Jurnal Riset Mahasiswa Matematika
Volume 1(6) (2022), Pages 283-287
p-ISSN: 2808-1552; e-ISSN: 2808-4926

Analisis Frekuensi Ciphertext dengan Algoritma Kriptografi DNA dan Transformasi Digraf

Widya Nur Faizah*, Muhammad Khudzaifah, Dewi Ismiarti

Program Studi Matematika, Fakultas Sains dan Teknologi, Universitas Islam Negeri Maulana Malik Ibrahim Malang, Indonesia

faizahwidya3@gmail.com, khudzaifah@uin-malang.ac.id, dewi.ismiarti@yahooo.com

Abstrak

Kriptografi DNA merupakan salah satu algoritma baru dalam kriptografi yang digunakan untuk enkripsi data dengan cara mengubah untaian DNA menjadi bilangan biner. Proses enkripsi diharapkan menghasilkan *ciphertext* yang acak dan tidak mudah terbaca. Penelitian ini bertujuan untuk mengetahui hasil analisis frekuensi terhadap *ciphertext* yang diperoleh dari proses enkripsi pesan menggunakan algoritma kriptografi DNA dan transformasi digraf. Pembentukan kunci simetri dilakukan untuk proses enkripsi pada kriptografi DNA, dan penggunaan aritmetika modulo untuk proses enkripsi dan dekripsi pada transformasi digraf. Proses enkripsi menghasilkan *ciphertext* dalam bentuk huruf dan simbol karena melibatkan penggunaan tabel ASCII. Analisis frekuensi dilakukan dengan cara membandingkan frekuensi kemunculan huruf pada *ciphertext* dengan frekuensi kemunculan huruf dalam Bahasa Inggris. Berdasarkan hasil analisis frekuensi, kesimpulan untuk penelitian ini yaitu *ciphertext* yang diperoleh terlihat acak, tidak mudah terbaca, dan sulit ditebak. Selain itu, proses dekripsi yang dilakukan mampu mengembalikan *ciphertext* menjadi pesan asli. Untuk penelitian selanjutnya, peneliti dapat mengubah pemilihan kombinasi kode biner pada kode DNA yang digunakan dalam algoritma kriptografi DNA, serta memperbanyak perbendaharaan karakter pada algoritma transformasi digraf, dan menggunakan beragam bahasa untuk disandikan.

Kata Kunci: Analisis Frekuensi; Kriptografi DNA; Transformasi Digraf.

Abstract

DNA Cryptography is one of new algortihm in cryptography that is used to encrypt the data by converting the DNA code into binary code. Encryption process is expected to produce a random and unreadable ciphertext. This research aims to determine the result of encryption frequency analysis of the ciphertext obtained from the encryption process using DNA Cryptography and Digraph Transformation algorithm. The formation of a symmetric key is carried out for the encryption and decryption process in DNA Cryptography, and modular arithmetic in Digraph Transformation algorithm. The encryption process produces ciphertext in the form of letters and symbols because if involves the use of an ASCII table. Frequency analysis is done by comparing the frequency of occurence of letters in the ciphertext with frequency of occurence of letters in English. The conclusion for this research is that the ciphertext looks random, not easy to read, and hard to guess. For the future work, researcher can change the choice of binary code combinatory in DNA Cryptographic algorithms, increase the character vocabulary in the Digraph Transformation algorithm, and use various languages to code.

Keywords : Frequency Analysis; DNA Cryptography; Digraph Transformation.

PENDAHULUAN

Terdapat perkembangan ilmu yang menggunakan matematika sebagai dasar ilmunya. Salah satu ilmu tersebut adalah ilmu kriptografi yang menggunakan aritmetika modulo sebagai salah satu dasar ilmunya [1]. Operasi modulo menghasilkan sisa pembagian dari suatu bilangan terhadap bilangan lain [2]. Banyak dokumen serta pesan yang bersifat rahasia membutuhkan keamanan yang tepat [3]. Kriptografi merupakan ilmu serta seni yang digunakan untuk menjaga

Submitted: 20 Desember 2021 Reviewed: 26 Juli 2022 Accepted: 28 Agustus 2022
Doi: http://dx.doi.org/10.18860/jrmm.v1i6.14591

keamanan pesan dengan menyandikan dalam bentuk yang tidak dapat dipahami lagi maknanya [3]. Pada saat ini, kriptografi dibutuhkan bukan hanya sekedar *privacy*, akan tetapi juga bertujuan untuk *data integrity*, *authentication*, dan *non-repudiation* [4]. Kriptografi DNA merupakan lapangan baru dalam kriptografi yang digunakan untuk enkripsi data [5]. Kriptografi DNA juga termasuk salah satu metode kriptografi [6]. Algoritma yang digunakan kriptografi DNA dalam proses enkripsi pesan adalah mengubah karakter pada pesan menjadi kode penyusun DNA. Algoritma enkripsi dan dekripsi kriptografi DNA meniru cara penerjemahan DNA [7].

