Jurnal Riset Mahasiswa Matematika
Volume 3(3) (2024), Pages 148-156
p-ISSN: 2808-1552; e-ISSN: 2808-4926

Penerapan Algoritma DNA dalam Membangkitkan Kunci pada Algoritma Elgamal

Ihda Umdatul Khoiroh*, Turmudi, Imam Sujarwo

Program Studi Matematika, Fakultas Sains dan Teknologi, UIN Maulana Malik Ibrahim Malang, Indonesia

19610002@student.uin-malang.ac.id, turmudi_msi@yahoo.com, imamsujarwo@mat.uin-malang.ac.id

Abstrak

Keamanan pesan rahasia merupakan hal penting yang harus dijaga agar informasi yang ada di dalamnya tidak diketahui publik. Salah satu cara untuk mengamankan pesan adalah dengan menggunakan bantuan ilmu kriptografi. Dengan menggunakan algoritma yang ada dalam kriptografi, pesan akan disamarkan sehingga sulit untuk dipecahkan. Dalam penelitian ini digunakan algoritma DNA dalam proses pembangkitan kunci pada algoritma Elgamal. Tujuan dari penelitian ini adalah untuk meningkatkan keamanan *plaintext* dengan memodifikasi proses pembangkitan kunci, sehingga pihak lain akan kesulitan untuk memecahkan kunci tersebut. Hasil dari penelitian ini adalah kunci privat x yang sudah dienkripsi dengan menggunakan algoritma DNA dan kunci publik g berupa akar primitif dari bilangan prima yang telah dipilih yang kemudian di enkripsi dengan menggunakan algoritma DNA sehingga menghasilkan kunci publik baru. Sehingga untuk mengenkripsi *plaintext* perlu dilakukan dekripsi terhadap kunci publik terlebih dahulu.

Kata kunci: enkripsi; dekripsi; algoritma elgamal; algoritma DNA

Abstract

The security of secret messages is an important aspect that must be preserved to prevent public knowledge of the information contained within. One way to secure messages is by utilizing the assistance of cryptography. By employing algorithms found in cryptography, messages are disguised in a manner that makes them difficult to decipher. In this research, the DNA algorithmis used in the key generation process of the Elgamal algorithm. The objective of this research is to enhance the security of plaintext by modifying the key generation process, thereby making it difficult for others to crack the key. The result of this research is the encrypted private key x using the DNA algorithm and the public key g, which is a primitive root of the selected prime number that is further encrypted using the DNA algorithm, resulting in a new public key. Consequently, prior to encrypting the plaintext, decryption of the public key must be performedfirst.

Keywords:encryption; decription; elgamal algorithm; DNA algorithm

PENDAHULUAN

Keamanan informasi sudah menjadi masalah sejak zaman dahulu hingga saat ini. Pada zaman modern, informasi merupakan hal yang harus dipastikan keamanannya karena dengan kemajuan teknologi yang ada suatu informasi bisa didapatkan dengan mudah jika tingkat keamananya rendah. Informasi yang bersifat rahasia dan sensitif perlu dijaga keamanannya agar tidak dapat diakses oleh pihak lain yang tidak berhubungan atas informasi tersebut [1]. Salah satu kejahatan yang diakibatkan oleh kurangnya tingkat keamanan informasi adalah penyadapan. Kejahatan seperti ini sering terjadi pada informasi yang didistribusikan melalui internet, sedangkan internet telah menjadi media dalam pendistribusian informasi dewasa ini, karena itu tingkat kejahatan seperti penyadapan akan semakin tinggi jika tidak diimbangi dengan tingkat keamanan yang tinggi pula. Salah satu contoh kasus penyadapan adalah

Submitted: 21 Januari 2023 Reviewed: 2 Mei 2023 Accepted: 19 Januari 2024
Doi: http://dx.doi.org/10.18860/jrmm.v3i3.23302

pembobolan informasi mengenai data nasabah bank, pencurian dokumen negara, dan juga penyadapan surat- surat penting milik negara yang dilakukan oleh pihak-pihak yang tidak bertanggungjawab. Hal ini menjadikan peringatan bagi kita bahwa keamanan informasi pada saat ini sudah menjadi suatu kebutuhan [1]. Oleh karena itu dibutuhkan sebuah alat untuk memperkuat tingkat keamanan terhadap informasi-informasi tersebut, salah satunya dengan memanfaatkan ilmu kriptografi.

