lebih lama karena kompleksitas proses dekripsinya yang rumit. Dibutuhkan dua kali komputasi karena ukuran chiperteks yang lebih besar dibandingkan plainteksnya.

Langkah–langkah penyelesaian metode kriptografi elgamal adalah sebagai berikut:

a. Pilih sembarang bilangan prima *p,* dengan syarat p
b. Pilih 2 bilangan acak, *g* dan *x* dimana $g < p$ dan $1 \leq x \leq p-2$
c. Pembentukan pasangan kunci, yang terdiri dari kunci publik dan kunci private
d. User memasukkan *plaintext* yang akan dienkripsi
e. Proses enkripsi menggunakan kunci publik
f. Hasil proses enkripsi berupa *chipertext*

g. Untuk memperoleh *plaintext* kembali, dilakukan dekripsi terhadap *plaintext* menggunakan kunci *private*




**Gambar 1.** Tahapan Penyelesaian Algoritma ElGamal

**B. Algoritma Kriptografi Caesar Cipher**

*Caesar Cipher* merupakan salah satu algoritma *cipher* tertua dan paling diketahui dalam perkembangan ilmu kriptografi. *Caesar cipher* merupakan salah satu jenis cipher substitusi yang membentuk cipher dengan cara melakukan penukaran karakter pada plainteks menjadi tepat satu karakter pada chiperteks. Teknik seperti ini disebut juga sebagai chiper abjad tunggal.Algoritma kriptografi *Caesar Cipher* sangat mudah untuk digunakan. Inti dari algoritma kriptografi ini adalah melakukan pergeseran terhadap semua karakter pada plainteks dengan nilai pergeseran yang sama. Adapun langkah-langkah yang dilakukan untuk membentuk chiperteks dengan *Caesar Cipher* adalah:

a. Menentukan besarnya pergeseran karakter yang digunakan dalam membentuk cipherteks ke plainteks
b. Menukarkan karakter pada plainteks menjadi cipherteks dengan berdasarkan pada pergeseran yang telah ditentukan sebelumnya.

Algoritma dari *Caesar Cipher* adalah C = E (P) = (P + K) mod 26 untuk fungsi enkripsi. Sedangkan untuk fungsi dekripsi adalah P = D (C) = (C - K) mod 26.

## 3. Hasil dan Pembahasan

### 3.1. Analisa Kriptografi ElGamal

Besar-besaran yang dibutuhkan untuk perhitungan algoritma ElGamal adalah sebagai berikut:

1. Bilangan prima, p (dimana p > 255 dan bersifat public atau tidak rahasia)
2. Bilangan acak, g (dimana g < p dan bersifat public atau tidak rahasia)
3. Bilangan acak, x (dimana $1 \leq x \leq p - 2$ dan bersifat private atau rahasia)
4. Bilangan acak, k (dimana k < p dan bersifat private atau rahasia)
5. m merupakan plainteks dan bersifat private/rahasia
6. a dan b merupakan pasangan chiperteks hasil enkripsi bersifat private atau tidak rahasia

**The ASCII code**

American Standard Code for Information Interchange

**www.theasciicode.com.ar**

**ASCII control characters**

| DEC | HEX | Simbolo ASCII | |
|---|---|---|---|
| 00 | 00h | NULL | (carácter nulo) |
| 01 | 01h | SOH | (inicio encabezado) |
| 02 | 02h | STX | (inicio texto) |
| 03 | 03h | ETX | (fin de texto) |
| 04 | 04h | EOT | (fin transmisión) |
| 05 | 05h | ENQ | (enquiry) |
| 06 | 06h | ACK | (acknowledgement) |
| 07 | 07h | BEL | (timbre) |
| 08 | 08h | BS | (retroceso) |
| 09 | 09h | HT | (tab horizontal) |
| 10 | 0Ah | LF | (salto de línea) |
| 11 | 0Bh | VT | (tab vertical) |
| 12 | 0Ch | FF | (form feed) |
| 13 | 0Dh | CR | (retorno de carro) |
| 14 | 0Eh | SO | (shift Out) |
| 15 | 0Fh | SI | (shift In) |
| 16 | 10h | DLE | (data link escape) |
| 17 | 11h | DC1 | (device control 1) |
| 18 | 12h | DC2 | (device control 2) |
| 19 | 13h | DC3 | (device control 3) |
| 20 | 14h | DC4 | (device control 4) |
| 21 | 15h | NAK | (negative acknowle.) |
| 22 | 16h | SYN | (synchronous idle) |
| 23 | 17h | ETB | (end of trans. block) |
| 24 | 18h | CAN | (cancel) |
| 25 | 19h | EM | (end of medium) |
| 26 | 1Ah | SUB | (substitute) |
| 27 | 1Bh | ESC | (escape) |
| 28 | 1Ch | FS | (file separator) |
| 29 | 1Dh | GS | (group separator) |
| 30 | 1Eh | RS | (record separator) |
| 31 | 1Fh | US | (unit separator) |
| 127 | 20h | DEL | (delete) |

