ANALISIS FREKUENSI HASIL ENKRIPSI PESAN TEKS DENGAN ALGORITMA KRIPTOGRAFI DNA DAN TRANSFORMASI DIGRAF

SKRIPSI

OLEH
WIDYA NUR FAIZAH
NIM. 17610029

PROGRAM STUDI MATEMATIKA
FAKULTAS SAINS DAN TEKNOLOGI
UNIVERSITAS ISLAM NEGERI MAULANA MALIK IBRAHIM
MALANG
2021

ANALISIS FREKUENSI HASIL ENKRIPSI PESAN TEKS DENGAN ALGORITMA KRIPTOGRAFI DNA DAN TRANSFORMASI DIGRAF

SKRIPSI

Diajukan Kepada
Fakultas Sains dan Teknologi
Universitas Islam Negeri Maulana Malik Ibrahim Malang
untuk Memenuhi Salah Satu Persyaratan dalam
Memperoleh Gelar Sarjana Matematika (S.Mat)

Oleh
Widya Nur Faizah
NIM. 17610029

PROGRAM STUDI MATEMATIKA
FAKULTAS SAINS DAN TEKNOLOGI
UNIVERSITAS ISLAM NEGERI MAULANA MALIK IBRAHIM
MALANG
2021

ANALISIS FREKUENSI HASIL ENKRIPSI PESAN TEKS DENGAN ALGORITMA KRIPTOGRAFI DNA DAN TRANSFORMASI DIGRAF

SKRIPSI

Oleh
Widya Nur Faizah
NIM. 17610029

Telah Diperiksa dan Disetujui untuk Diuji
Tanggal 07 November 2021

Pembimbing I,	Pembimbing II,
Muhammad Khudzaifah, M.Si	Dewi Ismiarti, M.Si
NIDT. 19900511 20160801 1 057	NIDT. 19870505 20160801 2 058

Mengetahui,
Ketua Program Studi Matematika

Dr. Elly Susanti, S.Pd., M.Sc
NIP. 19741129 200012 2 005

ANALISIS FREKUENSI HASIL ENKRIPSI PESAN TEKS DENGAN ALGORITMA KRIPTOGRAFI DNA DAN TRANSFORMASI DIGRAF

SKRIPSI

Oleh
Widya Nur Faizah
NIM. 17610029

Telah Dipertahankan di Depan Dewan Penguji Skripsi
dan Dinyatakan Diterima sebagai Salah Satu Persyaratan
untuk Memperoleh Gelar Sarjana Matematika (S.Mat)
Tanggal 19 November 2021

Penguji Utama	:	Evawati Alisah, M.Pd	.....
Ketua Penguji	:	Dr. H. Wahyu H. Irawan, M.Pd	.....
Sekretaris Penguji	:	Muhammad Khudzaifah, M.Si	.....
Anggota Penguji	:	Dewi Ismiarti, M. Si	.....

Mengetahui,
Ketua Program Studi Matematika

Dr. Elly Susanti, S.Pd., M.Sc
NIP. 19741129 200012 2 005

PERNYATAAN KEASLIAN TULISAN

Saya yang bertanda tangan di bawah ini:

Nama : Widya Nur Faizah

NIM : 17610029

Jurusan : Matematika

Fakultas : Sains dan Teknologi

Judul Skripsi : Analisis Frekuensi Hasil Enkripsi Pesan Teks dengan Algoritma Kriptografi DNA dan Transformasi Digraf

menyatakan dengan sebenarnya bahwa skripsi yang saya tulis ini benar-benar merupakan hasil karya sendiri, bukan merupakan pengambilan data, tulisan, atau pikiran orang lain yang saya akui sebagai hasil tulisan atau pikiran saya sendiri, kecuali dengan mencantumkan sumber cuplikan pada daftar rujukan. Apabila di kemudian hari terbukti bahwa skripsi ini hasil jiplakan, maka saya bersedia menerima sanksi atas pebuatan tersebut.

Malang, 7 Desember 2021
Yang membuat pernyataan,

Widya Nur Faizah
NIM. 17610029

MOTTO

وَمَنْ يَتَّقِ اللَّهَ يَجْعَلْ لَهُ مَخْرَجًا وَيَرْزُقْهُ مِنْ حَيْثُ لَا يَحْتَسِبُ

"Barangsiapa bertaqwa kepada Allah niscaya Dia akan mengadakan baginya jalan keluar. Dan memberinya rezeki dari arah yang tiada disangka-sangka"
(QS. At-Tholaq/65:2-3).

PERSEMBAHAN

Dengan rasa syukur kepada Allah Swt, dengan segala kerendahan hati, skripsi ini penulis persembahkan untuk:

Ayah tercinta Bibit Asrori, ibu tercinta Nani Triana, mbah Eti Suheti, mbah Rustam, yang senantiasa ikhlas mendoakan, menjadi nasihat dengan kasih sayang dan motivasi, serta adik tersayang Humam Hisyam yang memberi semangat bagi penulis untuk bersabar menuntut ilmu, dan mengabdi.

KATA PENGANTAR

Assalamu'alaikum Warahmatullahi Wabarakatuh

Segala puji dan syukur kepada Allah Swt., yang telah memberi rahmat, serta hidayah-Nya kepada kita, khususnya kepada penulis sehingga mampu menyelesaikan skripsi dengan judul "Analisis Frekuensi Hasil Enkripsi Pesan Teks dengan Algoritma Kriptografi DNA dan Transformasi Digraf". Sholawat serta salam kepada baginda Nabi Muhammad Saw., yang semoga kita memperoleh syafa'at-Nya hingga akhir kelak. Penyusunan skripsi ini ditujukan sebagai salah satu persyaratan dalam menyelesaikan program Sarjana Matematika Universitas Islam Negeri Maulana Malik Ibrahim Malang serta sebagai partisipasi penulis untuk menerapkan ilmu yang telah diperoleh ketika penulis masih menimba ilmu di Program Studi Matematika Fakultas Sains dan Teknologi.

Penulis menyampaikan terima kasih yang sebesar-besarnya kepada semua pihak yang telah membantu dalam menyelesaikan penyusunan skripsi ini, baik secara langsung maupun tidak langsung, oleh karena itu perkenankan penulis mengucapkan terimakasih kepada:

1. Prof. Dr. H. M. Zainuddin, M.A., selaku rektor Universitas Islam Negeri Maulana Malik Ibrahim Malang.
2. Dr. Sri Harini, M.Si, selaku dekan Fakultas Sains dan Teknologi Universitas Islam Negeri Maulana Malik Ibrahim Malang dan selaku dosen wali yang memberikan arahan kepada penulis.
3. Dr. Elly Susanti, S.Pd., M.Sc, selaku ketua Program Studi Matematika Fakultas Sains dan Teknologi Universitas Islam Negeri Maulana Malik Ibrahim Malang.
4. Muhammad Khudzaifah, M.Si., selaku dosen pembimbing I dan Dewi Ismiarti, M.Si., selaku dosen pembimbing II yang telah banyak memberikan arahan, nasihat, dan pengalaman berharga kepada penulis.
5. Evawati Alisah, M.Pd., selaku penguji utama dan Dr. H. Wahyu H. Irawan, M.Pd, selaku ketua penguji skripsi, yang telah memberikan nasihat kepada penulis.

6. Segenap civitas akademika Program Studi Matematika Fakultas Sains dan Teknologi, Universitas Islam Negeri Maulana Malik Ibrahim Malang terutama seluruh dosen, terimakasih atas segala ilmu dan bimbingannya.
7. Ayah dan Ibu, mbah kung dan mbah putri yang selalu memberikan doa, semangat, serta motivasi kepada penulis sampai saat ini.
8. Seluruh teman-teman di Program Studi Matematika angkatan 2017 yang berjuang bersama-sama untuk meraih mimpi.
9. Semua pihak yang ikut membantu dalam menyelesaikan skripsi ini baik berupa materil maupun moril.

Semoga Allah Swt., melimpahkan rahmat dan karunia-Nya kepada kita semua. Selain itu, penulis berharap semoga skripsi ini dapat bermanfaat bagi penulis dan bagi pembaca.

Wassalamu'alaikum Warahmatullahi Wabarakatuh.

Malang, 7 Desember 2021

Penulis

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

ABSTRAK

Faizah, Widya Nur. 2021. **Analisis Frekuensi Hasil Enkripsi Pesan Teks dengan Algoritma Kriptografi DNA dan Transformasi Digraf**. Skripsi. Program Studi Matematika Fakultas Sains dan Teknologi, Universitas Islam Negeri Maulana Malik Ibrahim Malang. Pembimbing: (I) Muhammad Khudzaifah, M.Si. (II) Dewi Ismiarti, M.Si.

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

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.

ABSTRACT

Faizah, Widya Nur. 2021. **On The Analysis of Text Message Encryption Result Frequency Using DNA Cryptography and Digraph Transformation Algorithm**. Thesis. Mathematics Department Science and Technology Faculty, Maulana Malik Ibrahim State Islamic University Malang. Advisors : (I) Muhammad Khudzaifah, M.Si (II) Dewi Ismiarti, M.Si.

Keywords : DNA Cryptography, Digraph Transformation, Frequency Analysis.

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.

ملخص

فائزة، ويديا نور. ٢٠٢١. **تحليل تردد نتائج تشفير الرسائل النصية باستخدام خوارزمية تشفير الحمض النووي وتحويل الديجراف**. البحث العلمي. قسم الرياضيات ، كلية العلوم والتكنولوجيا، جامعة مولانا مالك إبراهيم الإسلامية الحكومية مالانج. المشرف: (١) محمد خذيفة، الماجستير. (٢) ديوي إسميارتي، الماجستير.

الكلمات الرئيسية: تحليل الترددز (*Analisis Frekuensi*)، ترميز الحمض النووي (*Kriptografi DNA*)، تحويل الديغراف (*Transformai Digraf*)

ترميز الحمض النووي هو أحد ترميز *algoritma* الجديد الذي يستخدم لتشفير البيانات عن طريق تحويل رمز الحمض النووي إلى رمز ثنائي. ومن المتوقع أن تنتج عملية التشفير نصاً عشوائياً وغير قابل للقراءة.ء ويهدف هذا البحث إلى تحديد نتيجة تحليل التردد التشفيري للنص التشفيري الذي تم الحصول عليه من عملية التشفير باستخدام خوارزمية الترميز *DNA* والتحويل الديغراف (*Digraf*) . ويتم تشكيل مفتاح متناظر لعملية التشفير وفك التشفير في ترميز الحمض النووي ، والحسابات النمطية في خوارزمية تحويل (*Digraf*) . عملية التشفير تنتج النص في شكل حروف ورموز لأنه إذا كان ينطوي على استخدام جدول *ASCII*. يتم تحليل التردد عن طريق مقارنة تواتر تكرار الحروف في النص التشعبي مع تواتر حدوث الحروف في اللغة الإنجليزية.

الاستنتاج لهذا البحث هو أن النص الشفري يبدو عشوائيا ، ليس من السهل قراءته ، ومن الصعب تخمينه . بالنسبة للعمل المستقبلي ، يمكن للباحث تغيير اختيار الشفرة الثنائية المجمعة في خوارزميات ترميز الحمض النووي ، وزيادة مفردات الحرف في خوارزمية تحول (*Digraf*) ، واستخدام لغات مختلفة للترميز.

BAB I
PENDAHULUAN

1.1 Latar Belakang

Matematika dan pemrograman komputer memiliki suatu operasi yang disebut operasi modulo. Operasi modulo menghasilkan sisa pembagian dari suatu bilangan terhadap bilangan lain (Sasmita, 2014). 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 (Ginting, 2010). Tanpa disadari, dalam kehidupan kita sekarang ini telah dikelilingi kriptografi. Banyak dokumen serta pesan yang bersifat rahasia membutuhkan keamanan yang tepat (Munir, Kriptografi Edisi Kedua, 2019).

Kriptografi merupakan ilmu serta seni yang digunakan untuk menjaga keamanan pesan dengan menyandikan dalam bentuk yang tidak dapat dipahami lagi maknanya (Munir, Kriptografi Edisi Kedua, 2019). Kriptografi dikenal sebagai teknik rahasia dalam penulisan, dengan karakter yang khusus, yang menggunakan huruf serta karakter yang berbeda dari bentuk aslinya. Menezez (1996) dalam buku Rinaldi Munir (Munir, Kriptografi Edisi Kedua, 2019) menyatakan bahwa ilmu yang dipelajari dalam kriptografi merupakan teknik matematika yang memiliki hubungan dengan aspek keamanan informasi seperti kerahasiaan, integritas data, dan otentikasi. Terdapat berbagai macam algoritma kriptografi yang perlu dipelajari, salah satunya algoritma kriptografi DNA serta transformasi digraf.

Kriptografi DNA merupakan lapangan baru dalam kriptografi yang digunakan untuk enkripsi data (Vidhya & Rathipriya, 2018). Kriptografi DNA

juga termasuk salah satu metode kriptografi (Mahesa, Sugiantoro, & Prayudi, 2019). 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, yaitu dengan cara mengubah untaian DNA berupa Adenin (A), Timin (T), Citosin (C), dan Guanin (G) menjadi bilangan biner (Raj, J. Frank Vijay, & T. Mahalakshmi, 2016). Penggunaan kriptografi DNA terdapat dalam penelitian Mohammad Reza Najaftorkaman (2015) yang berjudul "*A Method to Encrypt Information with DNA-Based Cryptography*" membahas tentang kriptografi DNA menjadi hal baru yang menarik untuk dikaji dalam proses keamanan data. Penelitian tersebut juga mendiskusikan proses enkripsi data menggunakan kriptografi DNA. Kemudian, hasil penelitian tersebut menyatakan bahwa kekuatan algoritma kriptografi DNA diperoleh berdasarkan sifat untaian DNA. Selain itu, Bonny B. Raj dkk (2016) melakukan penelitian menggunakan algoritma simetri dalam lingkup kriptografi DNA. Pada penelitian tersebut, penggunaan kunci acak berdasarkan barisan untaian DNA telah membuat proses keamanan menjadi kompleks. Penelitian Elfadel Ajaeb (2014) yang berjudul "*Cryptography by Means of Linear Algebra and Number Theory*" menjelaskan tentang teknik kriptografi dalam aljabar linear dan teori bilangan. Penelitian tersebut memaparkan beberapa proses dalam kriptografi yang menerapkan teori bilangan. Salah satu teknik kriptografi yang dijelaskan adalah transformasi digraf. Menurut Elfadel Ajaeb (2014), teknik kriptografi yang menggunakan teori bilangan akan lebih sulit dalam proses perhitungan. Akan tetapi, tidak mudah dalam proses menentukan invers dari bilangan prima modulo n pada transformasi digraf. Transformasi digraf

melakukan penyandian terhadap dua karakter sekaligus. Setiap digraf diberi kode bilangan dan terdiri dari dua karakter (Kromodimoeljo, 2009).

Proses enkripsi dan dekripsi menggunakan kriptografi diimplementasikan untuk mengamankan proses pengiriman pesan (Suhelna, 2020). 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 (Riskiyah, 2016). Dalam firman Allah Swt. pada surat Al-Mukminun ayat 8, yang artinya:

"*Dan orang-orang yang memelihara amanah-amanah (yang dipikulnya) dan janjinya*". (QS. Al-Mukminun/23:8).

Pada penelitian dengan judul "Implementasi Kriptografi DNA dan Transformasi Digraf untuk Mengamankan Pesan Teks", akan dilakukan percobaan melakukan konversi *plaintext* menggunakan transformasi digraf, dan kemudian dilanjutkan dengan konversi teks ke dalam kriptografi DNA. Proses konversi tersebut membutuhkan bantuan dari tabel *alphabet*, tabel ASCII, dan Tabel kunci pembangun acak kriptografi DNA. Selanjutnya, untuk mengetahui kedua algoritma tersebut cukup aman dari kriptanalis, maka dilakukan analisis frekuensi terhadap hasil enkripsinya. Penulis berharap, dengan adanya penggunaan metode baru dalam proses enkripsi dekripsi pesan teks tersebut, proses keamanan pesan teks akan lebih efektif.

1.2 Rumusan Masalah

Berdasarkan latar belakang yang telah dijelaskan sebelumnya, maka rumusan masalah dalam penelitian ini adalah bagaimana analisis frekuensi hasil enkripsi teks menggunakan algoritma kriptografi DNA dan transformasi digraf?

1.3 Tujuan Penelitian

Dengan adanya rumusan masalah yang telah dijelaskan sebelumnya, maka tujuan dalam penelitian ini yaitu untuk mengetahui analisis frekuensi hasil enkripsi teks menggunakan kriptografi DNA dan transformasi digraf.

1.4 Manfaat Penelitian

Penelitian ini diharapkan dapat memberikan manfaat sebagai berikut:

1. Manfaat Teoritis

   Hasil Penelitian diharapkan dapat digunakan untuk mengembangkan proses analisis frekuensi pada hasil enkripsi pesan menggunakan algoritma kriptografi DNA dan transformasi digraph, serta dapat mengembangkan ilmu pengetahuan tentang teori bilangan yang digunakan dalam algoritma kriptografi.