Kriptografi merupakan salah satu cabang ilmu matematika yang dapat digunakan untuk meningkatkan keamanan informasi. Kriptografi merupakan solusi yang tepat untuk mengatasi masalah keamanan [2]. Sebuah ilmu dan seni untuk menjaga kerahasiaan sebuah pesan dengan cara mengubah pesan kedalam bentuk sandi hingga maknanya tidak dapat dipahami merupakan fungsi dari kriptografi [1]. Penyandian pesan dalam kriptografi disebut dengan enkripsi, sedangkan proses mengembalikan pesan yang sudah disandi menjadi pesan asli disebut dekripsi. Kriptografi membentuk sebuah sistem yang didalamnya berisi himpunan yang terdiri dari algoritma enkripsi, algoritma dekripsi, ruang kunci, dan seluruh *plaintext* dan *ciphertext* yang terdapat di dalamnya [1]. Kriptografi memiliki berbagai macam algoritma untuk menyandikan pesan, dalam penelitian ini digunakan algoritma DNA dan algoritma Elgamal.

Deoxyrbose Nucleic Acid (DNA) dalam ilmu biologi merupakan salah satu molekul asam nukleat, dimana asam nukleat adalah salah satu senyawa polimer utama yang berada didalam sel. Dalam DNA tersimpan informasi genetik spesifik yang dimiliki oleh individu dan spesies-spesies tertentu yang kemudian diwariskan ke generasi berikutnya [3]. Pada awalnya hubungan kriptografi dan biologi molekuler memang tidak relevan, namun dengan adanya penelitian yang mendalami masalah terkait bioteknologi modern dan komputasi DNA, maka dua ilmu yang berbeda ini saling bekerjasama [4].

DNA dalam kriptografi merupakan pembawa sekaligus pengguna teknik biologi modern sebagai alat aplikasi. Algoritma DNA merupakan hal baru dalam dunia kriptografi. Algoritma DNA lahir setelah adanya penelitian dalam bidang komputasi DNA oleh Adlemen. DNA berbentuk heliks dengan panjang 2 untai nukleotida [5]. Pada setiap DNA terdapat 4 macam nukleotida yaitu *Adenine* (A), *Guanine* (G), *Cytosin* (C), dan *Thymine* (T). Teknik pada kriptografi DNA digunakan untuk mengintegrasikan operator DNA dan penyandian DNA kedalam struktur jaringan feistel [2].

Algoritma kriptografi berikutnya adalah algoritma Elgamal. Algoritma Elgamal termasuk ke dalam jenis algoritma kriptografi asimetris, karena mempunyai kunci untuk enkripsi dan dekripsi yang berbeda. Algoritma kunci publik merupakan sebutan lain untuk algoritma Elgamal [6]. Algoritma Elgamal merupakan algoritma kriptografi yang cukup sulit untuk dipecahkan, karena proses pembentukan kunci membutuhkan bilangan prima dan pemecahan masalah dilakukan dengan menggunakan logaritma diskrit. Kesulitan perhitungan logaritma diskrit merupakan titik keamanan padaalgoritma Elgamal [7].

METODE

Referensi diambil dari beberapa sumber yang berhubungan dengan kriptografi, kemudian melakukan studi literatur yang berhubungan dengan metode pada kriptografi yang digunakan dalam penelitian.

1. KRIPTOGRAFI

Kriptografi merupakan gabungan dari kata *cryptos* dan *graphein* yang berasal dari bahasa Yunani yang memiliki arti rahasia dan tulisan. Kriptografi secara harfiah berarti tulisan rahasia [1]. Kriptografi merupakan ilmu yang mempelajari metode untuk menyamarkan pesan sehingga pesan hanya dapat dibaca oleh penerima [8]. Kriptografi merupakan disiplin ilmu yang didalamnya mempelajari teknik-teknik matematika yang memiliki hubungan dengan keamanan suatu informasi [9].