**ASCII printable characters**

| DEC | HEX | Simbolo | DEC | HEX | Simbolo | DEC | HEX | Simbolo |
|---|---|---|---|---|---|---|---|---|
| 32 | 20h | espacio | 64 | 40h | @ | 96 | 60h | ` |
| 33 | 21h | ! | 65 | 41h | A | 97 | 61h | a |
| 34 | 22h | " | 66 | 42h | B | 98 | 62h | b |
| 35 | 23h | # | 67 | 43h | C | 99 | 63h | c |
| 36 | 24h | $ | 68 | 44h | D | 100 | 64h | d |
| 37 | 25h | % | 69 | 45h | E | 101 | 65h | e |
| 38 | 26h | & | 70 | 46h | F | 102 | 66h | f |
| 39 | 27h | ' | 71 | 47h | G | 103 | 67h | g |
| 40 | 28h | ( | 72 | 48h | H | 104 | 68h | h |
| 41 | 29h | ) | 73 | 49h | I | 105 | 69h | i |
| 42 | 2Ah | * | 74 | 4Ah | J | 106 | 6Ah | j |
| 43 | 2Bh | + | 75 | 4Bh | K | 107 | 6Bh | k |
| 44 | 2Ch | , | 76 | 4Ch | L | 108 | 6Ch | l |
| 45 | 2Dh | - | 77 | 4Dh | M | 109 | 6Dh | m |
| 46 | 2Eh | . | 78 | 4Eh | N | 110 | 6Eh | n |
| 47 | 2Fh | / | 79 | 4Fh | O | 111 | 6Fh | o |
| 48 | 30h | 0 | 80 | 50h | P | 112 | 70h | p |
| 49 | 31h | 1 | 81 | 51h | Q | 113 | 71h | q |
| 50 | 32h | 2 | 82 | 52h | R | 114 | 72h | r |
| 51 | 33h | 3 | 83 | 53h | S | 115 | 73h | s |
| 52 | 34h | 4 | 84 | 54h | T | 116 | 74h | t |
| 53 | 35h | 5 | 85 | 55h | U | 117 | 75h | u |
| 54 | 36h | 6 | 86 | 56h | V | 118 | 76h | v |
| 55 | 37h | 7 | 87 | 57h | W | 119 | 77h | w |
| 56 | 38h | 8 | 88 | 58h | X | 120 | 78h | x |
| 57 | 39h | 9 | 89 | 59h | Y | 121 | 79h | y |
| 58 | 3Ah | : | 90 | 5Ah | Z | 122 | 7Ah | z |
| 59 | 3Bh | ; | 91 | 5Bh | [ | 123 | 7Bh | { |
| 60 | 3Ch | < | 92 | 5Ch | \ | 124 | 7Ch | \| |
| 61 | 3Dh | = | 93 | 5Dh | ] | 125 | 7Dh | } |
| 62 | 3Eh | > | 94 | 5Eh | ^ | 126 | 7Eh | ~ |
| 63 | 3Fh | ? | 95 | 5Fh | _ | | | |