Bonny B. Raj dkk (2016) [7] melakukan penelitian menggunakan algoritma simetri dalam lingkup kriptografi DNA. Dalam algoritma kunci simetri, kunci tunggal digunakan untuk proses enkripsi dan dekripsi [8]. Pada penelitian tersebut, penggunaan kunci acak berdasarkan barisan untaian DNA telah membuat proses keamanan menjadi kompleks. Heider dan Barnekow merupakan peneliti yang pada tahun 2007 mengajukan sebuah algoritma yang digunakan untuk mengkodekan informasi biner menjadi barisan DNA [9]. Pada sistem bilangan biner, terdapat bilangan yang saling berkomplemen yaitu 0 dan 1 atau 00 dan 11, 10 dan 01 [10]. Penelitian Elfadel Ajaeb (2014) [11] yang berjudul "*Cryptography by Means of Linear Algebra and Number Theory*" menjelaskan tentang teknik kriptografi dalam aljabar linear dan teori bilangan. Menurut Elfadel Ajaeb (2014), teknik kriptografi yang menggunakan teori bilangan akan lebih sulit dalam proses perhitungan. Transformasi digraf melakukan penyandian terhadap dua karakter sekaligus. Setiap digraf diberi kode bilangan dan terdiri dari dua karakter [12]. Salah satu kelemahan proses enkripsi dan dekripsi menggunakan *cipher* substitusi adalah tidak dapat menyembunyikan hubungan statistik, sehingga kriptanalis menggunakan kelemahan tersebut untuk menganalisis pesan menggunakan Teknik analisis frekuensi [3].

Proses enkripsi dan dekripsi menggunakan kriptografi diimplementasikan untuk mengamankan proses pengiriman pesan [13]. Pengirim pesan harus menjaga pesan tersebut agar tidak terpecahkan oleh kriptanalis. Proses enkripsi dan dekripsi teks bertujuan menjaga pesan agar tidak terbuka oleh penerima yang salah, sebagaimana konsep ayat Al-Quran yang bertujuan sebagai pengingat untuk menjadi orang yang amanah dalam menyimpan rahasia [14]. Dalam firman Allah Swt. pada surat Al-Mukminun ayat 8, menjelaskan tentang amanah dan janji mencakup segala hal yang dipikul manusia baik dalam hal agama maupun dunia. Amanah tersebut dapat berupa ucapan ataupun perbuatan. Setiap janji adalah amanah tentang apa yang telah disampaikan, baik berupa ucapan, perbuatan, maupun keyakinan [15].

METODE

Penelitian ini menggunakan metode studi literatur, dengan mempelajari buku-buku, artikel, dan tugas akhir tentang algoritma kriptografi. Jenis penelitian yang dipilih adalah penelitian kualitatif, karena penelitian ini melakukan analisis frekuensi terhadap hasil enkripsi pesan yang diperoleh dari algoritma kriptografi DNA dan transformasi digraf.

HASIL DAN PEMBAHASAN

1. Proses Enkripsi *Plaintext* dengan Algoritma Kriptografi DNA dan Transformasi Digraf.

Berikut ini adalah tahap-tahap yang digunakan untuk proses enkripsi dengan algoritma transformasi digraf adalah sebagai berikut:
Diberikan suatu *plaintext* dari *alphabet* $A - Z$ (banyaknya perbendaharaan karakter adalah $N = 26$). Selanjutnya akan diubah menjadi *ciphertext* menggunakan algoritma transformasi digraf, dengan langkah sebagai berikut:

1. Jika banyaknya huruf pada *plaintext* ganjil, maka tambahkan huruf Z di akhir teks.
2. Membuat pasangan huruf XY dari *plaintext* secara berurutan.
3. Menetapkan nilai parameter a dan b yang akan digunakan untuk proses enkripsi pesan menggunakan algoritma transformasi digraf. Berikut tahapan yang dilakukan:

a. Mencari bilangan a yang relatif prima dengan N^2.
b. Memilih sebarang bilangan bulat positif b.