Kriptografi menjadi syarat penting dalam keamanan teknologi informasi, terlebih dalam pengiriman pesan rahasia. Proses pengiriman pesan rahasia rentan terhadap mengalami

penyerangan seperti penyadapan, pemutusan komunikasi, pengubahan isi pesan dan lain sebagainya. Keamanan dalam pengiriman pesan dapat meningkat dengan adanya kriptografi, pengamanan pesan dilakukan dengan mengubah pesan dalam bentuk sandi dengan menggunakan sebuah algoritma dan kunci tertentu yang hanya diketahui oleh pihak-pihak yang berwenang.

a. Sistem Kriptografi

Kriptografi membentuk sebuah sistem yang disebut sebagai sistem kriptografi (*cryptosystem*). Sistem kriptografi adalah himpunan yang terdiri dari lima bagian sebagai berikut [10]:

1. *Plaintext*

   Plaintext atau teks asli adalah pesan asli yang dapat terbaca. *Plaintext* merupakan *input* algoritma enkripsi.

2. *Secret Key*

   Secret key adalah kunci rahasia yang merupakan input bagi algoritma enkripsi. *Secret key* merupakan nilai yang bebas terhadap teks asli dan menentukan hasil *output* untuk algoritma enkripsi.

3. *Ciphertext*

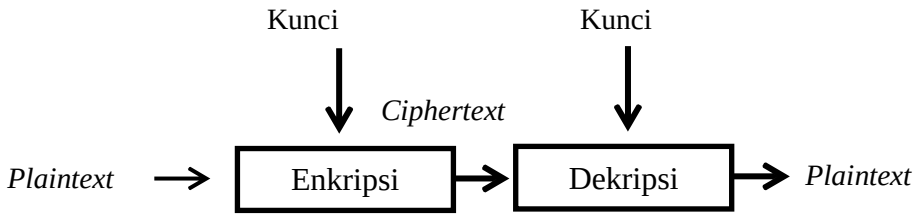
   Ciphertext merupakan *output* dari algoritma enkripsi. *Ciphertext* juga diartikan sebagai pesan yang tersembunyi karena sudah melalui proses enkripsi. *Ciphertext* yang acak dan sulit dipahami dapat dihasilkan dengan menggunakan algoritma enkripsi yang baik.

4. Algoritma Enkripsi

   Terdapat dua input yang dibutuhkan dalam algoritma enkripsi, yaitu *plaintext* dan *secret key*. Pada proses enkripsi *plaintext* ditransformasi sehingga menghasilkan *ciphertext*.

5. Algoritma Dekripsi

   Terdapat dua *input* yang dibutuhkan dalam algoritma dekripsi, yaitu *ciphertext* dan *secret key*. Algoritma dekripsi mengembalikan *ciphertext* menjadi *plaintext* jika *secret key* yang digunakan pada algoritma dekripsi dan algoritma enkripsi sama.



Gambar 1.1 Skema Enkripsi dan Dekripsi

Proses enkripsi menerima *input* berupa *plaintext* dan kunci sehingga mendapatkan sebuah hasil *ciphertext* yang merupakan bentuk sandi dari *plaintext*. Sedangkan proses dekripsi menerima *input* berupa *ciphertext* dan kunci sehingga mendapatkan *output* berupa *plaintext* semula.

b. Tujuan Kriptografi

Sebagaimana cabang ilmu pada umumnya, kriptografi juga memiliki tujuan. Kriptografi bertujuan untuk memberi layanan keamanan antara lain:

1. Kerahasiaan (*confidentiality*)

   Kerahasiaan merupakan layanan kriptografi dengan tujuan menjaga pesan sehingga pihak lain yang tidak berkepentingan tidak dapat membaca pesan tersebut. Kerahasiaan juga disebut dengan *secrecy* atau *privacy*.
2. Integritas data (*data integrity*)

   Layanan kriptografi yang memastikan keaslian dan keutuhan pesan merupakan arti dari integritas data. Pesan yang telah dikirimkan dapat dipastikan tidak dimanipulasi selama pengiriman berlangsung. Sistem keamanan harus mampu untuk mendeteksi keaslian pesan untuk menjaga integritas pesan tersebut. Realisasi layanan data integritas dalam kriptografi berupa fungsi hash dan tanda-tanda digital (*digital signature)*.
3. Otentikasi (*authentication*)