theASCIIcode.com.ar

**Extended ASCII characters**

| DEC | HEX | Simbolo | DEC | HEX | Simbolo | DEC | HEX | Simbolo | DEC | HEX | Simbolo |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 128 | 80h | Ç | 160 | A0h | á | 192 | C0h | └ | 224 | E0h | Ó |
| 129 | 81h | ü | 161 | A1h | í | 193 | C1h | ┴ | 225 | E1h | ß |
| 130 | 82h | é | 162 | A2h | ó | 194 | C2h | ┬ | 226 | E2h | Ô |
| 131 | 83h | â | 163 | A3h | ú | 195 | C3h | ├ | 227 | E3h | Ò |
| 132 | 84h | ä | 164 | A4h | ñ | 196 | C4h | ─ | 228 | E4h | õ |
| 133 | 85h | à | 165 | A5h | Ñ | 197 | C5h | ┼ | 229 | E5h | Õ |
| 134 | 86h | å | 166 | A6h | ª | 198 | C6h | ã | 230 | E6h | µ |
| 135 | 87h | ç | 167 | A7h | º | 199 | C7h | Ã | 231 | E7h | þ |
| 136 | 88h | ê | 168 | A8h | ¿ | 200 | C8h | ╚ | 232 | E8h | Þ |
| 137 | 89h | ë | 169 | A9h | ® | 201 | C9h | ╔ | 233 | E9h | Ú |
| 138 | 8Ah | è | 170 | AAh | ¬ | 202 | CAh | ╩ | 234 | EAh | Û |
| 139 | 8Bh | ï | 171 | ABh | ½ | 203 | CBh | ╦ | 235 | EBh | Ù |
| 140 | 8Ch | î | 172 | ACh | ¼ | 204 | CCh | ╠ | 236 | ECh | ý |
| 141 | 8Dh | ì | 173 | ADh | ¡ | 205 | CDh | ═ | 237 | EDh | Ý |
| 142 | 8Eh | Ä | 174 | AEh | « | 206 | CEh | ╬ | 238 | EEh | ¯ |
| 143 | 8Fh | Å | 175 | AFh | » | 207 | CFh | ¤ | 239 | EFh | ´ |
| 144 | 90h | É | 176 | B0h | ░ | 208 | D0h | ð | 240 | F0h | |
| 145 | 91h | æ | 177 | B1h | ▒ | 209 | D1h | Ð | 241 | F1h | ± |
| 146 | 92h | Æ | 178 | B2h | ▓ | 210 | D2h | Ê | 242 | F2h | ‗ |
| 147 | 93h | ô | 179 | B3h | │ | 211 | D3h | Ë | 243 | F3h | ¾ |
| 148 | 94h | ö | 180 | B4h | ┤ | 212 | D4h | È | 244 | F4h | ¶ |
| 149 | 95h | ò | 181 | B5h | Á | 213 | D5h | ı | 245 | F5h | § |
| 150 | 96h | û | 182 | B6h | Â | 214 | D6h | Í | 246 | F6h | ÷ |
| 151 | 97h | ù | 183 | B7h | À | 215 | D7h | Î | 247 | F7h | ¸ |
| 152 | 98h | ÿ | 184 | B8h | © | 216 | D8h | Ï | 248 | F8h | ° |
| 153 | 99h | Ö | 185 | B9h | ╣ | 217 | D9h | ┘ | 249 | F9h | ¨ |
| 154 | 9Ah | Ü | 186 | BAh | ║ | 218 | DAh | ┌ | 250 | FAh | · |
| 155 | 9Bh | ø | 187 | BBh | ╗ | 219 | DBh | █ | 251 | FBh | ¹ |
| 156 | 9Ch | £ | 188 | BCh | ╝ | 220 | DCh | ▄ | 252 | FCh | ³ |
| 157 | 9Dh | Ø | 189 | BDh | ¢ | 221 | DDh | ¦ | 253 | FDh | ² |
| 158 | 9Eh | × | 190 | BEh | ¥ | 222 | DEh | Ì | 254 | FEh | ■ |
| 159 | 9Fh | ƒ | 191 | BFh | ┐ | 223 | DFh | ▀ | 255 | FFh | |

**Gambar 2.** Tabel Kode ASCII

Contoh :
Siti akan mengirim pesan “Selamat PAGI” kepada Nunuy melalui Fitri. Siti tidak ingin pesan tersebut diketahui oleh Fitri. Maka Siti mengenkripsi pesan tersebut untuk sampai kepada Nunuy. Kemudian Siti memberikan pesan tersebut dan kunci pribadi *(private key)* untuk proses dekripsi kepada Nunuy melalui Fitri. Penyelesaian perhitungan manual enkripsi dengan Metode ElGamal:

a. Pembentukan Kunci
   Siti membangkitkan pasangan kunci dengan memilih bilangan :
   p = 787  g = 185  x = 32
   Kemudian p, g, x digunakan untuk menghitung y :
   $y = g^x \bmod p$
   $y = 185^{32} \bmod 787$
   y = 754

   jadi kunci public yang dimiliki Siti adalah y = 754, g = 185, p = 787 dan kunci private yang akan dikirim kepada Nunuy untuk proses dekripsi adalah adalah x =32, p = 787.

b. Enkripsi Pesan
   Nilai ASCII dari pesan “Selamat PAGI” adalah 83 101 108 97 109 97 116 32 80 65 71 73
   Kemudian nilai ASCII tersebut dimasukkan kedalam blok-blok nilai m secara berurutan, dengan perhitungan :

   1) Untuk $m_1 = 83$
      Generate k = 673, $1 \le k \le p - 2$
      $a = g^k \bmod p$
      $a = 185^{673} \bmod 787$
      a = 347

      $b = y^k * m \bmod p$
      $b = 754^{673} * 83 \bmod 787$
      b = 531

   2) Untuk $m_2 = 101$
      Generate k = 220, $1 \le k \le p - 2$
      $a = g^k \bmod p$
      $a = 185^{220} \bmod 787$
      a = 267

      $b = y^k * m \bmod p$
      $b = 754^{220} * 101 \bmod 787$
      b = 225

   3) Untuk $m_3 = 108$
      Generate k = 497, $1 \le k \le p - 2$
      $a = g^k \bmod p$
      $a = 185^{497} \bmod 787$
      a = 447

      $b = y^k * m \bmod p$
      $b = 754^{497} * 108 \bmod 787$
      b = 506

   4) Untuk $m_4 = 97$
      Generate k = 535, $1 \le k \le p - 2$
      $a = g^k \bmod p$
      $a = 185^{535} \bmod 787$
      a = 147

      $b = y^k * m \bmod p$
      $b = 754^{535} * 97 \bmod 787$
      b = 728

   5) Untuk $m_5 = 109$
      Generate k = 299, $1 \le k \le p - 2$
      $a = g^k \bmod p$
      $a = 185^{299} \bmod 787$
      a = 643