2. Manfaat Praktis

   a. Bagi Pembaca

      1) Memudahkan pembaca untuk mempelajari salah satu metode yang digunakan dalam kriptografi.
      2) Memberikan informasi kepada pembaca untuk pengembangan penelitian selanjutnya.

b. Bagi Penulis

1) Memperoleh pengetahuan dan wawasan yang dipelajari saat menggali informasi tentang kriptografi.

2) Mampu mengimplementasikan serta mengembangkan ilmu yang diperoleh saat perkuliahan.

1.5 Batasan Masalah

Batasan masalah pada penelitian ini adalah sebagai berikut:

1. Konversi bilangan biner menggunakan kombinasi pengkodean basa DNA dengan konversi A menjadi 00, T menjadi 11, G menjadi 10, dan C menjadi 01.
2. Analisis frekuensi dengan frekuensi kemunculan 1 huruf dalam Bahasa Inggris.
3. Karakter yang digunakan dalam algoritma transformasi digraf berupa huruf A – Z.

1.6 Metode Penelitian

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. Berikut ini adalah tahap-tahap yang digunakan untuk menyelesaikan penelitian adalah sebagai berikut:

1. 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:
   a. Jika banyaknya huruf pada *plaintext* ganjil, maka tambahkan huruf Z di akhir teks.
   b. Membuat pasangan huruf XY dari *plaintext* secara berurutan.
   c. Menetapkan nilai parameter a dan b yang akan digunakan untuk proses enkripsi pesan menggunakan algoritma transformasi digraf. Berikut tahapan yang dilakukan:
      i. Mencari bilangan a yang relatif prima dengan N^2.
      ii. Memilih sebarang bilangan bulat positif b.
   d. Memilih sebarang bilangan k, kemudian membuat tabel *alphabet* dengan menambahkan k pada indeks masing-masing huruf, untuk $0 < k < 25$.
   e. Mencari kode numerik dari $X = x, Y = y$ berdasarkan tabel *alphabet* dengan $k < x, y < k + 26$.
   f. Menentukan kode bilangan masing-masing pasangan dengan nilai numerik yang diperoleh dari tabel *alphabet* menggunakan persamaan:
   $$p = (x + k)N + (y + k).$$
   g. Melakukan enkripsi teks menggunakan persamaan:
   $$C \equiv ap + b \ (mod\ N^2).$$
   h. Mengubah hasil enkripsi ke dalam bentuk persamaan:
   $$C = (x' + k)N + (y' + k).$$
   i. Memperoleh hasil enkripsi berdasarkan tabel *alphabet*.

2. 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:
   a. Menentukan kode desimal dan biner masing-masing karakter berdasarkan tabel ASCII.
   b. Mengonversi menjadi untaian DNA.
   c. Menentukan nilai untaian DNA berdasarkan tabel kunci pembangun acak kriptografi DNA.
   d. Melakukan konversi nilai untaian DNA menjadi karakter berdasarkan tabel ASCII.
   e. Memperoleh *ciphertext*.
3. Melakukan analisis frekuensi terhadap hasil enkripsi pesan menggunakan algoritma kriptografi DNA dan transformasi digraf. Berikut ini tahapan dalam proses analisis frekuensi setelah memperoleh *ciphertext*:
   a. Mengasumsikan *plaintext* yang akan ditebak, dienkripsi dengan *cipher* abjad tunggal.
   b. Melakukan perhitungan frekuensi kemunculan relatif huruf-huruf dalam *ciphertext*.
   c. Membandingkan hasil pada langkah kedua dengan Tabel 2. 2 Frekuensi Kemunculan (Relatif) Huruf Dalam Bahasa Inggris.
   d. Mengulangi langkah untuk huruf dengan frekuensi terbanyak berikutnya.
   e. Interpretasi hasil.

4. Melakukan proses dekripsi pesan menggunakan kriptografi DNA, setelah memperoleh *ciphertext* yang akan didekripsikan. Berikut tahapan yang dilakukan:
   a. Menentukan kode desimal masing-masing karakter pada *ciphertext* berdasarkan tabel ASCII.
   b. Melakukan konversi kode desimal menjadi untaian DNA berdasarkan tabel kunci pembangun acak kriptografi DNA.
   c. Mengubah bentuk untaian DNA menjadi bilangan biner.
   d. Memperoleh kode desimal karakter berdasarkan tabel ASCII.
   e. Memperoleh hasil dekripsi.
5. Melanjutkan proses dekripsi *ciphertext* dari *alphabet* $A - Z$ (banyaknya perbendaharaan karakter adalah $N = 26$). Setelah memperoleh hasil dekripsi mengunakan algoritma kriptografi DNA, selanjutnya akan diubah menjadi *plaintext* menggunakan algoritma transformasi digraf, dengan langkah sebagai berikut:
   a. Membuat pasangan huruf $X'Y'$ dari *ciphertext* secara berurutan.
   b. Menetapkan nilai parameter a' dan b' yang akan digunakan untuk proses dekripsi pesan menggunakan algoritma transformasi digraf. Berikut tahapan yang dilakukan :
      i. Mengetahui nilai parameter a dan b yang telah dipilih.
      ii. Memperoleh nilai parameter a' yaitu nilai invers dari parameter a, menggunakan persamaan:

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

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

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

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

c. Memilih sebarang bilangan k, kemudian membuat tabel *alphabet* dengan menambahkan k pada indeks masing-masing huruf, untuk $0 < k < 25$.

d. Mencari kode numerik dari $X' = x', Y' = y'$ berdasarkan tabel *alphabet* dengan $k < x, y < k + 26$.

e. Menentukan kode bilangan masing-masing pasangan dengan nilai numerik yang diperoleh dari tabel *alphabet* menggunakan persamaan:

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

f. Melakukan dekripsi pesan menggunakan persamaan:

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

f. Mengubah hasil dekripsi ke dalam bentuk persamaan:

$$P = (x - k)N + (y - k).$$

g. Memperoleh hasil dekripsi berdasarkan tabel *alphabet*.

1.7 Sistematika Penulisan

Agar pembahasan dalam skripsi ini mudah dipahami, maka penulis menggunakan sistematika penulisan yang terdiri atas empat bab. Masing-masing bab akan dibagi ke dalam beberapa subbab dengan rincian sebagai berikut:

BAB I : Pendahuluan

Bab pendahuluan mencakup latar belakang, rumusan masalah, tujuan dan manfaat penelitian, batasan masalah, metode penelitian serta sistematika penulisan.

BAB II : Kajian Pustaka

Pada bab ini, terdapat penjelasan mengenai konsep-konsep yang mendukung penelitian. Konsep-konsep tersebut yaitu tentang keterbagian, algoritma pembagian, Faktor Persekutuan Terbesar (FPB), aritmetika modulo, kongruensi, balikan modulo (*invers* modulo), kriptografi, kriptografi DNA, Algoritma kunci simetri, Transformasi Digraf, analisis frekuensi, serta terdapat kajian keislaman.

BAB III : Pembahasan

Pembahasan mengenai penelitian yang dilakukan akan dikaji pada bab pembahasan. Bab ini terdiri dari penjelasan proses enkripsi dan dekripsi pesan teks menggunakan kriptografi DNA dan Transformasi Digraf, kemudian analisis frekuensi terhadap hasil enkripsi pesan tersebut.

BAB IV : Penutup

Bab penutup berisi kesimpulan terhadap hasil penelitian serta terdapat saran untuk penelitian selanjutnya.

BAB II
KAJIAN PUSTAKA

2.1 Keterbagian

Definisi 2.1.1

Misalkan $p, q \in \mathbb{Z}$, dengan $p \neq 0$, maka p disebut membagi q (ditulis $p|q$) apabila $q = pk$, untuk suatu $k \in \mathbb{Z}$ (Irawan, Hijriyah, & Habibi, 2014).

Berdasarkan definisi tersebut, bilangan bulat p dengan $p \neq 0$, disebut membagi q apabila terdapat suatu bilangan bulat k sedemikian hingga $q = pk$. Kemudian notasi $p|q$ dapat dibaca dengan "p membagi q" atau "p faktor dari q" atau "q kelipatan dari p" atau "p pembagi q". Apabila p tidak membagi q, maka dapat ditulis notasi $p \nmid q$ (Irawan, Hijriyah, & Habibi, 2014).

2.1.1 Teorema Algoritma Pembagian

Untuk sebarang bilangan bulat p dan n dengan $n > 0$, terdapat bilangan bulat q dan r secara tunggal, dengan $q, r \in \mathbb{Z}$, sedemikian sehingga hubungan antara bilangan p dan q dapat dinyatakan sebagai

$$p = nq + r, \qquad 0 \leq r < n.$$

Jika $n \nmid p$, maka r memenuhi ketaksamaan $0 < r < n$ (Gallian, 2012).

Bukti.

Misalkan $p, n \in \mathbb{Z},\ p > 0$.

Perhatikan himpunan berikut:

$$S = \{p - na \mid a \in \mathbb{Z},\ p - na \geq 0\}.$$

Akan dibuktikan bahwa $S \neq 0$.

Perhatikan kasus berikut:

(1) Misalkan $a = p$. Jika $p \leq 0$, dan karena $1 - n \leq 0$, maka:

$$p - np = (1 - n)p \geq 0.$$

(2) Jikaa $p > 0$, pilih $a = -1$, maka:

$$p - na = p - n(-1) = p + n \geq 0.$$

Oleh karena itu, $S \neq 0$.

Akan dibuktikan terdapat bilangan bulat q dan r.

(1) Misalkan $0 \in S$. Maka $p - na = 0$ untuk suatu $a \in \mathbb{Z}$.

Sehingga bisa dipilih $r = 0$ dan $p = nq \Longrightarrow q = \frac{p}{n}$.

(2) Misalkan $0 \notin S$. Karena S adalah subhimpunan tak kosong dari himpunan bilangan asli, maka S memenuhi prinsip terurut baik, yaitu S memiliki unsur terkecil. Misalkan $r \in S$ adalah unsur terkecil tersebut, maka dapat ditulis $r = p - nq$, untuk suatu $q \in \mathbb{Z}$.

Jelas bahwa $r \geq 0$, selanjutnya akan ditunjukkan bahwa $r < n$.

Andaikan $r \geq n$. Sehingga diperoleh:

$$r - n \geq 0$$

$$(p - nq) - n \geq 0$$

$$p - nq - n \geq 0$$

$$p - n(q + 1) \geq 0$$

Artinya $p - n(q + 1) \in S$ dan $p - n(q + 1) < p - nq$. Hal ini kontradiksi dengan $p - nq$ sebagai unsur terkecil di S. Jadi haruslah $0 \leq r < n$.

Selanjutnya akan ditunjukkan q dan r tunggal. Misalkan terdapat bilangan $q',\ r' \in \mathbb{Z}$, sehingga $p = nq' + r'$, dengan $0 \leq r' < n$ dan $r' \geq r$. Dapat dituliskan sebagai:

$$p = nq' + r' \geq 0$$

$$nq + r = nq' + r' \geq 0$$

$$nq - nq' = r' - r \geq 0$$

$$n(q - q') = r' - r \geq 0$$

Artinya, n membagi $r' - r$, akan tetapi $r' - r < n$, maka haruslah $r' - r = 0$.

Jadi, diperoleh $r' = r$ dan $q' = q$.

Dengan demikian, q dan r adalah tunggal.

Bilangan bulat q dalam algoritma pembagian disebut hasil bagi yang diperolah dari pembagian p oleh n. Bilangan bulat r disebut sisa hasil bagi p oleh n (Gallian, 2012).

2.1.2 Faktor Persekutuan Terbesar (FPB)

Misalkan terdapat dua bilangan bulat yang tidak keduanya nol yaitu p dan q. Faktor persekutuan terbesar (FPB – greatest common divisor atau *GCD*) dari p dan q merupakan bilangan bulat terbesar s sehingga $s \mid p$ dan $s \mid q$. Dapat kita tuliskan sebagai $FPB(p, q) = s$ (Munir, Teori Bilangan (Number Theory), 2004).

Definisi 2.1.2 Relatif Prima

Dua buah bilangan bulat p dan n disebut relatif prima jika $FPB(p, n) = 1$ (Sansani, 2008).

2.2 Aritmetika Modulo

Penggunaan aritmetika modulo dengan operator mod berperan penting dalam aplikasi kriptografi (Sansani, 2008). Penggunaan operator mod dalam

pembagian bilangan bulat akan menghasilkan sisa pembagian (Sansani, 2008). Berikut ini merupakan definisi operator mod :

Definisi 2.2.1

Misalkan p dan n merupakan bilangan bulat dengan $n > 0$. Operasi p mod n (dibaca "p modulo n") menghasilkan sisa jika p dibagi dengan n. Dapat dinyatakan pula sebagai p mod $n = r$ sedemikian sehingga $p = nq + r$, dengan $0 \leq r < n$ (Sansani, 2008).

Jika p merupakan kelipatan dari n, maka diperoleh p mod $n = 0$, yaitu n membagi habis p (Sansani, 2008).

Contoh 2.2.2

Berikut ini adalah beberapa contoh penggunaan operator modulo :

i. $29 \bmod 5 = 4,\ (29 = 5 \cdot 5 + 4)$
ii. $0 \bmod 15 = 0,\ (0 = 15 \cdot 0 + 0)$
iii. $-47 \bmod 7 = 2,\ (-47 = 7(-7) + 2)$

2.3 Kongruensi

Konsep kongruensi dapat digunakan untuk mengkaji lebih dalam konsep keterbagian dalam bilangan bulat beserta sifat-sifatnya (Irawan, Hijriyah, & Habibi, 2014).

Definisi 2.3.1

Jika sebuah bilangan bulat m yang tidak nol, membagi selisih $p - q$, maka kita katakan p kongruen modulo m dengan q, ditulis dengan (Irawan, Hijriyah, & Habibi, 2014):

$$p \equiv q \pmod{m} \qquad (2.\ 1)$$

Jika $p - q$ tidak terbagi oleh m, maka p dikatakan tidak kongruen modulo m dengan q, dituliskan dengan (Irawan, Hijriyah, & Habibi, 2014):

$$p \not\equiv q \pmod{m} \qquad (2.\ 2)$$

Kekongruenan $p \equiv q \pmod{m}$ dapat dituliskan pula dalam bentuk :

$$p = q + km \qquad (2.\ 3)$$

dengan k merupakan bilangan bulat (Munir, Teori Bilangan (Number Theory), 2004).

Contoh 2.3.2

i. $29 \equiv 7 \pmod{11}$ dapat dituliskan sebagai $29 = 7 + 2 \cdot 11$
ii. $-7 \equiv 15 \pmod{11}$ dapat dituliskan dengan $-7 = 15 + (-2)11$

2.4 Balikan Modulo (*Invers* Modulo)

Balikan (*invers*) dari p modulo n dapat ditemukan apabila p dan n relatif prima yaitu $FPB(p, n) = 1$ dengan $n > 1$ (Sansani, 2008). Suatu bilangan bulat p^{-1} merupakan balikan dari p modulo n, sedemikian sehingga $pp^{-1} \equiv 1\ mod\ n$. Berdasarkan definisi relatif prima, diketahui bahwa $FPB(p, n) = 1$, maka terdapat bilangan bulat a dan q sedemikian sehingga (Sansani, 2008)

$$ap + qn = 1$$

Yang mengimplikasikan bahwa

$$ap + qn \equiv 1 \pmod{n}$$

Karena $qn \equiv 0 \pmod{n}$, maka diperoleh

$$ap \equiv 1 \pmod{n}$$

Berdasarkan penjelasan di atas, balikan dari p modulo n dapat kita cari dengan cara membuat kombinasi linear dari p modulo n sehingga sama dengan 1.

Koefisien a yang diperoleh dari kombinasi linear tersebut merupakan balikan dari p modulo n (Munir, Teori Bilangan (Number Theory) , 2004).

Terdapat beberapa alasan penggunaan aritmetika modulo digunakan untuk beberapa algoritma kriptografi, yaitu sebagai berikut (Munir, Teori Bilangan (Number Theory), 2004):

i. Karena nilai aritmetika modulo berada dalam himpunan berhingga, yaitu 0 sampai dengan modulo $m - 1$. Sehingga kita tidak perlu khawatir dengan hasil perhitungan.
ii. Karena dalam kriptografi bekerja dengan bilangan bulat, maka kita tidak khawatir dengan kehilangan informasi yang disebabkan oleh pembulatan.

2.5 Kriptografi

Kriptografi atau *cryptography* berasal dari Bahasa Yunani yaitu “cryptos” berarti rahasia, dan “*graphein*” berarti tulisan. Sehingga, secara harfiah, kriptografi berarti tulisan rahasia (Munir, Kriptografi Edisi Kedua, 2019). Suatu ilmu dan seni yang mempelajari bagaimana merahasiakan suatu informasi dengan cara mengubah informasi tersebut ke dalam suatu bentuk yang tidak mudah dibaca oleh orang yang tidak berhak disebut kriptografi (Suhelna, 2020). Pada saat ini, kriptografi dibutuhkan bukan hanya sekedar *privacy*, akan tetapi juga bertujuan untuk *data integrity*, *authentication*, dan *non-repudiation* (Munir, informatika.stei.itb.ac.id). Terdapat beberapa aspek keamanan yang menjadi tujuan utama dalam sistem kriptografi (Munir, Kriptografi, 2006), diantaranya sebagai berikut :

1. Kerahasiaan (*confidentiality*)

Masalah keamanan pesan yang disebut kerahasian adalah bagaimana cara mengamankan pesan agar tidak mudah dibaca orang yang tidak berhak (Munir, Kriptografi Edisi Kedua, 2019). Pendekatan yang digunakan untuk menjaga kerahasiaan secara fisik yaitu algoritma matematika yang membuat data tidak dapat mudah dipahami.