   Otentikasi adalah layanan kriptografi dengan cara mengidentifikasi kebenaran pihak-pihak yang melakukan komunikasi. Otentikasi harus dilakukan oleh seluruh pihak yang saling berkomunikasi, sehingga tidak ada keraguan dalam pengiriman maupun penerimaan pesan. Pesan yang dikirimkan melalui saluran komunikasi seperti internet rawan dipalsukan, sehingga pesan tersebut juga harus diidentifikasi terlebih dahulu darimana sumbernya.
4. Anti-penyangkalan (*non-repudiation*)

   Layanan kriptografi untuk mencegah pihak yang melakukan komunikasi melakukan penyangkalan terhadap apa yang telah dikirim adalah fungsi dari layanan kriptografi anti-penyangkalan. Tanda tangan pada lembar surat merupakan salah satu anti-penyangkalan dalam surat-menyurat, sedangkan dalam kriptografi hal ini dapat dilakukan dengan penggunaan tanda-tanda digital.

c. Algoritma Kriptografi

Algoritma kriptografi merupakan langkah-langkah yang disusun secara sistematis dan logis yang digunakan untuk menyembunyikan pesan. Dengan adanya algoritma, proses enkripsi pesan akan menjadi lebih mudah. Algoritma kriptografi dibagi menjadi dua jika dibedakan berdasarkan jenis kunci pada proses enkripsi dan dekripsi antara lain:

1. Kriptografi Kunci Simetri

   Kriptografi kunci simetri (*symmetric-key cryptography*) atau kriptografi konvensional merupakan algoritma kriptografi dimana proses enkripsi dan dekripsinya memiliki kunci yang sama. Letak keamanan pada kriptografi kunci simetri adalah pada kerahasiaan kuncinya [1].
2. Kriptografi Asimetri

   Kriptografi kunci asimetri (*asymmetric-key cryptography*) atau yang memiliki nama lain kriptografi kunci nirsimetri merupakan algoritma kriptografi yang memiliki kunci yang berbeda pada saat proses enkripsi dan dekripsi. Kriptografi asimetri disebut juga dengan kriptografi kunci publik (*public-key cryptography*). Kunci pada proses enkripsi dapat dibagikan kepada semua orang yang tidak mempunyai otoritas atas pesan tersebut, kunci ini disebut sebagai kunci publik (*public key*),

sedangkan kunci pada proses dekripsi tidak disebarkan dan hanya digunakan oleh pengirim pesan,kunci ini disebut dengan kunci pribadi (*private key*)[8].

2. ALGORITMA ELGAMAL

Algoritma Elgamal merupakan algoritma yang dibuat oleh Taher Elgamal pada tahun 1984. Pada awal keberadaannya algoritma ini digunakan untuk *digital signature*, seiring berjalannya waktu dilakukan modifikasi pada algoritma Elgamal agar dapat digunakan untuk proses enkripsi dan dekripsi [1].

Algoritma Elgamal merupakan algoritma kriptografi asimetris yang memiliki kunci berbeda untuk proses enkripsi dan dekripsi. Sistem kriptografi Elgamal bekerja pada sebuah grup perkalian (Ø,×) yang pada grup itu persoalan logaritma diskrit sulit dipecahkan. Grup perkalian Ø dapat berupa grup perkalian siklik $\langle\alpha\rangle$ dengan α adalah akar primitif pada ($Æ^*$,×) dengan p merupakan bilangan prima besar.

Secara umum besaran-besaran yang digunakan dalam algoritma Elgamal terdapat pada tabel 2.1 berikut:

Tabel 2.1 Besaran Pada Algoritma Elgamal

No	Besaran	Keterangan
1	Bilangan prima, p	Publik
2	Bilangan bulat g (akar primitif dari p)	Publik
3	Bilangan acak, x	Kunci privat
4	$y = g^x \ mod \ p$	Kunci publik
5	*Plaintext*, m	Privat
6	*Ciphertext*, a dan b	Publik