      $b = y^k * m \bmod p$
      $b = 754^{299} * 109 \bmod 787$
      b = 18

   6) Untuk $m_6 = 97$
      Generate k = 66, $1 \le k \le p - 2$
      $a = g^k \bmod p$
      $a = 185^{66} \bmod 787$
      a = 279

      $b = y^k * m \bmod p$
      $b = 754^{66} * 97 \bmod 787$
      b = 197

   7) Untuk $m_7 = 116$
      Generate k = 457, $1 \le k \le p - 2$
      $a = g^k \bmod p$
      $a = 185^{457} \bmod 787$
      a = 485

      $b = y^k * m \bmod p$
      $b = 754^{457} * 116 \bmod 787$
      b = 261

   8) Untuk $m_8 = 32$
      Generate k = 530, $1 \le k \le p - 2$
      $a = g^k \bmod p$
      $a = 185^{530} \bmod 787$
      a = 381

      $b = y^k * m \bmod p$
      $b = 754^{530} * 32 \bmod 787$
      b = 711

   9) Untuk $m_9 = 80$
      Generate k = 780, $1 \le k \le p - 2$
      $a = g^k \bmod p$
      $a = 185^{780} \bmod 787$

| Karakter (m) | ASCII | K (acak) | a = g^k mod p | b = y^k*m mod p | Cipher (a,b) |
|---|---|---|---|---|---|
| S | 83 | 673 | 347 | 531 | (347,531) |
| e | 101 | 220 | 267 | 225 | (267,225) |
| l | 108 | 497 | 447 | 506 | (447,506) |
| a | 97 | 535 | 147 | 728 | (147,728) |
| m | 109 | 299 | 643 | 18 | (643,18) |
| a | 97 | 66 | 279 | 197 | (279,197) |
| t | 116 | 457 | 485 | 261 | (485,261) |
| | 32 | 530 | 381 | 711 | (381,711) |
| P | 80 | 780 | 253 | 208 | (253,208) |
| a | 65 | 761 | 320 | 237 | (320,237) |
| g | 71 | 597 | 546 | 759 | (546,759) |
| i | 73 | 635 | 750 | 709 | (750,759) |

a = 253

b = $y^k$ * m mod p
b = $754^{780}$ * 80 mod 787
b = 208

10) Untuk $m_{10}$ = 65
Generate k = 761, 1 ≤ k ≤ p – 2
a = $g^k$ mod p
a = $185^{761}$ mod 787
a = 320

b = $y^k$ * m mod p
b = $754^{761}$ * 65 mod 787
b = 237

11) Untuk $m_{11}$ = 71
Generate k = 597, 1 ≤ k ≤ p – 2
a = $g^k$ mod p
a = $185^{597}$ mod 787
a = 546

b = $y^k$ * m mod p
b = $754^{597}$ * 71 mod 787
b = 759

12) Untuk $m_{12}$ = 73
Generate k = 635, 1 ≤ k ≤ p – 2
a = $g^k$ mod p
a = $185^{635}$ mod 787
a = 750

b = $y^k$ * m mod p
b = $754^{635}$ * 73 mod 787
b = 709

Setelah mendapatkan nilai a dan b, hasil perhitungan tersebut disusun dengan pola :

a1 b1, a2 b2, a3 b3, a4 b4, a5 b5, a6 b6, a7 b7, a8 b8, a9 b9, a10 b10, a11 b11, a12 b12.
Sehingga membentuk *chipertext* (pesan enkripsi yang dikirim) sebagai berikut:
347 531, 267 225, 447 506, 147 728, 643 18, 279 197, 485 261, 381 711, 253 208, 320 237, 546 759, 750 709.

**Tabel 1. Hasil Enkripsi ElGamal**

c. Dekripsi Pesan
Nunuy mendekripsikan pesan dari Siti dengan rumus :
mi = bi * $(a^x)^{-1}$ mod p dan kunci privat x=32 dan p=787

a. Cipher (a,b) = (347,531)
$(a^x)^{-1} = a^{p-1-x}$ mod p
$(a^x)^{-1} = 347^{787-1-32}$ mod 787
$(a^x)^{-1} = 347^{754}$ mod 787
$(a^x)^{-1}$ = 593

m = b * $(a^x)^{-1}$ mod p
m = 531 * 593 mod 787
m = 159075 mod 257
m = 83

b. Cipher (a,b) = (267,225)
$(a^x)^{-1} = a^{p-1-x}$ mod p
$(a^x)^{-1} = 267^{787-1-32}$ mod 787
$(a^x)^{-1} = 267^{754}$ mod 787
$(a^x)^{-1}$ = 707

m = b * $(a^x)^{-1}$ mod p
m = 225 * 707 mod 787
m = 81144 mod 257
m = 101

c. Cipher (a,b) = (447, 506)
$(a^x)^{-1} = a^{p-1-x}$ mod p
$(a^x)^{-1} = 447^{787-1-32}$ mod 787
$(a^x)^{-1} = 447^{754}$ mod 787
$(a^x)^{-1}$ = 725

m = b * $(a^x)^{-1}$ mod p
m = 506 * 725 mod 787
m = 366850 mod 257
m = 108

d. Cipher (a,b) = (147,728)
$(a^x)^{-1} = a^{p-1-x}$ mod p
$(a^x)^{-1} = 147^{787-1-32}$ mod 787
$(a^x)^{-1} = 147^{754}$ mod 787
m = 532896 mod 257
$(a^x)^{-1}$ = 732