2. Integritas Data (*data integrity*)

Penerima pesan menginginkan pesan yang telah diterima adalah pesan asli yang belum diubah, ditambah, maupun dihapus (Munir, Kriptografi Edisi Kedua, 2019). Integritas data dapat dijaga dengan adanya kemampuan sistem untuk mendeteksi manipulasi data yang menyangkut masalah penyisipan, penghapusan, dan pensubstitusian data.

3. Otentikasi (*authentication*)

Identitas yang dilakukan oleh pihak yang saling berkomunikasi disebut otentikasi. Identifikasi terhadap informasi yang diperoleh bertujuan untuk memastikan keaslian informasi tersebut. Identifikasi tersebut dapat berupa tanggal pembuatan, isi informasi, atau waktu kirim. Sehingga dapat dipastikan bahwa yang mengirimkan pesan adalah orang yang sesuai bukan orang lain yang menyamar (Munir, Kriptografi Edisi Kedua, 2019).

4. Anti Penyangkalan (*non-repudiation*)

Apabila terdapat kasus pengirim pesan menyangkal telah mengirim pesan atau penerima pesan menyangkal telah menerima pesan, maka dapat dilakukan pembuktian ketidakbenaran penyangkalan tersebut (Munir, Kriptografi Edisi Kedua, 2019).

Sistem kriptografi secara umum dapat terdiri dari lima bagian, diantaraya sebagai berikut (Nadeak, 2019):

1. Pesan Asli *(Plaintext)*

   Plaintext merupakan pesan dalam bentuk asli dan dapat terbaca. *Plaintext* dapat juga disebut teks asli yang merupakan masukan untuk algoritma enkripsi.

2. *Secret Key*

   Secret key disebut juga kunci rahasia yang merupakan masukan algoritma enkripsi. Kunci rahasia dapat menentukan hasil *output* dari algorima enkripsi.

3. Pesan Sandi (*Ciphertext)*

   Ciphertext merupakan pesan dalam bentuk tersembunyi. Jika algortima enkripsi yang digunakan baik, maka ciphertext yang dihasilkan terlihat acak dan tidak mudah terbaca pihak lain. *Ciphertext* disebut juga teks sandi.

4. Algoritma Enkripsi

   Proses untuk menyandikan *plainteks* menjadi *cipherteks* disebut enkripsi (Munir, Kriptografi Edisi Kedua, 2019). Terdapat 2 masukan teks yaitu *plainteks* dan kunci rahasia.

5. Algoritma Dekripsi

   Proses untuk mengembalikan *ciphertext* menjadi *plaintext* disebut dekripsi (Munir, Kriptografi Edisi Kedua, 2019). Terdapat 2 masukan teks yaitu *ciphertext* dan kunci rahasia.

2.6 Kriptografi DNA

Fungsi dasar dalam kriptografi yaitu proses enkripsi dan dekripsi pesan. Berikut adalah simbol yang digunakan untuk proses enkripsi.

$$E_K(M) = C$$

Berikut adalah simbol yang digunakan untuk proses dekripsi.

$$D_K(C) = M$$

Keterangan:

E : Fungsi enkripsi

D : Fungsi dekripsi

M : Pesan asli (*plaintext*)

C : Pesan dalam bahasa sandi (*ciphertext*)

K : Kunci enkripsi atau dekripsi

Heider dan Barnekow merupakan peneliti yang pada tahun 2007 mengajukan sebuah algoritma yang digunakan untuk mengkodekan informasi biner menjadi barisan DNA (Hardjo, 2016). Pada sistem bilangan biner, terdapat bilangan yang saling berkomplemen yaitu 0 dan 1 atau 00 dan 11, 10 dan 01 (Qiao, 2015). Apabila dilakukan pengkodean bilangan biner menjadi pasangan komplemen DNA (A, T, G, C), terdapat 8 macam kombinasi pengkodean yang memenuhi aturan pasangan basa komplemen pada tabel berikut (Qiao, 2015).

Tabel 2. 1 Delapan Macam 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

Setelah menerima *plaintext* yang akan disandikan, proses enkripsi pesan menggunakan kriptografi DNA terdiri dari beberapa langkah yaitu sebagai berikut (Raj, J. Frank Vijay, & T. Mahalakshmi, 2016):

1. Konversi *plaintext* menjadi kode biner berdasarkan tabel ASCII.
2. Konversi kode biner dalam bentuk kode untaian DNA dengan mensubstitusikan kode DNA yang diperoleh dari Tabel 2. 1 Delapan Macam Bentuk Kombinasi Pengkodean DNA.
3. Konversi kode DNA menjadi kode desimal berdasarkan tabel kunci pembangun acak kriptografi DNA.
4. Memperoleh pesan sandi berdasarkan tabel ASCII.

Kemudian, setelah menerima *ciphertext* yang akan didekripsi, terdapat proses dekripsi pesan menggunakan kriptografi DNA. Adapun langkah-langkah dekripsi pesan adalah sebagai berikut (Raj, J. Frank Vijay, & T. Mahalakshmi, 2016):

1. Konversi pesan menjadi kode desimal berdasarkan tabel ASCII.
2. Konversi kode desimal menjadi untaian DNA berdasarkan tabel kunci pembangun acak.
3. Konversi kode DNA menjadi bentuk biner.
4. Konversi kode biner menjadi karakter berdasarkan tabel ASCII.
5. Memperoleh pesan asli.

Contoh 2.6.1 Proses Enkripsi

Konversi kriptografi DNA dengan cara mengubah “T” menjadi 11, “G” menjadi 10, “C” menjadi 01, dan “A” menjadi 00 (Raj, J. Frank Vijay, & T. Mahalakshmi, 2016).

Plaintext : BOY

Langkah 1 : Mencari nilai ASCII dari B, O, dan Y. Nilai ASCII diperoleh melalui tabel ASCII yaitu $B = 66, O = 79, Y = 89$.

$$B(66) \rightarrow 01000010 \rightarrow CAAG$$

$$O(79) \rightarrow 01001111 \rightarrow CATT$$

$$Y(89) \rightarrow 01011001 \rightarrow CCGC$$

Langkah 2 : Pesan BOY telah disubstitusikan ke dalam bentuk kombinasi DNA, diperoleh hasil konversi dari pesan BOY yaitu $CAAG - CATT - CCGC$.

Langkah 3 : Berdasarkan kunci acak tabel substitusi, kombinasi DNA $CAAG - CATT - CCGC$ akan menjadi 35,48,58.

Ciphertext : 35,48,58.

Contoh 2.6.2 Proses Dekripsi

Ciphertext : 35,48,58

Substitusikan pada kunci pembangun acak, yaitu :

$$35 \rightarrow CAAG \rightarrow 01000010 \rightarrow 66 \rightarrow B$$

$$48 \rightarrow CATT \rightarrow 01001111 \rightarrow 79 \rightarrow O$$

$$58 \rightarrow CCGC \rightarrow 01011001 \rightarrow 89 \rightarrow Y$$

Plaintext: BOY

2.7 Algoritma Kriptografi Kunci Simetri

Algoritma kunci simetri merupakan salah satu algoritma yang paling sering digunakan untuk proses enkripsi. Dalam algoritma kunci simetri, kunci tunggal digunakan untuk proses enkripsi dan dekripsi (Ayushi, 2010). Terdapat beberapa langkah untuk proses algoritma kunci simetri, yaitu sebagai berikut :

Langkah 1 : Membentuk nilai ASCII dari huruf.

Langkah 2 : Membentuk kode biner dari huruf tersebut. (Nilai biner harus 8 digit).

Langkah 3 : Balikkan kode biner tersebut.

Langkah 4 : Pilih 4 digit pembagi ($>= 1000$) sebagai kunci.

Langkah 5 : Membagi kode biner yang telah dibalik dengan pembagi.

Langkah 6 : Letakkan sisa pada 3 digit pertama dan hasil bagi pada 5 digit berikutnya (sisa dan hasil bagi tidak akan lebih dari 3 dan 5 digit). Jika diantaranya kurang dari 3 dan 5 digit , maka harus menambahkan angka 0 pada sisi kirinya. Sehingga akan terbentuk teks enkripsinya (Ayushi, 2010).

2.8 Transformasi Digraf

Analisa frekuensi akan lebih sulit jika enkripsi terhadap karakter tidak dilakukan secara satu per satu, melainkan terhadap beberapa karakter. Transformasi digraf menggunakan transformasi terhadap dua karakter sekaligus. Sebelum melakukan enkripsi, apabila jumlah huruf ganjil, maka teks dapat ditambahkan dengan karakter z sehingga menjadi genap. Setelah melakukan dekripsi, maka penambahan tersebut dapat ditiadakan kembali (Kromodimoeljo, 2009).

Algoritma yang digunakan dalam proses enkripsi teks pada transformasi digraf adalah :

$$C \equiv ap + b \ (mod\ N^2) \tag{2. 4}$$

$$p = (x + k)N + (y + k) \tag{2. 5}$$

Untuk proses dekripsi teks, menggunakan algoritma berikut (Elfadel, 2014):

$$P \equiv a'c - b' \ (mod\ N^2) \qquad (2.\ 6)$$

dimana,

$$c = (x' - k)N + (y' - k) \qquad (2.\ 7)$$

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

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

Berikut adalah keterangan penggunaan simbol pada algoritma di atas :

x : nilai numerik dari huruf pertama pada *plaintext*.

y : nilai numerik dari huruf kedua pada *plaintext*.

x' : nilai numerik dari huruf pertama pada *ciphertext*.

y' : nilai numerik dari huruf kedua pada *ciphertext*.

N : banyaknya huruf *alphabet*.

a : bilangan yang relatif prima dengan N^2.

b : sebarang bilangan acak

Dengan nilai x, y, x', dan y' adalah:

$$k \leq x, y, x', y' \leq k + 26, \qquad 0 \leq k \leq 25$$

Contoh 2.8.1 Proses Enkripsi dan Dekripsi untuk $k = 0$

Diberikan contoh untuk penggunaan nilai numerik dengan $k = 0$. Dengan langkah pengerjaan serupa dengan proses enkripsi sebelumnya, maka diperoleh hasil enkripsi sebagai berikut:

i. Proses Enkripsi

Plaintext: HELP ME→ HE LP ME

$$N = 26$$

$$N^2 = 26^2 = 676, \ \ a = 451, \ \ b = 60$$

$$p = (x + k)N + (y + k)$$

$p_1(HE) = 7 \times 26 + 4 = 186$

$p_2(LP) = 11 \times 26 + 15 = 301$

$p_3(ME) = 12 \times 26 + 4 = 316$

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

$C_1(HE) = 451 \times 186 + 60 = 83946 \equiv 122\ mod\ 676 \Rightarrow 122 = 4 \times 26 + 18 \Rightarrow (ES)$

$C_2(LP) = 451 \times 301 + 60 = 135811 \equiv 611\ mod\ 676 \Rightarrow 611 = 23 \times 26 + 13 \Rightarrow (XN)$

$C_3(ME) = 451 \times 316 + 60 = 142576 \equiv 616\ mod\ 676 \Rightarrow 616 = 23 \times 26 + 18 \Rightarrow (XS)$

Diperoleh *ciphertext* yaitu ESXNXS**.**

ii. Proses Dekripsi

Ciphertext: ESXNXS

$$P \equiv a^{-1}c - a^{-1}b\ (mod\ N^2)$$

$$a^{-1} = x, \quad x \times a \equiv 1\ mod\ 676$$

$a^{-1} = 3$ karena $3 \times 451 = 1353 \equiv 1\ mod\ 676$.

$$a^{-1}b = 3 \times 60 = 180$$

$P_1(ES) = 3 \times 122 - 180 = 186 \equiv 186\ mod\ 676$

$P_2(XN) = 3 \times 611 - 180 = 1653 \equiv 301\ mod\ 676$

$P_3(XS) = 3 \times 616 - 180 = 1668 \equiv 316\ mod\ 676$

$$c = x'N + y'$$

$c_1(ES) = 186 = 7 \times 26 + 4 \Rightarrow HE$

$c_2(XN) = 301 = 11 \times 26 + 15 \Rightarrow LP$

$c_3(XS) = 316 = 12 \times 26 + 4 \Rightarrow ME$

Plaintext : HELP ME

Contoh 2.8.2 Proses Enkripsi dan Dekripsi untuk $k = 9$

Akan diberikan contoh untuk penggunaan nilai numerik dengan $k = 9$. Dengan langkah pengerjaan serupa dengan proses enkripsi sebelumnya, maka diperoleh hasil enkripsi sebagai berikut:

$p(DO) \quad = (x + k)N + (y + k) \quad = 12 \times 26 + 23 \quad = 335$

$C(DO) \quad \equiv ap + b \ (mod\ N^2) \quad \equiv 49 \times 335 + 10(mod\ 676)$

$\equiv 16425 \ (mod\ 676) \quad \equiv 201 \ (mod\ 676) = 201$

$C(DO) \quad = 201 = (7 + 9) \times 26 + (19 + 9) \quad = 16 \times 26 + 28 \rightarrow HT$

Selanjutnya, akan diberikan contoh untuk proses dekripsi dengan langkah pengerjaan serupa dengan proses dekripsi sebelumnya, maka diperoleh hasil dekripsi sebagai berikut:

$c'(HT) \quad = (x' - k)N + (y' - k) \quad = (16 - 9) \times 26 + (28 - 9) \quad = 201$

$P(HT) \quad \equiv a^{-1}c'_{16} - a^{-1}b \ (mod\ N^2) \quad \equiv 69 \times 201 - 14(mod\ 676)$

$\equiv 13855 \ (mod\ 676) \quad \equiv 335 \ (mod\ 676) = 335$

$P(HT) \quad = 335 = (12 - 9) \times 26 + (23 - 9) = 7 \times 26 + 18 \quad \rightarrow DO$

2.9 Analisis Frekuensi

Proses enkripsi dan dekripsi yang menggunakan *cipher* substitusi memiliki beberapa kelemahan. Salah satunya adalah tidak dapat menyembunyikan hubungan statistik antara *plaintext* dan *ciphertextnya* (Munir, Kriptografi Edisi Kedua, 2019). Hal tersebut dapat diketahui dari huruf yang paling sering muncul pada *plaintext* akan sering muncul juga pada *ciphertext*. Kelemahan tersebut

menjadi dasar untuk melakukan kriptanalisis menggunakan metode analisis frekuensi (Munir, Kriptografi Edisi Kedua, 2019). Kriptanalis menggunakan metode tersebut dengan cara menggunakan tabel frekuensi munculnya huruf-huruf, sehingga mampu menerka huruf *plaintext* (Munir, Kriptografi Edisi Kedua, 2019). Terdapat tabel frekuensi huruf dalam Bahasa Inggris yang memperlihatkan kemunculan huruf-huruf *alphabet* yang diambil dari sampel sebanyak 300.000 karakter (Munir, Kriptografi Edisi Kedua, 2019).

Tabel 2. 2 Frekuensi Kemunculan (Relatif) Huruf Dalam Bahasa Inggris

Huruf	**%**	**Huruf**	**%**	**Huruf**	**%**	**Huruf**	**%**
a	8,2	**h**	6,1	**o**	7,5	**v**	1,0
b	1,5	**i**	7,0	**p**	1,9	**w**	2,4
c	2,8	**j**	0,1	**q**	0,1	**x**	2,0
d	4,2	**k**	0,8	**r**	6,0	**y**	0,1
e	12,7	**l**	4,0	**s**	6,3	**z**	0,1
f	2,2	**m**	2,4	**t**	9,0		
g	2,0	**n**	6,7	**u**	2,8		

Metode analisis frekuensi dilakukan dalam beberapa langkah sebagai berikut (Munir, Kriptografi Edisi Kedua, 2019):

1. Mengasumsikan *plaintext* dienkripsi dengan *cipher* abjad tunggal.
2. Melakukan perhitungan frekuensi kemunculan relatif huruf-huruf dalam *ciphertext*.
3. Membandingkan hasil pada langkah kedua dengan Tabel 2. 2 Frekuensi Kemunculan (Relatif) Huruf Dalam Bahasa Inggris.
4. Mengulangi langkah untuk huruf dengan frekuensi terbanyak berikutnya.

2.10 Kajian Keagamaan

Masing-masing individu memiliki ciri-ciri yang berbeda. Dalam menilai kepribadian seseorang, ciri-ciri jasad kurang penting dibandingkan dengan ciri-ciri ruh. Ciri-ciri seseorang yang berkaitan dengan ruh dimaksud dengan pengertian akhlak (Wassil, 2009). Agama Islam mengajarkan orang mukmin untuk berakhlak mulia. Terdapat beberapa ayat Al Quran yang menjelaskan tentang ciri-ciri utama orang beriman. Salah satu ayat Al Quran tersebut adalah surat Al Mukminun ayat 8 yang artinya:

"Dan orang-orang yang memelihara amanah-amanah (yang dipikulnya) dan janjinya". (QS. Al-Mukminun/23:8).