Prosedur penyandian pesan menggunakan algoritma Elgamal dimulai dengan pembangkitan kunci privat dan kunci publik oleh pihak pengirim dan pihak penerima pesan, kemudian dilanjutkan dengan enkripsi pesan dan diakhiri dengan dekripsi pesan. Penjelasan lebih lengkapnya adalah sebagai berikut:

a. Pembangkitan kunci privat dan kunci publik

Sebelum masuk kedalam proses enkripsi dilakukan pembangkitan kunci privat dan kunci publik dengan cara pengirim dan penerima pesan menentukan bilangan prima p dan bilangan bulat g yang merupakan akar primitif dari p. p setidaknya memiliki 1 faktor prima besar, jika p hanya memiliki 1 faktor prima kecil maka akan memudahkan penghitungan logaritma diskrit [11]. Kemudian pengirim dan penerima pesan membangkitkan kunci privat dan kunci publik dengan memilih sebuah bilangan acak x dengan syarat $1 < x < p - 1$. Kemudian membangkitkan kunci publik dengan persamaan

$$y = g^x \bmod p$$

Keterangan:

y : Kunci publik

g : Kunci publik (akar primitif dari p)

x : Bilangan acak, kunci privat

p : Bilangan prima

Sehingga dari hasil penghitungan, diperoleh kunci privat x dan kuncipublik (y, g, p).

b. Proses Enkripsi

Langkah pertama sebelum melakukan enkripsi adalah menyatakan pesan sebagai bilangan bulat m dan harus terletak dalam interval $[0, p-1]$. Untuk m yang besar, bagi m menjadi blok-blok m_1, m_2, ..., yang berukuran lebih kecil sehingga nilai didalam interval $[0, p-1]$ direpresentasikan oleh setiap blok. Misalkan pengirim pesan sudah mengetahui kunci publik penerima pesan yaitu (y, p, g). Berikut langkah-langkah enkripsi:

1. Pengirim memilih bilangan acak k, dengan $1 \leq k \leq p-1$.
2. Pengirim mengenkripsi pesan m menjadi pasangan nilai (a, b) dengan persamaan

$$a = g^k \bmod p \quad (2.2)$$

$$b = y^k m \bmod p \quad (2.3)$$

Keterangan:
a : *Ciphertext* 1
b : *Ciphertext* 2
g : Kunci publik (akar primitif p)
k : Bilangan acak
y : Kunci publik
m : *Plaintext*
p : Bilangan prima

Pasangan a dan b adalah *ciphertext* untuk pesan m. Jadi ukuran *ciphertext* duakali ukuran *plaintext*nya. Pengirim mengirim (a, b) kepada penerima.

c. Proses Dekripsi

Penerima pesan menggunakan kunci privat x untuk mendekripsi a dan b menjadi *plaintext* m.

3. ALGORITMA DNA

Kriptografi DNA merupakan hal yang baru dalam lingkup kriptografi. Kriptografi DNA didefinisikan sebagai alat untuk menyembunyikan data kedalam urutan DNA [12]. Setiap himpunan DNA terdiri dari 4 macam nukleotida, antara lain : *Adenine* (A), *Guanine* (G), *Cytosin* (C), dan *Thymine* (T). Pada struktur DNA *Adenine* dipasangkan dengan *Thymine*, sedangkan *Guanine* dipasangkan dengan *Cytoshin*. Dalam kriptografi DNA, pasangan DNA digunakan sebagai pembawa informasi [2]. *De- Oxy Ribo* merupakan asam nukleat yang dijadikan acuan dalam komputasi DNA. *De- Oxy Ribo* merupakan asam nukleat yang mengandung informasi genetik yang dibutuhkan pada saat proses pertumbuhan serta fungsi pasa organisme hidup. Komputasi DNA memiliki beberapa keuntungan diantaranya adalah kecepatan dan persyaratan daya minimal. Satu gram DNA mengandung kurang lebih 1021 basis DNA atau setara dengan 108 *tera-byte*. Oleh karena itu beberapa gram DNA berpotensi untuk menyimpan semua data yang terdapat didunia [4].

Dalam sistem biner 0 dan 1 saling berkomplemen, sehingga 00 dan 11, begitu pula dengan 10 dan 01 juga saling berkomplemen. Apabila 00, 11, 10, dan 01 dikodekan dengan basa nukleat A, T, G, dan C maka diperoleh 24 macam skema penyandian. Karena antar basa DNA memiliki hubungan komplemen, maka terdapat delapan macam kombinasi penyandi yang memenuhi prinsip pasangan basa komplementer.