$m = b * (a^x)^{-1} \bmod p$
$m = 728 * 732 \bmod 787$
$m = 97$

e. Cipher (a,b) = (643,18)
$(a^x)^{-1} = a^{p-1-x} \bmod p$
$(a^x)^{-1} = 643^{787-1-32} \bmod 787$
$(a^x)^{-1} = 643^{754} \bmod 787$
$(a^x)^{-1} = 487$

$m = b * (a^x)^{-1} \bmod p$
$m = 18 * 487 \bmod 787$
$m = 8766 \bmod 257$
$m = 109$

f. Cipher (a,b) = (279,197)
$(a^x)^{-1} = a^{p-1-x} \bmod p$
$(a^x)^{-1} = 279^{787-1-32} \bmod 787$
$(a^x)^{-1} = 279^{754} \bmod 787$
$(a^x)^{-1} = 388$

$m = b * (a^x)^{-1} \bmod p$
$m = 197 * 388 \bmod 787$
$m = 76436 \bmod 257$
$m = 97$

g. Cipher (a,b) = (485,261)
$(a^x)^{-1} = a^{p-1-x} \bmod p$
$(a^x)^{-1} = 485^{787-1-32} \bmod 787$
$(a^x)^{-1} = 485^{754} \bmod 787$
$(a^x)^{-1} = 700$

$m = b * (a^x)^{-1} \bmod p$
$m = 261 * 700 \bmod 787$
$m = 182700 \bmod 257$
$m = 116$

h. Cipher (a,b) = (381,711)
$(a^x)^{-1} = a^{p-1-x} \bmod p$
$(a^x)^{-1} = 381^{787-1-32} \bmod 787$
$(a^x)^{-1} = 381^{754} \bmod 787$
$(a^x)^{-1} = 41$

$m = b * (a^x)^{-1} \bmod p$

| Cipher (a,b) | (a^x)^-1 = a^p-1-x mod p | m = b * (a^x)-1 mod p | Karakter (m) |
|---|---|---|---|
| (347,531) | 593 | 83 | S |
| (267,225) | 707 | 101 | e |
| (447,506) | 725 | 108 | l |
| (147,728) | 732 | 97 | a |
| (643,18) | 487 | 109 | m |
| (279,197) | 388 | 97 | a |
| (485,261) | 700 | 116 | t |
| (381,711) | 41 | 32 | |
| (253,208) | 182 | 80 | P |
| (320,237) | 422 | 65 | A |
| (546,759) | 138 | 71 | G |
| (750,759) | 554 | 73 | I |

$m = 711 * 41 \bmod 787$
$m = 29151 \bmod 257$
$m = 32$

i. Cipher (a,b) = (253,208)
$(a^x)^{-1} = a^{p-1-x} \bmod p$
$(a^x)^{-1} = 253^{787-1-32} \bmod 787$
$(a^x)^{-1} = 253^{754} \bmod 787$
$(a^x)^{-1} = 182$

$m = b * (a^x)^{-1} \bmod p$
$m = 208 * 182 \bmod 787$
$m = 37856 \bmod 257$
$m = 80$

j. Cipher (a,b) = (320,237)
$(a^x)^{-1} = a^{p-1-x} \bmod p$
$(a^x)^{-1} = 320^{787-1-32} \bmod 787$
$(a^x)^{-1} = 320^{754} \bmod 787$
$(a^x)^{-1} = 422$

$m = b * (a^x)^{-1} \bmod p$
$m = 237 * 422 \bmod 787$
$m = 100014 \bmod 257$
$m = 65$

k. Cipher (a,b) = (546,759)
$(a^x)^{-1} = a^{p-1-x} \bmod p$
$(a^x)^{-1} = 546^{787-1-32} \bmod 787$
$(a^x)^{-1} = 546^{754} \bmod 787$
$(a^x)^{-1} = 138$

$m = b * (a^x)^{-1} \bmod p$
$m = 759 * 138 \bmod 787$
$m = 104742 \bmod 257$
$m = 71$

l. Cipher (a,b) = (750,709)
$(a^x)^{-1} = a^{p-1-x} \bmod p$

$(a^x)^{-1} = 750^{787-1-32} \bmod 787$
$(a^x)^{-1} = 750^{754} \bmod 787$
$(a^x)^{-1} = 554$

$m = b * (a^x)^{-1} \bmod p$
$m = 709 * 554 \bmod 787$
$m = 392786 \bmod 257$
$m = 73$