4. Memilih sebarang bilangan k, kemudian membuat tabel *alphabet* dengan menambahkan k pada indeks masing-masing huruf, untuk $0 < k < 25$.
5. Mencari kode numerik dari $X = x, Y = y$ berdasarkan tabel *alphabet* dengan $k < x, y < k + 26$.
6. Menentukan kode bilangan masing-masing pasangan dengan nilai numerik yang diperoleh dari tabel *alphabet* menggunakan persamaan:

$$p = (x + k)N + (y + k) \quad (1)$$

7. Melakukan enkripsi teks menggunakan persamaan:

$$C \equiv ap + b \ (mod\ N^2) \quad (2)$$

8. Mengubah hasil enkripsi ke dalam bentuk persamaan:

$$C = (x' + k)N + (y' + k) \quad (3)$$

9. Memperoleh hasil enkripsi berdasarkan tabel *alphabet*.

Setelah memperoleh *plaintext* berdasarkan hasil enkripsi mengunakan algoritma transformasi digraph, selanjutnya yaitu melanjutkan proses enkripsi pesan menggunakan algoritma kriptografi DNA. Berikut ini tahapan yang dilakukan:

1. Menentukan kode desimal dan biner masing-masing karakter berdasarkan tabel ASCII.
2. Mengonversi menjadi untaian DNA.
3. Menentukan nilai untaian DNA berdasarkan tabel kunci pembangun acak kriptografi DNA.
4. Melakukan konversi nilai untaian DNA menjadi karakter berdasarkan tabel ASCII.
5. Memperoleh *ciphertext*.

Untaian DNA yang diperoleh pada proses enkripsi menggunakan algoritma kriptografi DNA memiliki nilai berdasarkan tabel kunci pembangun acak kriptografi DNA. Tabel kunci pembangun acak diperoleh dengan menggunakan algoritma kunci simetri, dengan pemilihan kunci 1000. Pembentukan tabel kunci pembangun acak dilakukan terhadap kode biner karakter pada tabel ASCII.

2. Proses Analisis Frekuensi Terhadap Hasil Enkripsi Pesan.

Berdasarkan hasil enkripsi pesan menggunakan algoritma kriptografi DNA dan transformasi digraf, diperoleh *ciphertext* yang akan dianalisis frekuensinya. Sebelum melakukan analisis frekuensi, penulis mengasumsikan bahwa *ciphertext* dienkripsi menggunakan *cipher* abjad tunggal. Berikut ini tahapan dalam proses analisis frekuensi setelah memperoleh *ciphertext*:

1. Mengasumsikan *plaintext* yang akan ditebak, dienkripsi dengan *cipher* abjad tunggal.
2. Melakukan perhitungan frekuensi kemunculan relatif huruf-huruf dalam *ciphertext*.
3. Membandingkan hasil pada langkah kedua dengan tabel frekuensi kemunculan (relatif) huruf-huruf dalam Bahasa Inggris.
4. Mengulangi langkah untuk huruf dengan frekuensi terbanyak berikutnya.
5. Interpretasi hasil.

Berdasarkan hasil iterasi, *plaintext* masih sulit untuk ditebak. Berdasarkan urutan huruf yang telah diubah, tetap tidak dapat menebak *plaintext* secara jelas. Sehingga dapat diketahui bahwa *plaintext* terenkripsi secara acak dan tidak mudah ditebak menggunakan teknik analisis frekuensi.

3. Proses Dekripsi *Ciphertext* dengan Algoritma Kriptografi DNA dan Transformasi Digraf

Pada penelitian ini, proses dekripsi pesan dilakukan untuk memastikan bahwa hasil pesan sandi menggunakan algoritma enkripsi menggunakan algoritma transformasi digraf dan kriptografi DNA, dapat dikembalikan ke dalam bentuk pesan asli menggunakan algoritma dekripsinya. Proses dekripsi diawali dengan menggunakan algoritma kriptografi DNA dan

dilanjutkan dengan algoritma transformasi digraf. Langkah pertama yang dilakukan yaitu proses dekripsi pesan menggunakan kriptografi DNA, setelah memperoleh *ciphertext* yang akan didekripsikan, sebagai berikut:

1. Menentukan kode desimal masing-masing karakter pada *ciphertext* berdasarkan tabel ASCII.
2. Melakukan konversi kode desimal menjadi untaian DNA berdasarkan tabel kunci pembangun acak kriptografi DNA.
3. Mengubah bentuk untaian DNA menjadi bilangan biner.
4. Memperoleh kode desimal karakter berdasarkan tabel ASCII.
5. Memperoleh hasil dekripsi.

Langkah selanjutnya, melanjutkan proses dekripsi *ciphertext* dari *alphabet* $A - Z$ (banyaknya perbendaharaan karakter adalah $N = 26$) dengan algoritma transformasi digraf, dengan langkah sebagai berikut:

1. Membuat pasangan huruf $X'Y'$ dari *ciphertext* secara berurutan.
2. Menetapkan nilai parameter a' dan b' yang akan digunakan untuk proses dekripsi pesan menggunakan algoritma transformasi digraf. Berikut tahapan yang dilakukan :
   a. Mengetahui nilai parameter a dan b yang telah dipilih.
   b. Memperoleh nilai parameter a' yaitu nilai invers dari parameter a, menggunakan persamaan:

$$aa^{-1} \equiv 1 \ (mod\ N^2). \qquad (4)$$

$$a' = a^{-1} (mod\ N^2) \qquad (5)$$

   c. Memperoleh nilai parameter b', yaitu menggunakan persamaan:

$$b' = \ -a^{-1}b \ (mod\ N^2) \qquad (6)$$

3. Memilih sebarang bilangan k, kemudian membuat tabel *alphabet* dengan menambahkan k pada indeks masing-masing huruf, untuk $0 < k < 25$.
4. Mencari kode numerik dari $X' = x', Y' = y'$ berdasarkan tabel *alphabet* dengan $k < x, y < k + 26$.
5. Menentukan kode bilangan masing-masing pasangan dengan nilai numerik yang diperoleh dari tabel *alphabet* menggunakan persamaan:

$$c = (x' - k)N + (y' - k) \qquad (7)$$

6. Melakukan dekripsi pesan menggunakan persamaan:

$$P \equiv a'c - b' \ (mod\ N^2) \qquad (8)$$

7. Mengubah hasil dekripsi ke dalam bentuk persamaan:

$$P = (x - k)N + (y - k) \qquad (9)$$

8. Memperoleh hasil dekripsi berdasarkan tabel *alphabet*.

KESIMPULAN

Berdasarkan hasil analisis frekuensi yang telah dilakukan, mengamati urutan huruf yang telah diubah, tetap tidak dapat menebak *plaintext* secara jelas. Hal tersebut dikarenakan proses enkripsi menggunakan algoritma transformasi digraf menghasilkan *ciphertext* yang acak secara berpasangan. Setiap huruf yang dienkripsi memiliki hasil perubahan yang berbeda-beda. Kemudian dilanjutkan dengan algoritma kriptografi DNA, membuat hasil enkripsi semakin

kompleks dan meluas, karena karakter yang diperoleh dari hasil enkripsi berbentuk huruf dan simbol. Sehingga dapat diketahui bahwa *plaintext* terenkripsi secara acak dan tidak mudah ditebak menggunakan teknik analisis frekuensi.

DAFTAR PUSTAKA

[1] D. B. Ginting, "Peranan Aritmetika Modulo dan Bilangan Prima Pada Algoritma Kriptografi RSA," *Media Informasi Vol. 9 No. 2,* p. 48, 2010.

[2] A. Sasmita, "Makalah Aritmetika Modulo," 2014.

[3] R. Munir, Kriptografi Edisi Kedua, Bandung: INFORMATIKA, 2019.

[4] R. Munir, "informatika.stei.itb.ac.id," [Online]. Available: https://informatika.stei.itb.ac.id/~rinaldi.munir/Buku/Kriptografi/Bab-1_Pengantar%20Kriptografi.pdf. [Accessed 21 November 2020].

[5] E. Vidhya and R. Rathipriya, "Two Level Text Data Encryption using DNA," *International Journal of Computational Intelligence and Informatics,* p. 107, 2018.

[6] K. Mahesa, B. Sugiantoro and Y. Prayudi, "Pemanfaatan Metode DNA Kriptografi Dalam Meningkatkan Keamanan Citra Digital," *Jurnal Ilmiah Informatika (JIF), Vol.07 No. 02,* pp. 1-2, 2019.

[7] B. B. Raj, P. J. Frank Vijay and P. T. Mahalakshmi, "Secure Data Transfer through DNA Cryptography using Symmetric Algorithm," *International Journal of Computer Applications Volume 133- No. 2,* p. 22, 2016.

[8] Ayushi, "A Symmetric Key Cryptographic Algorithm," *International Journal of Computer Applications (0975-8887) Volume 1 - No. 15,* pp. 1, 3, 2010.

[9] A. B. Hardjo, "Enkripsi Citra RGB dengan Algoritma Simplified-data Encryption Standar(S-DES) dan DNA-Vigenere Cipher," *Digital Repository Univrsitas Jember,* p. 14, 2016.

[10] C. S. Y. Qiao, "A Novel Image Encryption Algorithm Based on DNA Encoding and Spatiotemporal Chaos," *Entropy,* p. 6956, 2015.

[11] E. Ajaeb, "Cryptography by Means of Linear Algebra and Number Theory," pp. 41-43, 2014.

[12] S. Kromodimoeljo, Teori Aplikasi dan Kriptografi, SPK IT Consulting, 2009.

[13] Y. Suhelna, "Perancangan Aplikasi Penyandian Pesan Teks dengan Menggunakan Algoritma Digraph Cipher," *JUKI : Jurnal Komputer dan Informatika Volume 2 Nomor 1,* pp. 29-30, 2020.

[14] W. Riskiyah, "Enkripsi dan Dekripsi Pesan Menggunakan Grup Simetri untuk Mengamankan Informasi," *SKRIPSI,* pp. 2-3, 2016.

[15] S. Imam, Tafsir Al Qurthubi, Jakarta: PUSTAKA AZZAM, 2008.