Ayat tersebut menggambarkan salah satu sifat orang mukmin adalah memelihara janji dan amanah yang dipikulnya, baik amanah dari Allah Swt. maupun dari sesama manusia. Orang mukmin menunaikan amanat kepada yang berhak dan tidak berkhianat. Apabila berjanji, orang mukmin akan menepati syarat-syarat perjanjian (Az-Zuhaili, 2013). Seorang yang amanah dapat menghindarkan diri dari sifat munafik yang memiliki 3 tanda yaitu, apabila berbicara suka berdusta, apabila berjanji suka mengingkari dan apabila diberi amanah atau dipercaya suka berkhianat (RI, 2011).

Kebanyakan ulama membaca dengan lafadzh لِأَمَٰنَٰتِهِمْ, yakni dalam bentuk jamak. Sedangkan, lafadzh yang dibaca oleh Ibnu Katsir yaitu لِأَمَانَتِهِمْ, yaitu dalam bentuk tunggal (Imam, 2008). 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 (Imam, 2008). Bentuk amanah Allah Swt. terhadap hamba-Nya yaitu harus melaksanakan

apa yang Allah perintahkan dan menjauhi larangan Allah. Sedangkan amanah seseorang terhadap sesamanya diantaranya yaitu mengembalikan barang titipan kepada yang memiliki, tidak melakukan penipuan, serta menjaga rahasia orang lain (Abidin, 2017).

Adanya proses enkripsi dan dekripsi pesan memberikan pengajaran untuk selalu berbuat jujur dan amanah dalam melakukan segala perbuatan. Konsep amanah dan menjaga rahasia dalam Al Quran Surat Al-Mukminun ayat 8 digunakan sebagai pengingat untuk selalu berkata jujur dan amanah dalam menjaga rahasia. Selain itu, proses analisis frekuensi mengajarkan untuk berhati-hati dalam menerima pesan dari orang yang belum jelas kebenarannya. Sehingga tidak akan ada perselisihan yang disebabkan ketidakjujuran. Sebagai seorang mukmin sudah seharusnya berusaha untuk memiliki akhlak mulia salah satunya adalah dengan berkata jujur, menjaga rahasia dan amanah dalam segala perbuatannya. Karena setiap perbuatan dan amanah akan diminta pertanggungjawaban oleh Allah Swt.

BAB III
PEMBAHASAN

3.1 Proses Enkripsi Pesan Teks

Berikut ini merupakan penurunan proses enkripsi pesan teks menggunakan algoritma transformasi digraf.

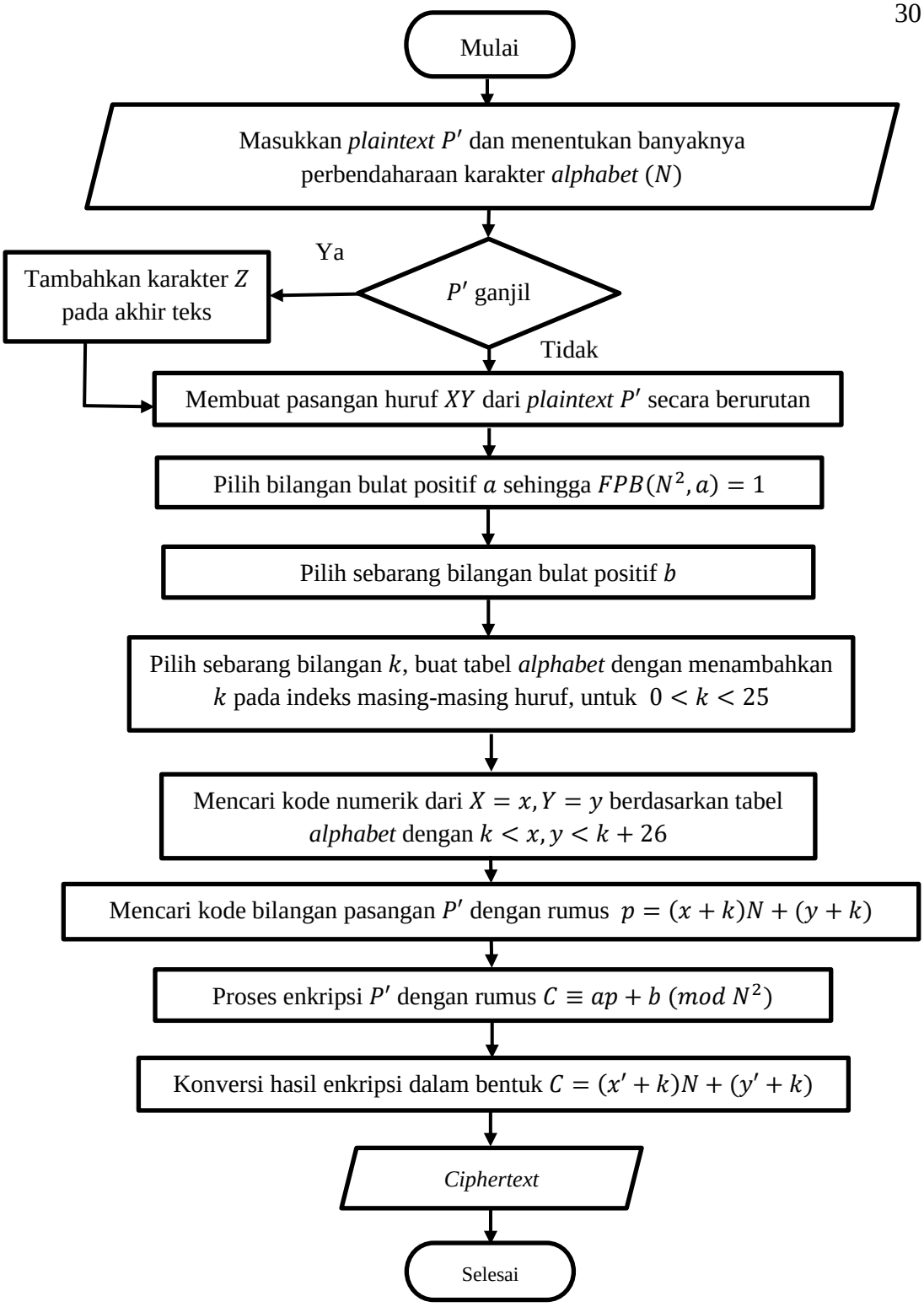
Misalkan a adalah bilangan bulat positif yang relatif prima dengan N^2 dan $h \in \mathbb{Z}$.

$C \equiv ap + b \ (mod\ N^2)$	Rumus enkripsi
$N^2 \mid C - (ap + b\ )$	Definisi kongruensi
$C - (ap + b\ ) = N^2 \cdot h$	Definisi keterbagian
$C - ap - b = N^2 \cdot h$	Sifat distributif

Karena a relatif prima dengan N^2, berarti $FPB(a, N^2) = 1$. Oleh karena itu, a memiliki *invers* modulo N^2, yaitu disimbolkan dengan a^{-1}.

$a^{-1} \times (C - ap - b) = (N^2 \cdot h) \times a^{-1}$	Kedua ruas dikalikan a^{-1}
$a^{-1}C - a^{-1}ap - a^{-1}b = N^2 \cdot (a^{-1}h)$	Sifat distributif
$a^{-1}C - p - a^{-1}b = N^2 \cdot (a^{-1}h)$	Sifat invers
$-1 \times (a^{-1}C - p - a^{-1}b) = (N^2 \cdot (a^{-1}h)) \times -1$	Kedua ruas dikalikan -1
$-a^{-1}C + p + a^{-1}b = N^2 \cdot (-a^{-1}h)$	Sifat distributif
$p + a^{-1}b - a^{-1}C = N^2 \cdot (-a^{-1}h)$	Sifat komutatif
$p - (a^{-1}C - a^{-1}b) = N^2 \cdot (-a^{-1}h)$	Sifat distributif
$N^2 \mid \big(p - (a^{-1}C - a^{-1}b)\big)$	Definisi keterbagian
$p \equiv a^{-1}C - a^{-1}b (mod\ N^2)$	Definisi kongruensi

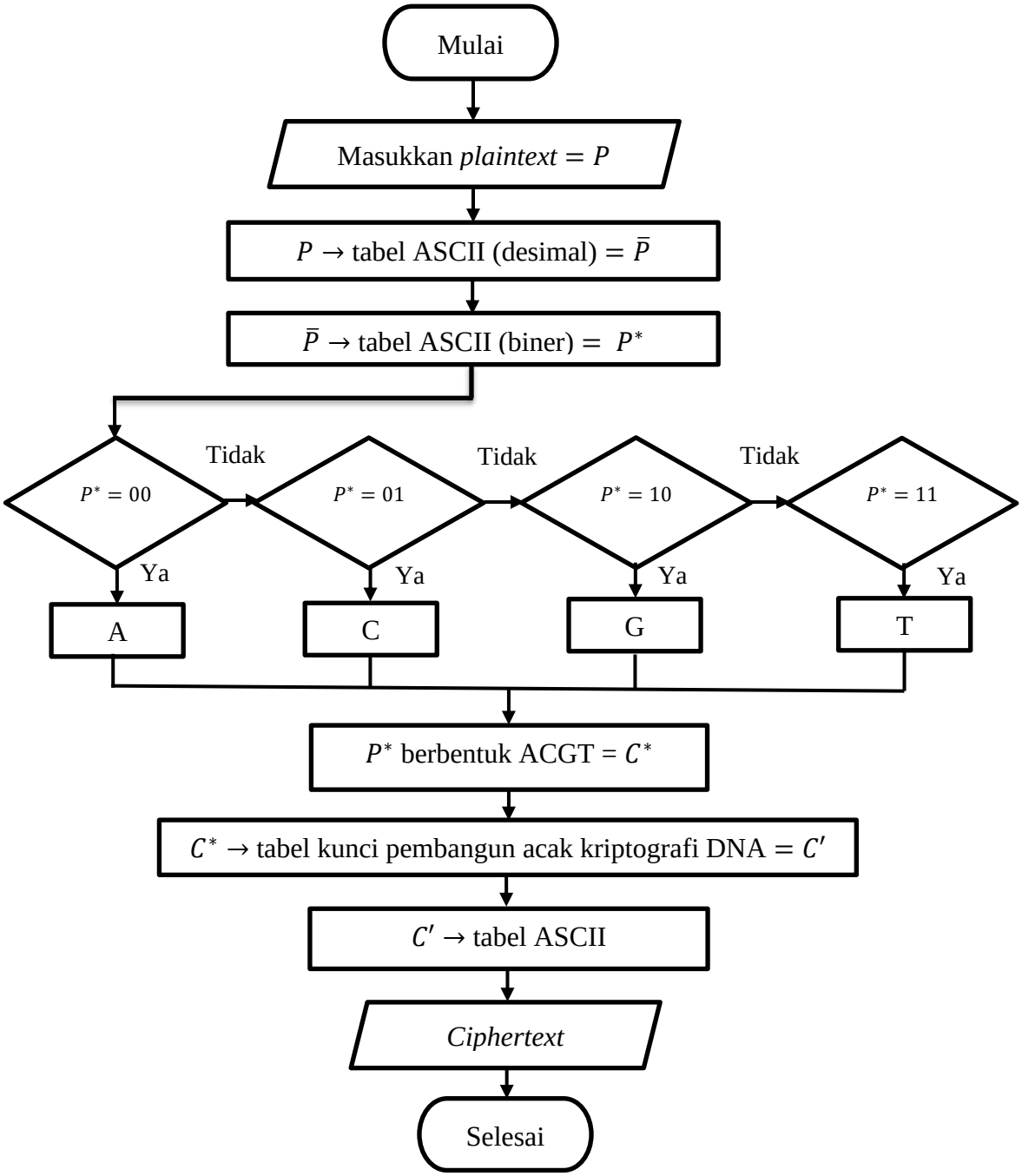
Kemudian akan ditunjukkan *flowchart* untuk proses enkripsi pesan teks menggunakan algoritma transformasi digraf, sebagai berikut:



Gambar 3.1 *Flowchart* Proses Enkripsi Algoritma Transformasi Digraf

Langkah selanjutnya adalah proses enkripsi pesan teks menggunakan algoritma kritografi DNA. *Plaintext* yang digunakan untuk proses enkripsi menggunakan algoritma kriptografi DNA merupakan *ciphertext* yang diperoleh

dari hasil enkripsi dengan transformasi digraf. Berikut merupakan *flowchart* untuk proses enkripsi pesan teks menggunakan algoritma kriptografi DNA.



Gambar 3.2 *Flowchart* Proses Enkripsi Algoritma Kriptografi DNA

Selanjutnya adalah contoh proses enkripsi pesan teks menggunakan algoritma transformasi digraf. *Plaintext* yang digunakan yaitu DO SOMETHING TODAY THAT YOUR FUTURE WILL THANK YOU FOR IT BECAUSE

SUCCESS COMES FROM WHAT YOU DO CONSISTENLY. Langkah pertama, memecah *plaintext* secara berpasangan. *Plaintext* dipecah menjadi:

DO	SO	ME	TH	IN	GT	OD	AY	TH
AT	YO	UR	FU	TU	RE	WI	LL	TH
AN	KY	OU	FO	RI	TB	EC	AU	SE
SU	CC	ES	SC	OM	ES	FR	OM	WH
AT	YO	UD	OC	ON	SI	ST	EN	LY

Banyak perbendaharaan karakter yang dipilih adalah huruf kapital A – Z, yaitu sebanyak 26, disimbolkan dengan $N = 26$, untuk penggunaan nilai numerik dengan $k = 0$. Karena pada transformasi digraf, dilakukan perubahan terhadap 2 karakter, maka jumlah kemungkinan perubahan huruf sebanyak $N^2 = 26^2 = 676$. Kemudian, penulis harus mencari bilangan a yang relatif prima dengan $N^2 = 676$. Agar parameter a memiliki *invers*, maka haruslah $\text{FPB}(a, N^2) = 1$. Bilangan a yang dipilih adalah 49, karena $\text{FPB}(49, 676) = 1$. Sedangkan sebarang bilangan bulatv positif b yang dipilih adalah 10. Sehingga diperoleh nilai sebagai berikut:

$$N = 26$$

$$N^2 = 26^2 = 676$$

$$a = 49$$

$$b = 10$$

Langkah selanjutnya, menentukan kode bilangan masing-masing pasangan berdasarkan nilai numerik yang diperoleh dari tabel *alphabet*. Kode bilangan diperoleh melalui persamaan (2. 5), sehingga dapat diperoleh:

$p_1(DO) \quad = x_1 N + y_1 \quad = 3 \times 26 + 14 \quad = 92$

$$p_2(SO) = x_2N + y_2 = 18 \times 26 + 14 = 482$$

$$p_3(ME) = x_3N + y_3 = 12 \times 26 + 4 = 316$$

$$p_4(TH) = x_4N + y_4 = 19 \times 26 + 7 = 501$$

$$p_5(IN) = x_5N + y_5 = 8 \times 26 + 13 = 221$$

$$p_6(GT) = x_6N + y_6 = 6 \times 26 + 19 = 175$$

$$p_7(OD) = x_7N + y_7 = 14 \times 26 + 3 = 367$$

$$p_8(AY) = x_8N + y_8 = 0 \times 26 + 24 = 24$$

$$p_9(TH) = x_9N + y_9 = 19 \times 26 + 7 = 501$$

$$p_{10}(AT) = x_{10}N + y_{10} = 0 \times 26 + 19 = 19$$

$$p_{11}(YO) = x_{11}N + y_{11} = 24 \times 26 + 14 = 638$$

$$p_{12}(UR) = x_{12}N + y_{12} = 20 \times 26 + 17 = 537$$

$$p_{13}(FU) = x_{13}N + y_{13} = 5 \times 26 + 20 = 150$$

$$p_{14}(TU) = x_{14}N + y_{14} = 19 \times 26 + 20 = 514$$

$$p_{15}(RE) = x_{15}N + y_{15} = 17 \times 26 + 4 = 446$$

$$p_{16}(WI) = x_{16}N + y_{16} = 22 \times 26 + 8 = 580$$

$$p_{17}(LL) = x_{17}N + y_{17} = 11 \times 26 + 11 = 297$$

$$p_{18}(TH) = x_{18}N + y_{18} = 19 \times 26 + 7 = 501$$

$$p_{19}(AN) = x_{19}N + y_{19} = 0 \times 26 + 13 = 13$$

$$p_{20}(KY) = x_{20}N + y_{20} = 10 \times 26 + 24 = 284$$

$$p_{21}(OU) = x_{21}N + y_{21} = 14 \times 26 + 20 = 384$$

$$p_{22}(FO) = x_{22}N + y_{22} = 5 \times 26 + 14 = 144$$

$$p_{23}(RI) = x_3N + y_{23} = 17 \times 26 + 8 = 450$$

$$p_{24}(TB) = x_{24}N + y_{24} = 19 \times 26 + 1 = 495$$

$$p_{25}(EC) = x_{25}N + y_{25} = 4 \times 26 + 2 = 106$$

$$p_{26}(AU) = x_{26}N + y_{26} = 0 \times 26 + 20 = 20$$

$$p_{27}(SE) = x_{27}N + y_{27} = 18 \times 26 + 4 = 472$$

$$p_{28}(SU) = x_{28}N + y_{28} = 18 \times 26 + 20 = 488$$

$$p_{29}(CC) = x_{29}N + y_{29} = 2 \times 26 + 2 = 54$$

$$p_{30}(ES) = x_{30}N + y_{30} = 4 \times 26 + 18 = 122$$

$$p_{31}(SC) = x_{31}N + y_{31} = 18 \times 26 + 2 = 470$$

$$p_{32}(OM) = x_{32}N + y_{32} = 14 \times 26 + 12 = 376$$

$$p_{33}(ES) = x_{33}N + y_{33} = 4 \times 26 + 18 = 122$$

$$p_{34}(FR) = x_{34}N + y_{34} = 5 \times 26 + 17 = 147$$

$$p_{35}(OM) = x_{35}N + y_{35} = 14 \times 26 + 12 = 376$$

$$p_{36}(WH) = x_{36}N + y_{36} = 22 \times 26 + 7 = 579$$

$$p_{37}(AT) = x_{37}N + y_{37} = 0 \times 26 + 19 = 19$$

$$p_{38}(YO) = x_{38}N + y_{38} = 24 \times 26 + 14 = 638$$

$$p_{39}(UD) = x_{39}N + y_{39} = 20 \times 26 + 3 = 523$$

$$p_{40}(OC) = x_{40}N + y_{40} = 14 \times 26 + 2 = 366$$

$$p_{41}(ON) = x_{41}N + y_{41} = 14 \times 26 + 13 = 377$$

$$p_{42}(SI) = x_{42}N + y_{42} = 18 \times 26 + 8 = 476$$

$$p_{43}(ST) = x_{43}N + y_{43} = 18 \times 26 + 19 = 487$$

$$p_{44}(EN) = x_{44}N + y_{44} = 4 \times 26 + 13 = 117$$

$$p_{45}(LY) = x_{45}N + y_{45} = 11 \times 26 + 24 = 310$$

Langkah berikutnya melakukan enkripsi menggunakan persamaan (2. 4), dan mengubah hasil enkripsi tersebut ke dalam bentuk persamaan (2. 5). Sehingga proses enkripsi dapat dituliskan sebagai berikut:

$$C_1(DO) \equiv ap_1 + b\ (mod\ N^2) \equiv 49 \times 92 + 10(mod\ 676)$$
$$\equiv 4518\ (mod\ 676) \equiv 462\ (mod\ 676) = 462$$
$$C_1(DO) = 462 = 17 \times 26 + 20 \rightarrow RU$$
$$C_2(SO) \equiv ap_2 + b(mod\ N^2) \equiv 49 \times 482 + 10(mod\ 676)$$
$$\equiv 23628\ (mod\ 676) \equiv 644\ (mod\ 676) = 644$$
$$C_2(SO) = 644 = 24 \times 26 + 20 \rightarrow YU$$
$$C_3(ME) \equiv ap_3 + b(mod\ N^2) \equiv 49 \times 316 + 10(mod\ 676)$$
$$\equiv 15494\ (mod\ 676) \equiv 622\ (mod\ 676) = 622$$
$$C_3(ME) = 622 = 23 \times 26 + 24 \rightarrow XY$$
$$C_4(TH) \equiv ap_4 + b(mod\ N^2) \equiv 49 \times 501 + 10(mod\ 676)$$
$$\equiv 24559\ (mod\ 676) \equiv 223\ (mod\ 676) = 223$$
$$C_4(TH) = 223 = 8 \times 26 + 15 \rightarrow IP$$
$$C_5(IN) \equiv ap_5 + b(mod\ N^2) \equiv 49 \times 221 + 10(mod\ 676)$$
$$\equiv 10839\ (mod\ 676) \equiv 23\ (mod\ 676) = 23$$
$$C_5(IN) = 23 = 0 \times 26 + 23 \rightarrow AX$$
$$C_6(GT) \equiv ap_6 + b(mod\ N^2) \equiv 49 \times 175 + 10(mod\ 676)$$
$$\equiv 8585\ (mod\ 676) \equiv 473\ (mod\ 676) = 473$$
$$C_6(GT) = 473 = 18 \times 26 + 5 \rightarrow SF$$
$$C_7(OD) \equiv ap_7 + b(mod\ N^2) \equiv 49 \times 367 + 10(mod\ 676)$$
$$\equiv 17993\ (mod\ 676) \equiv 417\ (mod\ 676) = 417$$
$$C_7(OD) = 417 = 16 \times 26 + 1 \rightarrow QB$$
$$C_8(AY) \equiv ap_8 + b(mod\ N^2) \equiv 49 \times 24 + 10(mod\ 676)$$
$$\equiv 1186\ (mod\ 676) \equiv 510\ (mod\ 676) = 510$$

$$C_8(AY) = 510 = 19 \times 26 + 16 \rightarrow TQ$$

$$C_9(TH) \equiv ap_9 + b(mod\ N^2) \equiv 49 \times 501 + 10(mod\ 676)$$

$$\equiv 24559\ (mod\ 676) \equiv 223\ (mod\ 676) = 223$$

$$C_9(TH) = 223 = 8 \times 26 + 15 \rightarrow IP$$

$$C_{10}(AT) \equiv ap_{10} + b(mod\ N^2) \equiv 49 \times 19 + 10(mod\ 676)$$

$$\equiv 941\ (mod\ 676) \equiv 265\ (mod\ 676) = 265$$

$$C_{10}(AT) = 265 = 10 \times 26 + 5 \rightarrow KF$$

$$C_{11}(YO) \equiv ap_{11} + b(mod\ N^2) \equiv 49 \times 638 + 10(mod\ 676)$$

$$\equiv 31272\ (mod\ 676) \equiv 176\ (mod\ 676) = 176$$

$$C_{11}(YO) = 176 = 6 \times 26 + 20 \rightarrow GU$$

$$C_{12}(UR) \equiv ap_{12} + b(mod\ N^2) \equiv 49 \times 537 + 10(mod\ 676)$$

$$\equiv 26323\ (mod\ 676) \equiv 635\ (mod\ 676) = 635$$

$$C_{12}(UR) = 635 = 24 \times 26 + 11 \rightarrow YL$$

$$C_{13}(FU) \equiv ap_{13} + b(mod\ N^2) \equiv 49 \times 150 + 10(mod\ 676)$$

$$\equiv 7360\ (mod\ 676) \equiv 600\ (mod\ 676) = 600$$

$$C_{13}(FU) = 600 = 23 \times 26 + 2 \rightarrow XC$$

$$C_{14}(TU) \equiv ap_{14} + b(mod\ N^2) \equiv 49 \times 514 + 10(mod\ 676)$$

$$\equiv 25196\ (mod\ 676) \equiv 184\ (mod\ 676) = 184$$

$$C_{14}(TU) = 184 = 7 \times 26 + 2 \rightarrow HC$$

$$C_{15}(RE) \equiv ap_{15} + b(mod\ N^2) \equiv 49 \times 446 + 10(mod\ 676)$$

$$\equiv 21864\ (mod\ 676) \equiv 232\ (mod\ 676) = 232$$

$$C_{15}(RE) = 232 = 8 \times 26 + 24 \rightarrow IY$$

$$C_{16}(WI) \equiv ap_{16} + b(mod\ N^2) \equiv 49 \times 580 + 10(mod\ 676)$$

$$\equiv 28430\ (mod\ 676) \qquad \equiv 38\ (mod\ 676) = 38$$

$$C_{16}(WI) \quad = 38 = 1 \times 26 + 12 \qquad \rightarrow BM$$

$$C_{17}(LL) \quad \equiv ap_{17} + b(mod\ N^2) \qquad \equiv 49 \times 297 + 10(mod\ 676)$$

$$\equiv 14563\ (mod\ 676) \qquad \equiv 367\ (mod\ 676) = 367$$

$$C_{17}(LL) \quad = 367 = 14 \times 26 + 3 \qquad \rightarrow OD$$

$$C_{18}(TH) \quad \equiv ap_{18} + b(mod\ N^2) \qquad \equiv 49 \times 501 + 10(mod\ 676)$$

$$\equiv 24559\ (mod\ 676) \qquad \equiv 223\ (mod\ 676) = 223$$

$$C_{18}(TH) \quad = 223 = 8 \times 26 + 15 \qquad \rightarrow IP$$

$$C_{19}(AN) \quad \equiv ap_{19} + b(mod\ N^2) \qquad \equiv 49 \times 13 + 10(mod\ 676)$$

$$\equiv 647\ (mod\ 676) \qquad \equiv 647\ (mod\ 676) = 647$$

$$C_{19}(AN) \quad = 647 = 24 \times 26 + 23 \qquad \rightarrow YX$$

$$C_{20}(KY) \quad \equiv ap_{20} + b(mod\ N^2) \qquad \equiv 49 \times 284 + 10(mod\ 676)$$

$$\equiv 13926\ (mod\ 676) \qquad \equiv 406\ (mod\ 676) = 406$$

$$C_{20}(KY) \quad = 406 = 15 \times 26 + 16 \qquad \rightarrow PQ$$

$$C_{21}(OU) \quad \equiv ap_{21} + b(mod\ N^2) \qquad \equiv 49 \times 384 + 10(mod\ 676)$$

$$\equiv 18826\ (mod\ 676) \qquad \equiv 574\ (mod\ 676) = 574$$

$$C_{21}(OU) \quad = 574 = 22 \times 26 + 2 \qquad \rightarrow WC$$

$$C_{22}(FO) \quad \equiv ap_{22} + b(mod\ N^2) \qquad \equiv 49 \times 144 + 10(mod\ 676)$$

$$\equiv 7066\ (mod\ 676) \qquad \equiv 306\ (mod\ 676) = 306$$

$$C_{22}(FO) \quad = 306 = 11 \times 26 + 20 \qquad \rightarrow LU$$

$$C_{23}(RI) \quad \equiv ap_{23} + b(mod\ N^2) \qquad \equiv 49 \times 450 + 10(mod\ 676)$$

$$\equiv 22060\ (mod\ 676) \qquad \equiv 428\ (mod\ 676) = 428$$

$$C_{23}(RI) \quad = 428 = 16 \times 26 + 12 \qquad \rightarrow QM$$

$$C_{24}(TB) \equiv ap_{24} + b(mod\ N^2) \equiv 49 \times 495 + 10(mod\ 676)$$
$$\equiv 24265\ (mod\ 676) \equiv 605\ (mod\ 676) = 605$$
$$C_{24}(TB) = 605 = 23 \times 26 + 7 \rightarrow XH$$
$$C_{25}(EC) \equiv ap_{25} + b(mod\ N^2) \equiv 49 \times 106 + 10(mod\ 676)$$
$$\equiv 5204\ (mod\ 676) \equiv 472\ (mod\ 676) = 472$$
$$C_{25}(EC) = 472 = 18 \times 26 + 4 \rightarrow SE$$
$$C_{26}(AU) \equiv ap_{26} + b(mod\ N^2) \equiv 49 \times 20 + 10(mod\ 676)$$
$$\equiv 990\ (mod\ 676) \equiv 314\ (mod\ 676) = 314$$
$$C_{26}(AU) = 314 = 12 \times 26 + 2 \rightarrow MC$$
$$C_{27}(SE) \equiv ap_{27} + b(mod\ N^2) \equiv 49 \times 472 + 10(mod\ 676)$$
$$\equiv 23138\ (mod\ 676) \equiv 154\ (mod\ 676) = 154$$
$$C_{27}(SE) = 154 = 5 \times 26 + 24 \rightarrow FY$$
$$C_{28}(SU) \equiv ap_{28} + b(mod\ N^2) \equiv 49 \times 488 + 10(mod\ 676)$$
$$\equiv 23922\ (mod\ 676) \equiv 262\ (mod\ 676) = 262$$
$$C_{28}(SU) = 262 = 10 \times 26 + 2 \rightarrow KC$$
$$C_{29}(CC) \equiv ap_{29} + b(mod\ N^2) \equiv 49 \times 54 + 10(mod\ 676)$$
$$\equiv 2656\ (mod\ 676) \equiv 628\ (mod\ 676) = 628$$
$$C_{29}(CC) = 628 = 24 \times 26 + 4 \rightarrow YE$$
$$C_{30}(ES) \equiv ap_{30} + b(mod\ N^2) \equiv 49 \times 122 + 10(mod\ 676)$$
$$\equiv 5988\ (mod\ 676) \equiv 580\ (mod\ 676) = 580$$
$$C_{30}(ES) = 580 = 22 \times 26 + 8 \rightarrow WI$$
$$C_{31}(SC) \equiv ap_{3I} + b(mod\ N^2) \equiv 49 \times 470 + 10(mod\ 676)$$
$$\equiv 23040\ (mod\ 676) \equiv 56\ (mod\ 676) = 56$$

$$C_{31}(SC) = 56 = 2 \times 26 + 4 \rightarrow CE$$

$$C_{32}(OM) \equiv ap_{32} + b(mod\ N^2) \equiv 49 \times 376 + 10(mod\ 676)$$

$$\equiv 18434\ (mod\ 676) \equiv 182\ (mod\ 676) = 182$$

$$C_{32}(OM) = 182 = 7 \times 26 + 0 \rightarrow HA$$

$$C_{33}(ES) \equiv ap_{33} + b(mod\ N^2) \equiv 49 \times 122 + 10(mod\ 676)$$

$$\equiv 5988\ (mod\ 676) \equiv 580\ (mod\ 676) = 580$$

$$C_{33}(ES) = 580 = 22 \times 26 + 8 \rightarrow WI$$

$$C_{34}(FR) \equiv ap_{34} + b(mod\ N^2) \equiv 49 \times 147 + 10(mod\ 676)$$

$$\equiv 7213\ (mod\ 676) \equiv 453\ (mod\ 676) = 453$$

$$C_{34}(FR) = 453 = 17 \times 26 + 11 \rightarrow RL$$

$$C_{35}(OM) \equiv ap_{35} + b(mod\ N^2) \equiv 49 \times 376 + 10(mod\ 676)$$

$$\equiv 18434\ (mod\ 676) \equiv 182\ (mod\ 676) = 182$$

$$C_{35}(OM) = 182 = 7 \times 26 + 0 \rightarrow HA$$

$$C_{36}(WH) \equiv ap_{36} + b(mod\ N^2) \equiv 49 \times 579 + 10(mod\ 676)$$

$$\equiv 28381\ (mod\ 676) \equiv 665\ (mod\ 676) = 665$$

$$C_{36}(WH) = 665 = 25 \times 26 + 15 \rightarrow ZP$$

$$C_{37}(AT) \equiv ap_{37} + b(mod\ N^2) \equiv (49 \times 19 + 10) mod\ 676$$

$$\equiv 941\ (mod\ 676) \equiv 265\ (mod\ 676) = 265$$

$$C_{37}(AT) = 265 = 10 \times 26 + 5 \rightarrow KF$$

$$C_{38}(YO) \equiv ap_{38} + b(mod\ N^2) \equiv 49 \times 638 + 10(mod\ 676)$$

$$\equiv 31272\ (mod\ 676) \equiv 176\ (mod\ 676) = 176$$

$$C_{38}(YO) = 176 = 6 \times 26 + 20 \rightarrow GU$$

$$C_{39}(UD) \equiv ap_{39} + b(mod\ N^2) \equiv 49 \times 523 + 10(mod\ 676)$$

$$\equiv 25637\ (mod\ 676) \qquad \equiv 625\ (mod\ 676) = 625$$

$$C_{39}(UD) = 625 = 24 \times 26 + 1 \qquad \rightarrow YB$$

$$C_{40}(OC) \equiv ap_{40} + b(mod\ N^2) \qquad \equiv 49 \times 366 + 10(mod\ 676)$$

$$\equiv 17944\ (mod\ 676) \qquad \equiv 368\ (mod\ 676) = 368$$

$$C_{40}(OC) = 368 = 14 \times 26 + 4 \qquad \rightarrow OE$$

$$C_{41}(ON) \equiv ap_{41} + b(mod\ N^2) \qquad \equiv 49 \times 377 + 10(mod\ 676)$$

$$\equiv 18483\ (mod\ 676) \qquad \equiv 231\ (mod\ 676) = 231$$

$$C_{41}(ON) = 231 = 8 \times 26 + 23 \qquad \rightarrow IX$$

$$C_{42}(SI) \equiv ap_{42} + b(mod\ N^2) \qquad \equiv 49 \times 476 + 10(mod\ 676)$$

$$\equiv 23334\ (mod\ 676) \qquad \equiv 350\ (mod\ 676) = 350$$

$$C_{42}(SI) = 350 = 13 \times 26 + 12 \qquad \rightarrow NM$$

$$C_{43}(ST) \equiv ap_{43} + b(mod\ N^2) \qquad \equiv 49 \times 487 + 10(mod\ 676)$$

$$\equiv 23873\ (mod\ 676) \qquad \equiv 213\ (mod\ 676) = 213$$

$$C_{43}(ST) = 213 = 8 \times 26 + 5 \qquad \rightarrow IF$$

$$C_{44}(EN) \equiv ap_{44} + b(mod\ N^2) \qquad \equiv 49 \times 117 + 10(mod\ 676)$$

$$\equiv 5743\ (mod\ 676) \qquad \equiv 335\ (mod\ 676) = 335$$

$$C_{44}(EN) = 335 = 12 \times 26 + 23 \qquad \rightarrow MX$$

$$C_{45}(LY) \equiv ap_{45} + b(mod\ N^2) \qquad \equiv 49 \times 310 + 10(mod\ 676)$$

$$\equiv 15200\ (mod\ 676) \qquad \equiv 328\ (mod\ 676) = 328$$

$$C_{45}(LY) = 328 = 12 \times 26 + 16 \qquad \rightarrow MQ$$

Diperoleh *ciphertext* yaitu:

RUYUXYIPAXSFQBTQIPKFGUYLXCHCIYBMODIPYXPQWCLUQMXHSE

MCFYKCYEWICEHAWIRLHAZPKFGUYBOEIXNMIFMXMQ**.**

Kemudian, *plaintext* yang digunakan untuk proses enkripsi menggunakan algoritma kriptografi DNA merupakan *ciphertext* yang diperoleh dari hasil enkripsi dengan transformasi digraf. Sehingga, *plaintext* yang diperoleh yaitu RUYUXYIPAXSFQBTQIPKFGUYLXCHCIYBMODIPYXPQWCLUQMXHSE MCFYKCYEWICEHAWIRLHAZPKFGUYBOEIXNMIFMXMQ. Langkah pertama untuk proses enkripsi menggunakan kriptografi DNA adalah memperoleh kode biner masing-masing karakter berdasarkan tabel ASCII. Sehingga, diperoleh kode desimal dan biner dari *plaintext* dalam tabel berikut:

Tabel 3.1 Kode Biner dari *Plaintext*

Karakter	**Kode Biner**	**Karakter**	**Kode Biner**	**Karakter**	**Kode Biner**
R	01010010	B	01000010	C	01000011
U	01010101	M	01001101	E	01000101
Y	01011001	O	01001111	H	01001000
U	01010101	D	01000100	A	01000001
X	01011000	I	01001001	W	01010111
Y	01011001	P	01010000	I	01001001
I	01001001	Y	01011001	R	01010010
P	01010000	X	01011000	L	01001100
A	01000001	P	01010000	H	01001000
X	01011000	Q	01010001	A	01000001
S	01010011	W	01010111	Z	01011010

Lanjutan Tabel 3.1

F	01000110	C	01000011	P	01010000
Q	01010001	L	01001100	K	01001011
B	01000010	U	01010101	F	01000110
T	01010100	Q	01010001	G	01000111
Q	01010001	M	01001101	U	01010101
I	01001001	X	01011000	Y	01011001
P	01010000	H	01001000	B	01000010

K	01001011	S	01010011	O	01001111
F	01000110	E	01000101	E	01000101
G	01000111	M	01001101	I	01001001
U	01010101	C	01000011	X	01011000
Y	01011001	F	01000110	N	01001110
L	01001100	Y	01011001	M	01001101
X	01011000	K	01001011	I	01001001
C	01000011	C	01000011	F	01000110
H	01001000	Y	01011001	M	01001101
C	01000011	E	01000101	X	01011000
I	01001001	W	01010111	M	01001101
Y	01011001	I	01001001	Q	01010001

Setelah menentukan kode biner, langkah selanjutnya yatu melakukan konversi kode biner dalam bentuk untaian DNA. Untaian DNA tersebut memiliki nilai berdasarkan tabel kunci pembangun acak kriptografi DNA pada

Lampiran 4: Tabel Kunci Pembangun Acak Kriptografi DNA. Proses pembentukan tabel kunci pembangun acak terdapat dalam Lampiran 3: Tabel Proses Perhitungan Kunci Pembangun Acak Kriptografi DNA dengan kunci yang dipilih adalah 1000. Berikut proses konversi kode biner ke dalam bentuk untaian DNA beserta nilainya, serta dikonversi menjadi karakter berdasarkan tabel ASCII:

$R \quad = 01010010 \rightarrow CCAG = 73 \rightarrow I$

$U \quad = 01010101 \rightarrow CCCC = 85 \rightarrow U$

$Y \quad = 01011001 \rightarrow CCGC = 83 \rightarrow S$

$U \quad = 01010101 \rightarrow CCCC = 85 \rightarrow U$

$X \quad = 01011000 \rightarrow CCGA = 67 \rightarrow C$

$Y \quad = 01011001 \rightarrow CCGC = 83 \rightarrow S$

$I \quad = 01001001 \rightarrow CAGC = 82 \rightarrow R$

$P \quad = 01010000 \rightarrow CCAA = 65 \rightarrow A$

$A \quad = 01000001 \rightarrow CAAC = 80 \rightarrow P$

$X \quad = 01011000 \rightarrow CCGA = 67 \rightarrow C$

$S \quad = 01010011 \rightarrow CCAT = 89 \rightarrow Y$

$F \quad = 01000110 \rightarrow CACG = 76 \rightarrow L$

$Q \quad = 01010001 \rightarrow CCAC = 81 \rightarrow Q$

$B \quad = 01000010 \rightarrow CAAG = 72 \rightarrow H$

$T \quad = 01010100 \rightarrow CCCA = 69 \rightarrow E$

$Q \quad = 01010001 \rightarrow CCAC = 81 \rightarrow Q$

$I \quad = 01001001 \rightarrow CAGC = 82 \rightarrow R$

$P \quad = 01010000 \rightarrow CCAA = 65 \rightarrow A$

$K \quad = 01001011 \rightarrow CAGT = 90 \rightarrow Z$

$F \quad = 01000110 \rightarrow CACG = 76 \rightarrow L$

$G \quad = 01000111 \rightarrow CACT = 92 \rightarrow \backslash$

$U \quad = 01010101 \rightarrow CCCC = 85 \rightarrow U$

$Y \quad = 01011001 \rightarrow CCGC = 83 \rightarrow S$

$L \quad = 01001100 \rightarrow CATA = 70 \rightarrow F$

$X \quad = 01011000 \rightarrow CCGA = 67 \rightarrow C$

$C \quad = 01000011 \rightarrow CAAT = 88 \rightarrow X$

$H \quad = 01001000 \rightarrow CAGA = 66 \rightarrow B$

$C \quad = 01000011 \rightarrow CAAT = 88 \rightarrow X$

$I \quad = 01001001 \rightarrow CAGC = 82 \rightarrow R$

$Y \quad = 01011001 \rightarrow CCGC = 83 \rightarrow S$

$B \quad = 01000010 \rightarrow CAAG = 72 \rightarrow H$

$M \quad = 01001101 \rightarrow CATC = 86 \rightarrow V$

$O \quad = 01001111 \rightarrow CATT = 94 \rightarrow$ ^

$D \quad = 01000100 \rightarrow CACA = 68 \rightarrow D$

$I \quad = 01001001 \rightarrow CAGC = 82 \rightarrow R$

$P \quad = 01010000 \rightarrow CCAA = 65 \rightarrow A$

$Y \quad = 01011001 \rightarrow CCGC = 83 \rightarrow S$

$X \quad = 01011000 \rightarrow CCGA = 67 \rightarrow C$

$P \quad = 01010000 \rightarrow CCAA = 65 \rightarrow A$

$Q \quad = 01010001 \rightarrow CCAC = 81 \rightarrow Q$

$W \quad = 01010111 \rightarrow CCCT = 93 \rightarrow$]

$C \quad = 01000011 \rightarrow CAAT = 88 \rightarrow X$

$L \quad = 01001100 \rightarrow CATA = 70 \rightarrow F$

$U \quad = 01010101 \rightarrow CCCC = 85 \rightarrow U$

$Q \quad = 01010001 \rightarrow CCAC = 81 \rightarrow Q$

$M \quad = 01001101 \rightarrow CATC = 86 \rightarrow V$

$X \quad = 01011000 \rightarrow CCGA = 67 \rightarrow C$

$H \quad = 01001000 \rightarrow CAGA = 66 \rightarrow B$

$S \quad = 01010011 \rightarrow CCAT = 89 \rightarrow Y$

$E \quad = 01000101 \rightarrow CACC = 84 \rightarrow T$

$M \quad = 01001101 \rightarrow CATC = 86 \rightarrow V$

$C \quad = 01000011 \rightarrow CAAT = 88 \rightarrow X$

$F \quad = 01000110 \rightarrow CACG = 76 \rightarrow L$

$Y \quad = 01011001 \rightarrow CCGC = 83 \rightarrow S$

$K \quad = 01001011 \rightarrow CAGT = 90 \rightarrow Z$

$C \quad = 01000011 \rightarrow CAAT = 88 \rightarrow X$

$Y \quad = 01011001 \rightarrow CCGC = 83 \rightarrow S$

$E \quad = 01000101 \rightarrow CACC = 84 \rightarrow T$

$W \quad = 01010111 \rightarrow CCCT = 93 \rightarrow]$

$I \quad = 01001001 \rightarrow CAGC = 82 \rightarrow R$

$C \quad = 01000011 \rightarrow CAAT = 88 \rightarrow X$

$E \quad = 01000101 \rightarrow CACC = 84 \rightarrow T$

$H \quad = 01001000 \rightarrow CAGA = 66 \rightarrow B$

$A \quad = 01000001 \rightarrow CAAC = 80 \rightarrow P$

$W \quad = 01010111 \rightarrow CCCT = 93 \rightarrow]$

$I \quad = 01001001 \rightarrow CAGC = 82 \rightarrow R$

$R \quad = 01010010 \rightarrow CCAG = 73 \rightarrow I$

$L \quad = 01001100 \rightarrow CATA = 70 \rightarrow F$

$H \quad = 01001000 \rightarrow CAGA = 66 \rightarrow B$

$A \quad = 01000001 \rightarrow CAAC = 80 \rightarrow P$

$Z \quad = 01011010 \rightarrow CCGG = 75 \rightarrow K$

$P \quad = 01010000 \rightarrow CCAA = 65 \rightarrow A$

$K \quad = 01001011 \rightarrow CAGT = 90 \rightarrow Z$

$F \quad = 01000110 \rightarrow CACG = 76 \rightarrow L$

$G \quad = 01000111 \rightarrow CACT = 92 \rightarrow \backslash$

$U \quad = 01010101 \rightarrow CCCC = 85 \rightarrow U$

$Y \quad = 01011001 \rightarrow CCGC = 83 \rightarrow S$

$B \quad = 01000010 \rightarrow CAAG = 72 \rightarrow H$

$O \quad = 01001111 \rightarrow CATT = 94 \rightarrow \wedge$

$E \quad = 01000101 \rightarrow CACC = 84 \rightarrow T$

$I \quad = 01001001 \rightarrow CAGC = 82 \rightarrow R$

$X \quad = 01011000 \rightarrow CCGA = 67 \rightarrow C$

$N \quad = 01001110 \rightarrow CATG = 78 \rightarrow N$

$M \quad = 01001101 \rightarrow CATC = 86 \rightarrow V$

$I \quad = 01001001 \rightarrow CAGC = 82 \rightarrow R$

$F \quad = 01000110 \rightarrow CACG = 76 \rightarrow L$

$M \quad = 01001101 \rightarrow CATC = 86 \rightarrow V$

$X \quad = 01011000 \rightarrow CCGA = 67 \rightarrow C$

$M \quad = 01001101 \rightarrow CATC = 86 \rightarrow V$

$Q \quad = 01010001 \rightarrow CCAC = 81 \rightarrow Q$

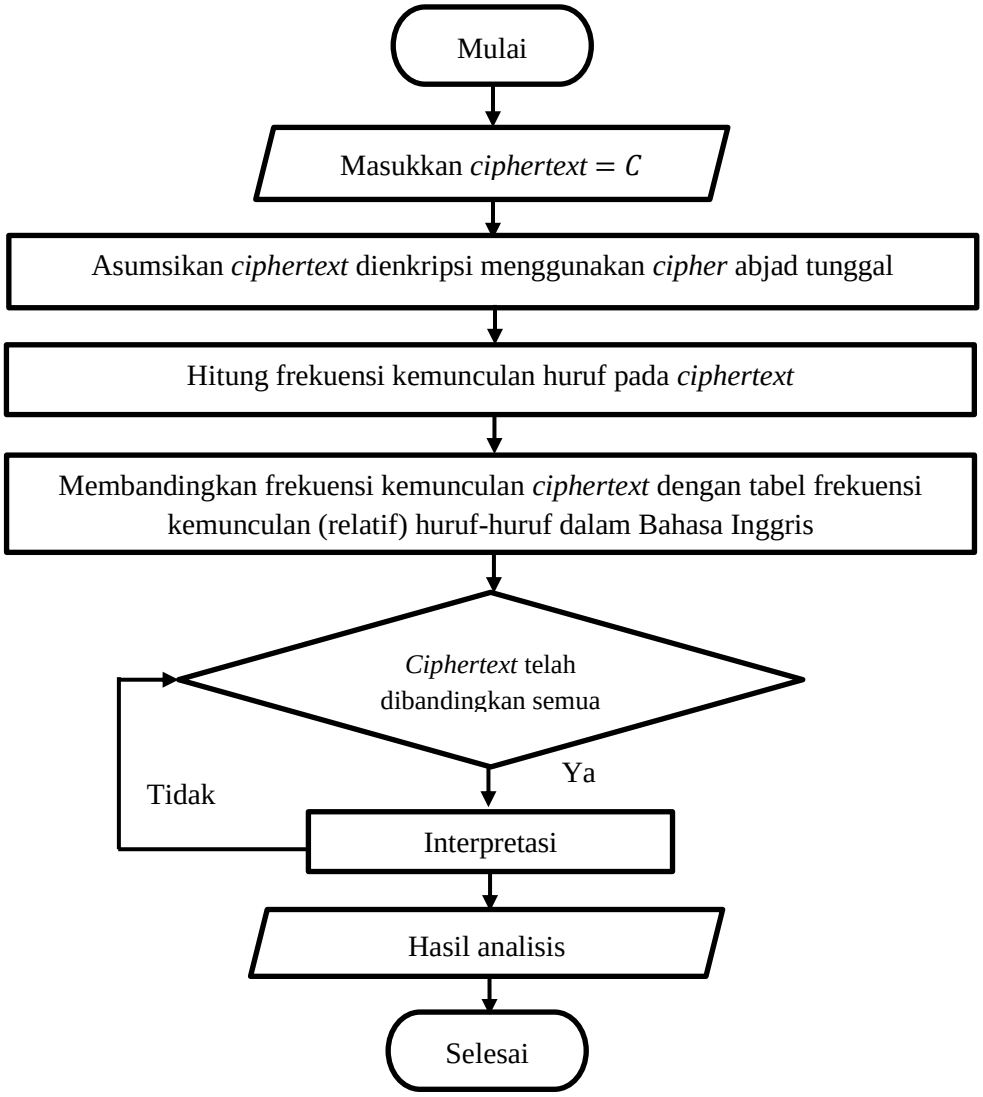
Dengan demikian, pesan teks DO SOMETHING TODAY THAT YOUR FUTURE WILL THANK YOU FOR IT BECAUSE SUCCESS COMES FROM

WHAT YOU DO CONSISTENLY setelah dienkripsi menggunakan algortima kriptografi DNA dan transformasi digraf, menjadi *ciphertext*:

IUSUCSRAPCYLQHEQRAZL\USFCXBXRSHV^DRASCAQ]XFUQVCBYTV XLSZXST]RXTBP]RIFBPKAZL\VSH^TRCNVRLVCVQ.

3.2 Analisis Frekuensi Hasil Enkripsi

Proses analisis frekuensi dilakukan terhadap hasil enkripsi pesan. Berikut merupakan *flowchart* untuk proses analisis frekuensi hasil enkripsi pesan teks.



Gambar 3.3 *Flowchart* Proses Analisis Frekuensi

Berdasarkan hasil enkripsi pesan menggunakan algoritma kriptografi DNA dan transformasi digraf, diperoleh *ciphertext*:

IUSUCSRAPCYLQHEQRAZL\USFCXBXRSHV^DRASCAQ]XFUQVCBYTV
XLSZXST]RXTBP]RIFBPKAZL\VSH^TRCNVRLVCVQ.

Sebelum melakukan analisis frekuensi, penulis mengasumsikan bahwa *ciphertext* dienkripsi menggunakan *cipher* abjad tunggal. Langkah pertama yaitu menghitung frekuensi kemunculan relatif huruf-huruf atau karakter dalam *ciphertext*. Berikut ini hasil perhitungan yang diperoleh:

Tabel 3.2 Frekuensi Kemunculan Relatif Huruf

Karakter	Frekuensi	Karakter	Frekuensi	Karakter	Frekuensi
S	8	**U**	4	**I**	2
R	8	**B**	4	^	2
C	7	**T**	4	\	2
V	7	**P**	3	**Y**	2
X	6	**H**	3	**E**	1
A	5	**Z**	3	**K**	1
L	5	**F**	3	**N**	1
Q	5	**]**	3	**D**	1

Langkah kedua yaitu membandingkan hasil pada Tabel 3.2 Frekuensi Kemunculan Relatif Huruf dengan Tabel 2. 2 Frekuensi Kemunculan (Relatif) Huruf Dalam Bahasa Inggris. Berikut ini hasil analisis frekuensi yang diperoleh melalui perbandingan:

Iterasi 1:

Berdasarkan Tabel 3.2 Frekuensi Kemunculan Relatif Huruf, terdapat dua karakter yang sering muncul di dalam *ciphertext*, yaitu karakter S dan R. Hal ini menunjukkan bahwa huruf pada *plaintext* yang berkoresponden juga sering muncul dalam pesan. Dua huruf yang sering muncul pada teks bahasa inggris berdasarkan Tabel 2. 2 Frekuensi Kemunculan (Relatif) Huruf Dalam Bahasa Inggris adalah huruf e dan t. Kita dapat menduga 2 asumsi sementara, bahwa karakter S berkoresponden dengan huruf e dan karakter R berkoresponden dengan huruf t, atau karakter R berkoresponden dengan huruf e dan karakter S

berkoresponden dengan huruf t. Selanjutnya, melakukan perubahan pada *ciphertext* menggunakan kedua asumsi.