Susunan hasil dekripsi :
m1, m2, m3, m4, m5, m6, m7, m8, m9, m10, m11, m12.
83, 101, 108, 97, 109, 97, 116, 32, 80, 65, 71, 73.
Jika diubah kedalam karakter, maka kode-kode tersebut menjadi:
Selamat PAGI

**Tabel 2. Hasil Dekripsi ElGamal**

Kelebihan kriptografi ElGamal :
1. Masalah keamanan pada distribusi kunci dapat lebih baik
2. Masalah manajemen kunci yang lebih baik karena jumlah kunci yang lebih sedikit.
3. Hanya kunci privat yang perlu dijaga kerahasiaannya oleh setiap entitas yang berkomuniaksi (tetapi, otentikasi kunci publik tetap harus terjamin). Tidak ada kebutuhan mengirim kunci kunci privat sebagaimana pada system simetri.
4. Pasangan kunci publik/kunci privat tidak perlu diubah, bahkan dalam periode waktu yang panjang.
5. Dapat digunakan untuk mengamankan pengiriman kunci simetri.
6. Beberapa algoritma kunci-publik dapat digunakan untuk memberi tanda tangan digital pada pesan (akan dijelaskan pada materi kuliah selanjutnya)

Kelemahan kriptografi ElGamal :
1. Enkripsi dan dekripsi data umumnya lebih lambat daripada sistem simetri, karena enkripsi dan dekripsi menggunakan bilangan yang besar dan melibatkan operasi perpangkatan yang besar.
2. Ukuran cipherteks lebih besar daripada plainteks (bisa dua sampai empat kali ukuran plainteks).
3. Ukuran kunci relatif lebih besar daripada ukuran kunci simetri.
4. Karena kunci publik diketahui secara luas dan dapat digunakan setiap orang, maka cipherteks tidak memberikan informasi mengenai otentikasi pengirim.
5. Tidak ada algoritma kunci-publik yang terbukti aman (sama seperti block cipher). Kebanyakan algoritma mendasarkan keamanannya pada sulitnya memecahkan persoalan-persoalan aritmetik (pemfaktoran, logaritmik, dsb) yang menjadi dasar pembangkitan kunci.

### 3.2. Analisa Kriptografi Caesar Cipher

*Caesar Cipher* merupakan salah satu algoritma *cipher* tertua dan paling diketahui dalam perkembangan ilmu kriptografi. *Caesar cipher* merupakan salah satu jenis *cipher* substitusi yang membentuk *cipher* dengan cara melakukan penukaran karakter pada *plainteks* menjadi tepat satu karakter pada *cipherteks*.

Teknik seperti ini disebut juga sebagai *cipher* abjad tunggal. Algoritma kriptografi *Caesar Cipher* sangat mudah untuk digunakan.

1. Enkripsi *Caesar Cipher*
   Cara kerja enkripsi dari algoritma *caesar cipher* dalam kriptografi adalah sebagai berikut :
   a. Tentukan nilai kunci (bilangan bulat positif)
   b. Konversikan setiap karakter plainteks ke desimal
   c. Lakukan proses enkripsidengan formula (rumus) Ci = (Pi+K) Mod 256
   d. Konversikan setiap nilai Ci ke karakter

Untuk pesan yang akan dikirim oleh Siti kepada Nunuy melalui Fitri akan dienkripsi terlebih dahulu dengan perhitungan menggunakan metode kriptografi *caesar cipher*. Dengan penyelesaian sebagai berikut :

Plainteks : Selamat PAGI
Key : 15

| S | e | l | a | m | a | t | | P | A | G | I |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 83 | 101 | 108 | 97 | 109 | 97 | 116 | 32 | 80 | 65 | 71 | 73 |

**Tabel 3. Enkripsi *Caesar Cipher***

Rumus : $C_i = (P_i + K) \bmod 256$
$C_1 = (P_1 + K) \bmod 256$
$C_1 = (S + 15) \bmod 256$
$C_1 = (83 + 15) \bmod 256$
$C_1 = 98 \bmod 256$
$C_1 = 98 \longrightarrow$ b

$C_4 = (P_4 + K) \bmod 256$
$C_4 = (a + 15) \bmod 256$
$C_4 = (97 + 15) \bmod 256$
$C_4 = 112 \bmod 256$
$C_4 = 112 \longrightarrow$ p

$C_2 = (P_2 + K) \bmod 256$
$C_2 = (e + 15) \bmod 256$
$C_2 = (101 + 15) \bmod 256$
$C_2 = 116 \bmod 256$
$C_2 = 116 \longrightarrow$ t

| Karakter (m) | $C_i = (P_i + K) \bmod 256$ | Cipher |
|---|---|---|
| S | 98 | b |
| e | 116 | t |
| l | 123 | { |
| a | 112 | p |
| m | 124 | \| |
| a | 112 | p |
| t | 131 | â |
| | 47 | / |
| P | 95 | _ |
| A | 80 | P |
| G | 86 | V |
| I | 88 | X |