Tabel 2.2 Bentuk Kombinasi Pengkodean DNA

	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**
A	00	00	01	01	10	10	11	11
T	11	11	10	10	01	01	00	00
G	01	10	00	11	00	11	01	10
C	10	01	11	00	11	00	10	01

HASIL DAN PEMBAHASAN

1. Penerapan Algoritma DNA untuk Membangkitkan Kunci pada AlgoritmaElgamal

Pembangkitan kunci pada algoritma Elgamal dilakukan oleh penerima pesan. Adapun kunci yang dibangkitkan merupakan kunci privat dan salah satu kunci publik. Langkah pertama untuk membangkitkan kunci privat adalah ambil sembarang bilangan prima p besar kemudian tentukan bilangan bulat g yang merupakan akar primitif dari p. Selanjutnya pilih bilangan bulat acak z dengan syarat $1 < z < 255$ karena nilai desimal tertinggi dalam tabel ASCII 256 adalah 255. Dilanjutkan dengan mengenkripsi z dengan menggunakan algoritma DNA dengan cara mengkonversi z ke dalam kode biner. Setelah didapatkan kode biner kemudian konversi kode biner kedalam kode DNA, data input biner dianggap sebagai bentuk pasangan yang digantikan oleh nukleotida DNA yaitu A untuk 00, T untuk 11, G untuk 10 dan C untuk 01. Kemudian konversi kode DNA yang telah diperoleh dengan menggunakan tabel kunci pembangun acak pada kriptografi DNA. Dari hasil konversi menggunakan kunci pembangun acak tersebut didapatkan sebuah kunci privat x.

Langkah selanjutnya dilakukan pembangkitan kunci publik dengan menggunakan persamaan

$$y = g^x mod\ p.$$

Dari penghitungan tersebut didapatkan kunci publik (y, g, p). Sebelum penerima pesan mengirimkan kunci publik ke pengirim pesan, akan dilakukan enkripsi kunci publik g dengan menggunakan algoritma DNA. Adapun langkah langkah untuk mengenkripsi kunci publik g adalah dengan mongkonversi g kedalam kode biner. Setelah didapatkan kode biner kemudian konversi kode biner kedalam kode DNA, data input biner dianggap sebagai bentuk pasangan yang digantikan oleh nukleotida DNA yaitu A untuk 00, T untuk 11, G untuk 10 dan C untuk 01. Kemudian konversi kode DNA yang telah diperoleh dengan menggunakan tabel kunci pembangun acak pada kriptografi DNA. Hasil enkripsi kunci publik g yaitu q akan dikirimkan penerima pesan pada pengirim pesan bersamaan dengan kunci publik (y, p).

2. SIMULASI PENERAPAN ALGORITMA DNA UNTUK MEMBANGKITKAN KUNCI PADA ALGORITMA ELGAMAL

Pada proses ini akan dilakukan pembangkitan kunci privat x dan kunci publik g pada algoritma Elgamal oleh penerima pesan dengan menggunakan algoritma DNA. Langkah pertama pilih bilangan prima $p = 4271$. Selanjutnya cari akar primitif dari 4271 yaitu 7, sehingga $g = 7$. Kemudian tentukan nilai z dimana $1 \leq z \leq 255$ dan diperoleh nilai $z = 212$. Enkripsi nilai z menggunakan algoritma DNA dengan cara mengkonversi $z = 212$ ke dalam kode biner yang sesuai dengan menggunakan tabel ASCII 256 sehingga diperoleh kode biner 11010100. Kemudian ubah kode biner 11010100 ke dalam kode DNA,

$$11 \rightarrow \text{T}$$
$$01 \rightarrow \text{C}$$
$$01 \rightarrow \text{C}$$

$$00 \rightarrow \text{A}$$

Sehingga didapatkan kode DNA TCCA, dari kode DNA tersebut kemudian dikonversi kembali dengan menggunakan kunci pembangun acak pada kriptografi DNA sehingga didapatkan nilai 101. Dari nilai tersebut didapatkan kunci privat x, sehingga $x = 101$. Kemudian hitung nilai y sebagai berikut

$$\begin{aligned} y &= g^x mod\ p \\ &= 7^{101} mod\ 4271 \\ &= 763 \end{aligned}$$