Tabel 3.3 Iterasi ke-1 Analisis Frekuensi

Asumsi 1	$S = e, R = t$	IUeUCetAPCYLQHEQtAZL\UeFCXBXte HV^DtAeCAQ]XFUQVCBYTVXLeZXeT]t XTBP]tIFBPKAZL\VeH^TtCNVtLVCVQ
Asumsi 2	$S = t, R = e$	IUtUCteAPCYLQHEQeAZL\UtFCXBXet HV^DeAtCAQ]XFUQVCBYTVXLtZXtT]e XTBP]eIFBPKAZL\VtH^TeCNVeLVCVQ

Iterasi 2:

Berdasarkan hasil iterasi ke-1, *plaintext* masih sulit untuk ditebak, sehingga perlu melakukan perbandingan terhadap karakter terbanyak selanjutnya. Berdasarkan Tabel 3.2 Frekuensi Kemunculan Relatif Huruf, karakter terbanyak selanjutnya adalah C dan V. Huruf yang sering muncul berdasarkan Tabel 2. 2 Frekuensi Kemunculan (Relatif) Huruf Dalam Bahasa Inggris adalah huruf a dan o. Diperoleh hasil iterasi kedua yaitu:

Tabel 3.4 Iterasi ke-2 Analisis Frekuensi

Asumsi 3	$S = e, R = t,$ $C = a, V = o$	IUeUaetAPaYLQHEQtAZL\UeFCXBXte Ho^DtAeaAQ]XFUQoaBYToXLeZXeT]t XTBP]tIFBPKAZL\oeH^TtaNotLoaoQ

Lanjutan Tabel 3.4

Asumsi 4	$S = t, R = e,$ $V = a, C = o$	IUtUoteAPoYLQHEQeAZL\UtFoXBXet Ha^DeAtoAQ]XFUQaoBYTaXLtZXtT]e XTBP]eIFBPKAZL\atH^TeoNaeLaoaQ
Asumsi 5	$S = e, R = t,$ $V = a, C = o$	IUeUoetAPoYLQHEQtAZL\UeFoXBXte Ha^DtAeoAQ]XFUQaoBYTaXLeZXeT]t XTBP]tIFBPKAZL\aeH^TtoNatLaoaQ
Asumsi 6	$S = t, R = e,$ $C = a, V = o$	IUtUateAPaYLQHEQeAZL\UtFaXBXet Ho^DeAtaAQ]XFUQoaBYToXLtZXtT]e XTBP]eIFBPKAZL\otH^TeaNoeLoaoQ

Iterasi 3:

Berdasarkan hasil iterasi ke-2, *plaintext* masih sulit untuk ditebak, sehingga perlu melakukan perbandingan terhadap karakter terbanyak selanjutnya. Berdasarkan Tabel 3.2 Frekuensi Kemunculan Relatif Huruf, karakter terbanyak selanjutnya adalah X. Huruf yang sering muncul pada teks bahasa inggris berdasarkan Tabel 2. 2 Frekuensi Kemunculan (Relatif) Huruf Dalam Bahasa Inggris adalah huruf i. Sehingga, diperoleh hasil iterasi ketiga yaitu:

Tabel 3. 5 Iterasi ke-3 Analisis Frekuensi

Asumsi 7	$S = e, R = t,$ $C = a, V = o,$ $X = i$	IUeUaetAPaYLQHEQtAZL\UeFCiBite Ho^DtAeaAQ]iFUQoaBYToiLeZieT]t iTBP]tIFBPKAZL\oeH^TtaNotLoaoQ
Asumsi 8	$S = t, R = e,$ $V = a, C = o,$ $X = i$	IUtUoteAPoYLQHEQeAZL\UtFoiBiet Ha^DeAtoAQ]iFUQaoBYTaiLtZitT]e iTBP]eIFBPKAZL\atH^TeoNaeLaoaQ

Lanjutan Tabel 3.5

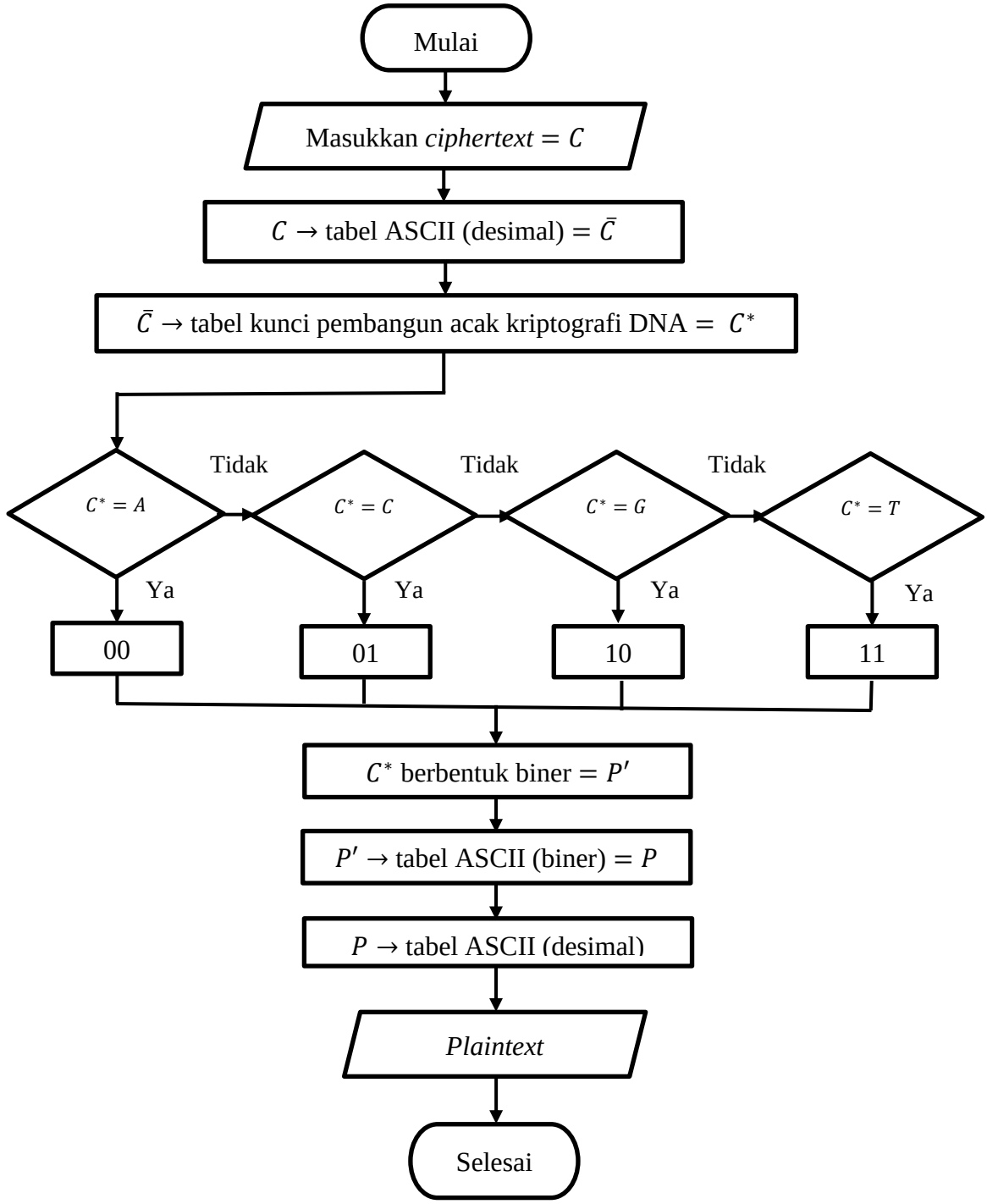
Asumsi 9	$S = e, R = t,$ $V = a, C = o,$ $X = i$	IUeUoetAPoYLQHEQtAZL\UeFoiBite Ha^DtAeoAQ]iFUQaoBYTaiLeZieT]t iTBP]tIFBPKAZL\aeH^TtoNatLaoaQ
Asumsi 10	$S = t, R = e,$ $C = a, V = o,$ $X = i$	IUtUateAPaYLQHEQeAZL\UtFaiBiet Ho^DeAtaAQ]iFUQoaBYToiLtZitT]e iTBP]eIFBPKAZL\otH^TeaNoeLoaoQ

Berdasarkan hasil iterasi ke-3, *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.

3.3 Proses Dekripsi Pesan Teks

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.

Berikut merupakan *flowchart* proses dekripsi pesan teks menggunakan algoritma kriptografi DNA.



Gambar 3.4 *Flowchart* Proses Dekripsi Algoritma Kriptografi DNA

Selanjutnya, proses dekripsi pesan menggunakan algoritma transformasi digraf persamaan (2. 7**)**.

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

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

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

Diperoleh rumus dekripsi yaitu,

$$P \equiv a^{-1}c - a^{-1}b \ (mod\ N^2)$$

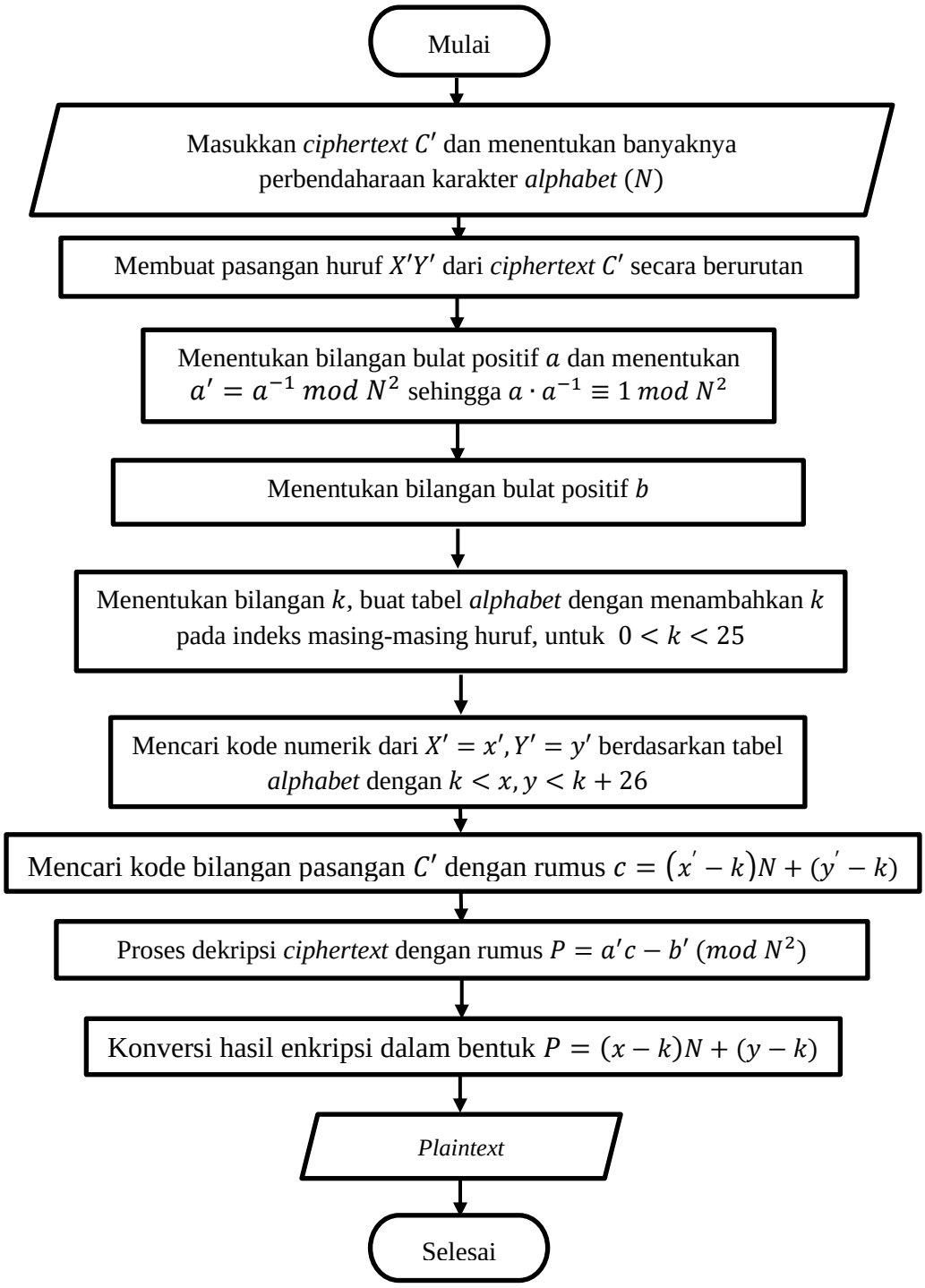
Misalkan a adalah bilangan bulat positif yang relatif prima dengan N^2dan $h \in \mathbb{Z}$.

$P \equiv a^{-1}c - a^{-1}b \ (mod\ N^2)$	Rumus dekripsi
$N^2 \mid P - (a^{-1}c - a^{-1}b)$	Definisi kongruensi
$P - (a^{-1}c - a^{-1}b) = N^2 \cdot h$	Definisi keterbagian
$P - a^{-1}c + a^{-1}b = N^2 \cdot h$	Sifat distributif

Karena a^{-1} adalah *invers* modulo N^2, maka a^{-1} memiliki balikan modulo N^2, yaitu disimbolkan dengan a.

$a \times (P - a^{-1}c + a^{-1}b) = (N^2 \cdot h) \times a$	Kedua ruas dikalikan a
$aP - aa^{-1}c + aa^{-1}b = N^2 \cdot (ah)$	Sifat distributif
$aP - c + b = N^2 \cdot (ah)$	Sifat invers
$-1 \times (aP - c + b) = (N^2 \cdot (ah)) \times -1$	Kedua ruas dikalikan -1
$-aP + c - b = N^2 \cdot (ah)$	Sifat distributif
$c - aP - b = N^2 \cdot (ah)$	Sifat komutatif
$c - (aP + b) = N^2 \cdot (ah)$	Sifat distributif
$N^2 \mid \big(c - (aP + b)\big)$	Definisi keterbagian
$c \equiv aP + b \ (mod\ N^2)$	Definisi kongruensi

Kemudian akan ditunjukkan *flowchart* proses dekripsi pesan teks menggunakan algoritma transformasi digraf.



Gambar 3.5 *Flowchart* Proses Dekripsi Algoritma Transformasi Digraf

Berikut ini contoh proses dekripsi pesan teks menggunakan algoritma kriptografi DNA:

Ciphertext:

IUSUCSRAPCYLQHEQRAZL\USFCXBXRSHV^DRASCAQ]XFUQVCBYTV

XLSZXST]RXTBP]RIFBPKAZL\VSH^TRCNVRLVCVQ.

Langkah yang dilakukan untuk proses dekripsi menggunakan algoritma kriptografi DNA yaitu mencari kode desimal *ciphertext* berdasarkan tabel ASCII. Kemudian, berdasarkan tabel kunci pembangun acak kriptografi DNA, kode desimal tersebut dikonversi dalam bentuk untaian DNA dan kemudian dikonversi dalam bentuk kode biner. Selanjutnya, kode biner tersebut dikonversi menjadi karakter berdasarkan tabel ASCII.