$C_5 = (P_5 + K) \bmod 256$
$C_5 = (m + 15) \bmod 256$
$C_5 = (109 + 15) \bmod 256$
$C_5 = 124 \bmod 256$
$C_5 = 124 \longrightarrow$ |

$C_3 = (P_3 + K) \bmod 256$
$C_3 = (l + 15) \bmod 256$
$C_3 = (108 + 15) \bmod 256$
$C_3 = 123 \bmod 256$
$C_3 = 123 \longrightarrow$ {

$C_6 = (P_6 + K) \bmod 256$
$C_6 = (a + 15) \bmod 256$
$C_6 = (97 + 15) \bmod 256$
$C_6 = 112 \bmod 256$
$C_6 = 112 \longrightarrow$ p

$C_7 = (P_7 + K) \bmod 256$
$C_7 = (t + 15) \bmod 256$
$C_7 = (116 + 15) \bmod 256$
$C_7 = 131 \bmod 256$
$C_7 = 131 \longrightarrow$ â

$C_{11} = (P_{11} + K) \bmod 256$
$C_{11} = (G + 15) \bmod 256$
$C_{11} = (71 + 15) \bmod 256$
$C_{11} = 86 \bmod 256$
$C_{11} = 86 \longrightarrow$ V

$C_8 = (P_8 + K) \bmod 256$
$C_8 = (espacio + 15) \bmod 256$
$C_8 = (32 + 15) \bmod 256$
$C_8 = 47 \bmod 256$
$C_8 = 47 \longrightarrow$ /

$C_{12} = (P_{12} + K) \bmod 256$
$C_{12} = (l + 15) \bmod 256$
$C_{12} = (73 + 15) \bmod 256$
$C_{12} = 88 \bmod 256$
$C_{12} = 88 \longrightarrow$ X

$C_9 = (P_9 + K) \bmod 256$
$C_9 = (P + 15) \bmod 256$
$C_9 = (80 + 15) \bmod 256$
$C_9 = 95 \bmod 256$
$C_9 = 95 \longrightarrow$ _

$C_{10} = (P_{10} + K) \bmod 256$
$C_{10} = (A + 15) \bmod 256$
$C_{10} = (65 + 15) \bmod 256$
$C_{10} = 80 \bmod 256$
$C_{10} = 80 \longrightarrow$ P

Hasil Enkripsi ($C_i$) : {b, t, {, p, |, p, â, /, _, P, V, X}

**Tabel 4. Hasil Enkripsi *Caesar Cipher***

2. Dekripsi Algoritma *Caesar Cipher*
   Cara kerja dekripsi dari algoritma *caesar cipher* dalam kriptografi adalah sebagai berikut :
   a. Konversikan setiap karakter *ciphertext* ke desimal
   b. Dekripsi dengan fromula (rumus) Pi = (Ci-K) Mod 256
   c. Konversikan Pi ke karakter

**Tabel 5. Dekripsi Algoritma *Caesar Cipher***

| b | t | { | p | \| | p | â | / | _ | P | V | X |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 98 | 116 | 123 | 112 | 124 | 112 | 131 | 47 | 95 | 80 | 86 | 88 |

Rumus : $P_i = (C_i - K) \bmod 256$
Key : 15
$P_1 = (C_1 - K) \bmod 256$
$P_1 = (b - 15) \bmod 256$
$P_1 = (98 - 15) \bmod 256$
$P_1 = 83 \bmod 256$
$P_1 = 83 \longrightarrow$ S

$P_8 = (C_8 - K) \bmod 256$
$P_8 = (/ - 15) \bmod 256$
$P_8 = (47 - 15) \bmod 256$
$P_8 = 32 \bmod 256$
$P_8 = 32 \longrightarrow$ espacio

$P_2 = (C_2 - K) \bmod 256$
$P_2 = (t - 15) \bmod 256$
$P_2 = (116 - 15) \bmod 256$
$P_2 = 101 \bmod 256$
$P_2 = 101 \longrightarrow$ e

$P_9 = (C_9 - K) \bmod 256$
$P_9 = (\_ - 15) \bmod 256$

| Cipher | $C_i = (P_i - K) \bmod 256$ | Karakter (m) |
|---|---|---|
| b | 83 | S |
| t | 101 | e |
| { | 108 | l |
| p | 97 | a |
| \| | 109 | m |
| p | 97 | a |
| â | 116 | t |
| / | 32 | |
| _ | 80 | P |
| P | 65 | A |
| V | 71 | G |
| X | 73 | I |

$P_9 = (95 - 15) \bmod 256$
$P_9 = 80 \bmod 256$
$P_9 = 80 \longrightarrow$ P

$P_3 = (C_3 - K) \bmod 256$
$P_3 = (\{ - 15) \bmod 256$
$P_3 = (123 - 15) \bmod 256$
$P_3 = 108 \bmod 256$
$P_3 = 108 \longrightarrow$ l