Dari penghitungan tersebut, didapatkan kunci publik $y = 763, g = 7, p = 4271$.Sebelum penerima pesan mengirim kunci publik ke pengirim pesan, penerima dilakukan enkripsi terhadap kunci publik g terlebih dahulu dengan menggunakan algoritma DNA dengan cara mengkonversi nilai $g = 7$ ke dalam kode biner dan didapatkan kode biner 00000111. Kemudian konversi kode biner kedalam kode DNA

$$\begin{aligned} 00 &\rightarrow \text{A} \\ 00 &\rightarrow \text{A} \\ 01 &\rightarrow \text{C} \\ 11 &\rightarrow \text{T} \end{aligned}$$

Sehingga didapatkan kode DNA AACT. Dan langkah terakhir adalah konversi kode DNA menggunakan kunci pembangun acak pada kriptografi DNA dan didapatkan nilai 28, sehingga $q = 28$. Karena kunci publik g sudah di enkripsi menjadi q, jadi penerima pesan mengirimkan kunci publik (y, q, p) ke pengirim pesan.

DAFTAR PUSTAKA

[1] Munir, R, Kriptografi. 2nd ed. Informatika Bandung, 2019.

[2] Satir, E. dan Kendirli, O, "A Symmetric DNA Encryption Process with a Biotechnical Hardware". *Journal of King Saud University*, 34(3), 1–10, 2022.

[3] Gaffar, S, Buku Ajar Bioteknologi Molekul. 2007.

[4] Mahesa, K., Sugiantoro, B., dan Prayudi, Y, Pemanfaatan Metode DNA Kriptografi dalam Meningkatkan Keamanan Citra Digital. Jurnal Ilmiah Informatika, 7(02), 108– 113, 2019.

[5] Ahmed, R. K. dan Mohammed, I. J, *Developing a New Hybrid Cipher Algorithm using DNA and RC4*. *International Journal of Advanced Computer Science and Applications*, 8(10), 171–176, 2017.

[6] Solin, R. dan Ramadhani, P, Modifikasi Pembangkit Kunci Algoritma Elgamal dengan Menerapkan Algoritma Freivalds. KOMIK (Konferensi Nasional Teknologi Informasi Dan Komputer), *4*(1), 2020.

[7] Warnilah, A. I. dan Nugraha, S. N, Komparasi Algoritma Kriptografi Elgamal dan Caesar Cipher untuk Enkripsi dan Dekripsi Pesan. IJCIT (*Indonesian Journal on Computer and Information Technology*), 3(2), 243–252, 2018.

[8] Jamaludin, Sulaiman, O. K., Tandungan, S., Putra, L. M., Yuswardi, Yulianti, N., Sidabutar, J., Aisa, S., Tantriawan, H., Arizal, Mardalius, dan Pakpahan, A. F, *Kriptografi: Teknik Keamanan Data*. Yayasan Kita Menulis, 2022.

[9] Menezes, A. J., Oorschoot, P. C., dan Vanstone, S. A, "Handbook of Applied Cryptography". *CRC Press*, 1996.

[10] Sadikin, R, Kriptografi untuk Keamanan Jaringan dan Implementasinya dalam Bahasa Java (T. A. Prabawati (ed.)). *CV. Andi Offset*, 2012.

[11] ElGamal, T,"A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms". *IEE Transactions on Information Theory*, *IT-31*(4), 469–472. ,1985.

[12] Raj, B. B., Vijay, J. F., dan Mahalakshmi, T,"Secure Data Transfer through DNA Cryptography using Symmetric Algorithm".International Journal of Computer Applications, 2016.

[13] Batten, L. M."Public Key Cryptography Applications and Attacks". *IEEE Press*, 2012

[14] Harahap, N, "Penelitian Kualitatif (H. Sazali (ed.))". *Wal Ashri Publishing*, 2020.
[15]Tantoni, A. dan Zaen, M. T. A, "Implementasi Double Caesar Cipher Menggunakan ASCII". Jurnal Informatika Dan Rekayasa Elektronik, 2018