$P_{10} = (C_{10} - K) \bmod 256$
$P_{10} = (P - 15) \bmod 256$
$P_{10} = (80 - 15) \bmod 256$
$P_{10} = 65 \bmod 256$
$P_{10} = 65 \longrightarrow$ A

$P_4 = (C_4 - K) \bmod 256$
$P_4 = (p - 15) \bmod 256$
$P_4 = (112 - 15) \bmod 256$
$P_4 = 97 \bmod 256$
$P_4 = 97 \longrightarrow$ a

$P_{11} = (C_{11} - K) \bmod 256$
$P_{11} = (V - 15) \bmod 256$
$P_{11} = (86 - 15) \bmod 256$
$P_{11} = 71 \bmod 256$
$P_{11} = 71 \longrightarrow$ G

$P_5 = (C_5 - K) \bmod 256$
$P_5 = (| - 15) \bmod 256$
$P_5 = (124 - 15) \bmod 256$
$P_5 = 109 \bmod 256$
$P_5 = 109 \longrightarrow$ m

$P_{12} = (C_{12} - K) \bmod 256$
$P_{12} = (X - 15) \bmod 256$
$P_{12} = (88 - 15) \bmod 256$
$P_{12} = 73 \bmod 256$
$P_{12} = 73 \longrightarrow$ I

$P_6 = (C_6 - K) \bmod 256$
$P_6 = (p - 15) \bmod 256$
$P_6 = (112 - 15) \bmod 256$
$P_6 = 97 \bmod 256$
$P_6 = 97 \longrightarrow$ a

$P_7 = (C_7 - K) \bmod 256$
$P_7 = (â - 15) \bmod 256$
$P_7 = (131 - 15) \bmod 256$
$P_7 = 116 \bmod 256$
$P_7 = 116 \longrightarrow$ t

Hasil Dekripsi ($P_i$) : {S, e, l, a, m, a, t, , P, A, G, l}

**Tabel 6. Hasil Dekripsi *Caesar Cipher***

Kelebihan kriptografi *Caesar Cipher* :
1. Teknik Enkripsi yang paling sederhana.
2. Algoritma cipher tertua dan paling diken al dalamperkembangan ilmu kiptografi.
3. Sangat mudah untuk di gunakan.

Kelemahan kriptografi *Caesar Cipher* :
1. Tingkat keamanannya rendah , dikarenakan jumlah kuncinya hanya 26 kunci saja.
2. Teknik pemecahan kata kunci tersebut dapat dilakukan dengan cara melakukan pengecekan terhadap semua kunci yang ada yang berjumlah 26 tersebut.

## 4. Kesimpulan

Metode ElGamal dapat mengubah pesan asli menjadi pesan terenkripsi menjadi kode-kode yang tidak dapat dibaca dan mengembalikannya kembali menjadi pesan aslinya tanpa merubah dan merusak pesan. Keamanan algoritma ElGamal terletak pada kesulitan perhitungan logaritma diskrit pada modulo prima yang besar, sehingga upaya untuk menyelesaikan masalah logaritma ini menjadi sulit untuk dipecahkan, sehingga metode ini dianggap paling baik untuk pengamanan pesan.

Metode *Caesar Cipher* dapat mengubah pesan menjadi *ciphertext* yang tidak dapat terbaca. Tingkat keamanan yang rendah dengan menggunakan metode *Caesar Cipher*, dikarenakan jumlah kuncinya hanya 26 kunci saja, sehingga teknik pemecahan kata kunci tersebut dapat dilakukan dengan cara melakukan pengecekan terhadap semua kunci yang ada yang berjumlah 26 tersebut.

Pembangunan aplikasi pengamanan pesan teks yang dirancang sangat diperlukan untuk memenuhi kebutuhan pengguna dalam berkomunikasi.

Pada penelitian selanjutnya diharapkan kedua metode ini dapat diterapkan kedalam aplikasi pengamanan pesan agar bisa lebih berguna lagi, dengan mengembangkan fitur lain agar penerapan algoritma kriptografi ini lebih efisien.

## Referensi


Al-Anshori, F., & Aribowo, E. (2014). Implementasi Algoritma Kriptografi Kunci Publik Elgamal Untuk Proses Enkripsi Dan Dekripsi Guna Pengamanan File Data. *Jurnal Informatika Februari 2014*.

Gumiring, R. R. A. (2014). Perancangan Aplikasi Pengamanan Pesan Dengan Algoritma Caesar Chiper, *Pelita Informatika Budi Darma*, 106–110.

Parmadi, B. (2017). Implementasi Algoritma Kriptografi Elgamal pada Data Text, *Journal of Information and Technology*, 1-5.

Priyono. (2016). Penerapan Algoritma Caesar Cipher Dan Algoritma Vigenere Cipher Dalam Pengamanan Pesan Teks. *Jurnal Riset Komputer (JURIKOM)*, 351–356.

Rachmawati, D., & Candra, A. (2015). Implementasi Kombinasi Caesar dan Affine Cipher untuk Keamanan Data Teks, *Jurnal Edukasi dan Penelitian Informatika (JEPIN)*, 60–63.