$I \quad = 73 = CCAG \rightarrow 01010010 \rightarrow R$

$U \quad = 85 = CCCC \rightarrow 01010101 \rightarrow U$

$S \quad = 83 = CCGC \rightarrow 01011001 \rightarrow Y$

$U \quad = 85 = CCCC \rightarrow 01010101 \rightarrow U$

$C \quad = 67 = CCGA \rightarrow 01011000 \rightarrow X$

$S \quad = 83 = CCGC \rightarrow 01011001 \rightarrow Y$

$R \quad = 82 = CAGC \rightarrow 01001001 \rightarrow I$

$A \quad = 65 = CCAA \rightarrow 01010000 \rightarrow P$

$P \quad = 80 = CAAC \rightarrow 01000001 \rightarrow A$

$C \quad = 67 = CCGA \rightarrow 01011000 \rightarrow X$

$Y \quad = 89 = CCAT \rightarrow 01010011 \rightarrow S$

$L \quad = 76 = CACG \rightarrow 01000110 \rightarrow F$

$Q \quad = 81 = CCAC \rightarrow 01010001 \rightarrow Q$

$H \quad = 72 = CAAG \rightarrow 01000010 \rightarrow B$

$E \quad = 69 = CCCA \rightarrow 01010100 \rightarrow T$

$Q \quad = 81 = CCAC \rightarrow 01010001 \rightarrow Q$

$R \quad = 82 = CAGC \rightarrow 01001001 \rightarrow I$

$A \quad = 65 = CCAA \rightarrow 01010000 \rightarrow P$

$Z \quad = 90 = CAGT \rightarrow 01001011 \rightarrow K$

$L \quad = 76 = CACG \rightarrow 01000110 \rightarrow F$

$\backslash \quad = 92 = CACT \rightarrow 01000111 \rightarrow G$

$U \quad = 85 = CCCC \rightarrow 01010101 \rightarrow U$

$S \quad = 83 = CCGC \rightarrow 01011001 \rightarrow Y$

$F \quad = 70 = CATA \rightarrow 01001100 \rightarrow L$

$C \quad = 67 = CCGA \rightarrow 01011000 \rightarrow X$

$X \quad = 88 = CAAT \rightarrow 01000011 \rightarrow C$

$B \quad = 66 = CAGA \rightarrow 01001000 \rightarrow H$

$X \quad = 88 = CAAT \rightarrow 01000011 \rightarrow C$

$R \quad = 82 = CAGC \rightarrow 01001001 \rightarrow I$

$S \quad = 83 = CCGC \rightarrow 01011001 \rightarrow Y$

$H \quad = 72 = CAAG \rightarrow 01000010 \rightarrow B$

$V \quad = 86 = CATC \rightarrow 01001101 \rightarrow M$

$\hat{} \quad = 94 = CATT \rightarrow 01001111 \rightarrow O$

$D \quad = 68 = CACA \rightarrow 01000100 \rightarrow D$

$R \quad = 82 = CAGC \rightarrow 01001001 \rightarrow I$

$A \quad = 65 = CCAA \rightarrow 01010000 \rightarrow P$

$S \quad = 83 = CCGC \rightarrow 01011001 \rightarrow Y$

$C \quad = 67 = CCGA \rightarrow 01011000 \rightarrow X$

$A \quad = 65 = CCAA \rightarrow 01010000 \rightarrow P$

$Q \quad = 81 = CCAC \rightarrow 01010001 \rightarrow Q$

$] \quad = 93 = CCCT \rightarrow 01010111 \rightarrow W$

$X \quad = 88 = CAAT \rightarrow 01000011 \rightarrow C$

$F \quad = 70 = CATA \rightarrow 01001100 \rightarrow L$

$U \quad = 85 = CCCC \rightarrow 01010101 \rightarrow U$

$Q \quad = 81 = CCAC \rightarrow 01010001 \rightarrow Q$

$V \quad = 86 = CATC \rightarrow 01001101 \rightarrow M$

$C \quad = 67 = CCGA \rightarrow 01011000 \rightarrow X$

$B \quad = 66 = CAGA \rightarrow 01001000 \rightarrow H$

$Y \quad = 89 = CCAT \rightarrow 01010011 \rightarrow S$

$T \quad = 84 = CACC \rightarrow 01000101 \rightarrow E$

$V \quad = 86 = CATC \rightarrow 01001101 \rightarrow M$

$X \quad = 88 = CAAT \rightarrow 01000011 \rightarrow C$

$L \quad = 76 = CACG \rightarrow 01000110 \rightarrow F$

$S \quad = 83 = CCGC \rightarrow 01011001 \rightarrow Y$

$Z \quad = 90 = CAGT \rightarrow 01001011 \rightarrow K$

$X \quad = 88 = CAAT \rightarrow 01000011 \rightarrow C$

$S \quad = 83 = CCGC \rightarrow 01011001 \rightarrow Y$

$T \quad = 84 = CACC \rightarrow 01000101 \rightarrow E$

$] \quad = 93 = CCCT \rightarrow 01010111 \rightarrow W$

$R \quad = 82 = CAGC \rightarrow 01001001 \rightarrow I$

$X \quad = 88 = CAAT \rightarrow 01000011 \rightarrow C$

$T \quad = 84 = CACC \rightarrow 01000101 \rightarrow E$

$B \quad = 66 = CAGA \rightarrow 01001000 \rightarrow H$

$P \quad = 80 = CAAC \rightarrow 01000001 \rightarrow A$

$] \quad = 93 = CCCT \rightarrow 01010111 \rightarrow W$

$R \quad = 82 = CAGC \rightarrow 01001001 \rightarrow I$

$I \quad = 73 = CCAG \rightarrow 01010010 \rightarrow R$

$F \quad = 70 = CATA \rightarrow 01001100 \rightarrow L$

$B \quad = 66 = CAGA \rightarrow 01001000 \rightarrow H$

$P \quad = 80 = CAAC \rightarrow 01000001 \rightarrow A$

$K \quad = 75 = CCGG \rightarrow 01011010 \rightarrow Z$

$A \quad = 65 = CCAA \rightarrow 01010000 \rightarrow P$

$Z \quad = 90 = CAGT \rightarrow 01001011 \rightarrow K$

$L \quad = 76 = CACG \rightarrow 01000110 \rightarrow F$

$\backslash \quad = 92 = CACT \rightarrow 01000111 \rightarrow G$

$U \quad = 85 = CCCC \rightarrow 01010101 \rightarrow U$

$S \quad = 83 = CCGC \rightarrow 01011001 \rightarrow Y$

$H \quad = 72 = CAAG \rightarrow 01000010 \rightarrow B$

$\hat{} \quad = 94 = CATT \rightarrow 01001111 \rightarrow O$

$T \quad = 84 = CACC \rightarrow 01000101 \rightarrow E$

$R \quad = 82 = CAGC \rightarrow 01001001 \rightarrow I$

$C \quad = 67 = CCGA \rightarrow 01011000 \rightarrow X$

$N \quad = 78 = CATG \rightarrow 01001110 \rightarrow N$

$V \quad = 86 = CATC \rightarrow 01001101 \rightarrow M$

$R \quad = 82 = CAGC \rightarrow 01001001 \rightarrow I$

$L \quad = 76 = CACG \rightarrow 01000110 \rightarrow F$

$V \quad = 86 = CATC \rightarrow 01001101 \rightarrow M$

$C \quad = 67 = CCGA \rightarrow 01011000 \rightarrow X$

$V \quad = 86 = CATC \rightarrow 01001101 \rightarrow M$

$Q \quad = 81 = CCAC \rightarrow 01010001 \rightarrow Q$

Diperoleh *plaintext* yaitu:

RUYUXYIPAXSFQBTQIPKFGUYLXCHCIYBMODIPYXPQWCLUQMXHSE

MCFYKCYEWICEHAWIRLHAZPKFGUYBOEIXNMIFMXMQ**.**

Langkah selanjutnya yaitu melanjutkan dekripsi pesan teks menggunakan algoritma transformasi digraf. *Ciphertext* yang digunakan merupakan *plaintext* yang diperoleh dari hasil dekripsi dengan kriptografi DNA. Sehingga diperoleh *ciphertext* yang telah dipisahkan secara berpasangan yaitu:

RU YU XY IP AX SF QB TQ IP KF GU YL

XC HC IY BM OD IP YX PQ WC LU QM XH

SE MC FY KC YE WI CE HA WI RL HA ZP

KF GU YB OE IX NM IF MX MQ.

Kemudian menentukan kode bilangan masing-masing pasangan huruf, sehingga diperoleh kode bilangan berikut:

$c'_1(RU) \quad = 17 \times 26 + 20 \quad = 462$

$c'_2(YU) \quad = 24 \times 26 + 20 \quad = 644$

$c'_3(XY) \quad = 23 \times 26 + 24 \quad = 622$

$c'_4(IP) \quad = 8 \times 26 + 15 \quad = 223$

$c'_5(AX) \quad = 0 \times 26 + 23 \quad = 23$

$c'_6(SF) = 18 \times 26 + 5 = 473$

$c'_7(QB) = 16 \times 26 + 1 = 417$

$c'_8(TQ) = 19 \times 26 + 16 = 510$

$c'_9(IP) = 8 \times 26 + 15 = 223$

$c'_{10}(KF) = 10 \times 26 + 5 = 265$

$c'_{11}(GU) = 6 \times 26 + 20 = 176$

$c'_{12}(YL) = 24 \times 26 + 11 = 635$

$c'_{13}(XC) = 23 \times 26 + 2 = 600$

$c'_{14}(HC) = 7 \times 26 + 2 = 184$

$c'_{15}(IY) = 8 \times 26 + 24 = 232$

$c'_{16}(BM) = 1 \times 26 + 12 = 38$

$c'_{17}(OD) = 14 \times 26 + 3 = 367$

$c'_{18}(IP) = 8 \times 26 + 15 = 223$

$c'_{19}(YX) = 24 \times 26 + 23 = 647$

$c'_{20}(PQ) = 15 \times 26 + 16 = 406$

$c'_{21}(WC) = 22 \times 26 + 2 = 574$

$c'_{22}(LU) = 11 \times 26 + 20 = 306$

$c'_{23}(QM) = 16 \times 26 + 12 = 428$

$c'_{24}(XH) = 23 \times 26 + 7 = 605$

$c'_{25}(SE) = 18 \times 26 + 4 = 472$

$c'_{26}(MC) = 12 \times 26 + 2 = 314$

$c'_{27}(FY) = 5 \times 26 + 24 = 154$

$c'_{28}(KC) = 10 \times 26 + 2 = 262$

$c'_{29}(YE) \quad = 24 \times 26 + 4 \quad = 628$

$c'_{30}(WI) \quad = 22 \times 26 + 8 \quad = 580$

$c'_{31}(CE) \quad = 2 \times 26 + 4 \quad = 56$

$c'_{32}(HA) \quad = 7 \times 26 + 0 \quad = 182$

$c'_{33}(WI) \quad = 22 \times 26 + 8 \quad = 580$

$c'_{34}(RL) \quad = 17 \times 26 + 11 \quad = 453$

$c'_{35}(HA) \quad = 7 \times 26 + 0 \quad = 182$

$c'_{36}(ZP) \quad = 25 \times 26 + 15 \quad = 665$

$c'_{37}(KF) \quad = 10 \times 26 + 5 \quad = 265$

$c'_{38}(GU) \quad = 6 \times 26 + 20 \quad = 176$

$c'_{39}(YB) \quad = 24 \times 26 + 1 \quad = 625$

$c'_{40}(OE) \quad = 14 \times 26 + 4 \quad = 368$

$c'_{41}(IX) \quad = 8 \times 26 + 23 \quad = 231$

$c'_{42}(NM) \quad = 13 \times 26 + 12 \quad = 350$

$c'_{43}(IF) \quad = 8 \times 26 + 5 \quad = 213$

$c'_{44}(MX) \quad = 12 \times 26 + 23 \quad = 335$

$c'_{45}(MQ) \quad = 12 \times 26 + 16 \quad = 328$

Sebelum melanjutkan dekripsi menggunakan algoritma transformasi digraf persamaan (2. 6**)**, penulis menentukan *invers* nilai parameter a yang akan digunakan pada persamaan (2. 6**)**. Suatu bilangan bulat a^{-1} merupakan balikan dari a modulo n, sedemikian sehingga $aa^{-1} \equiv 1 \; mod \; n$. Sehingga diperoleh nilai sebagai berikut :

$$N = 26, \qquad N^2 = 26^2 = 676$$

$$a = 49$$

$$b = 10$$

Misalkan

$$a^{-1} = x, \quad x \times a \equiv 1 \, mod \, 676.$$

Dipilih bilangan $x = 69$, karena $69 \times 49 = 3381 \equiv 1 \, mod \, 676$, maka $x = 69 = a^{-1} = a'$. Sehingga, diperoleh $a^{-1}b(mod\ 676) = 69 \times 10 = 690\ (mod\ 676) \equiv 14\ (mod\ 676)$.

Langkah selanjutnya yaitu melakukan dekripsi menggunakan algoritma transformasi digraf persamaan (2. 6**)**, kemudian dilanjutkan dengan mengubah hasil dekripsi yang telah diperoleh, ke dalam bentuk persamaan (2. 7) dan memperoleh karakter berdasarkan tabel *alphabet*.

$$\begin{aligned}
P_1(RU) &\equiv a^{-1}c'_1 - a^{-1}b(mod\ N^2) && \equiv 69 \times 462 - 14(mod\ 676) \\
&\equiv 31864\ (mod\ 676) && \equiv 92\ (mod\ 676) = 92 \\
P_1(RU) &= 92 = 3 \times 26 + 14 && \rightarrow DO \\
P_2(YU) &\equiv (a^{-1}c'_2 - a^{-1}b) mod\ N^2 && \equiv (69 \times 644 - 14) mod\ 676 \\
&\equiv 44422\ (mod\ 676) && \equiv 482\ (mod\ 676) = 482 \\
P_2(YU) &= 482 = 18 \times 26 + 14 && \rightarrow SO \\
P_3(XY) &\equiv a^{-1}c'_3 - a^{-1}b(mod\ N^2) && \equiv 69 \times 622 - 14(mod\ 676) \\
&\equiv 42904\ (mod\ 676) && \equiv 316\ (mod\ 676) = 316 \\
P_3(XY) &= 316 = 12 \times 26 + 4 && \rightarrow ME \\
P_4(IP) &\equiv a^{-1}c'_4 - a^{-1}b(mod\ N^2) && \equiv 69 \times 223 - 14(mod\ 676) \\
&\equiv 15373\ (mod\ 676) && \equiv 501\ (mod\ 676) = 501 \\
P_4(IP) &= 501 = 19 \times 26 + 7 && \rightarrow TH \\
P_5(AX) &\equiv a^{-1}c'_5 - a^{-1}b\ (mod\ N^2) && \equiv 69 \times 23 - 14\ (mod\ 676)
\end{aligned}$$

$$\equiv 1573\ (mod\ 676) \qquad \equiv 221\ (mod\ 676) = 221$$

$$P_5(AX) \quad = 221 = 8 \times 26 + 13 \qquad \rightarrow IN$$

$$P_6(SF) \quad \equiv a^{-1}c'_6 - a^{-1}b\ (mod\ N^2) \qquad \equiv 69 \times 473 - 14\ (mod\ 676)$$

$$\equiv 32623(mod\ 676) \qquad \equiv 175\ (mod\ 676) = 175$$

$$P_6(SF) \quad = 175 = 6 \times 26 + 19 \qquad \rightarrow GT$$

$$P_7(QB) \quad \equiv a^{-1}c'_7 - a^{-1}b(mod\ N^2) \qquad \equiv 69 \times 417 - 14(mod\ 676)$$

$$\equiv 28759\ (mod\ 676) \qquad \equiv 367\ (mod\ 676) = 367$$

$$P_7(QB) \quad = 367 = 14 \times 26 + 3 \qquad \rightarrow OD$$

$$P_8(TQ) \quad \equiv a^{-1}c'_8 - a^{-1}b\ (mod\ N^2) \qquad \equiv 69 \times 510 - 14\ (mod\ 676)$$

$$\equiv 35176(mod\ 676) \qquad \equiv 24\ (mod\ 676) = 24$$

$$P_8(TQ) \quad = 24 = 0 \times 26 + 24 \qquad \rightarrow AY$$

$$P_9(IP) \quad \equiv a^{-1}c'_9 - a^{-1}b\ (mod\ N^2) \qquad \equiv 69 \times 223 - 14\ (mod\ 676)$$

$$\equiv 15373\ (mod\ 676) \qquad \equiv 501\ (mod\ 676) = 501$$

$$P_9(IP) \quad = 501 = 19 \times 26 + 7 \qquad \rightarrow TH$$

$$P_{10}(KF) \quad \equiv a^{-1}c'_{10} - a^{-1}b\ (mod\ N^2) \qquad \equiv 69 \times 265 - 14\ (mod\ 676)$$

$$\equiv 18271\ (mod\ 676) \qquad \equiv 19\ (mod\ 676) = 19$$

$$P_{10}(KF) \quad = 19 = 0 \times 26 + 19 \qquad \rightarrow AT$$

$$P_{11}(GU) \quad \equiv a^{-1}c'_{11} - a^{-1}b(mod\ N^2) \qquad \equiv 69 \times 176 - 14\ (mod\ 676)$$

$$\equiv 12130\ (mod\ 676) \qquad \equiv 638\ (mod\ 676) = 638$$

$$P_{11}(GU) \quad = 638 = 24 \times 26 + 14 \qquad \rightarrow YO$$

$$P_{12}(YL) \quad \equiv a^{-1}c'_{12} - a^{-1}b\ (mod\ N^2) \qquad \equiv 69 \times 635 - 14\ (mod\ 676)$$

$$\equiv 43801(mod\ 676) \qquad \equiv 537\ (mod\ 676) = 537$$

$$P_{12}(YL) \quad = 537 = 20 \times 26 + 17 \qquad \rightarrow UR$$

$$P_{13}(XC) \equiv a^{-1}c'_{13} - a^{-1}b\ (mod\ N^2) \equiv 69 \times 600 - 14\ (mod\ 676)$$
$$\equiv 41386\ (mod\ 676) \equiv 150\ (mod\ 676) = 150$$
$$P_{13}(XC) = 150 = 5 \times 26 + 20 \rightarrow FU$$
$$P_{14}(HC) \equiv a^{-1}c'_{14} - a^{-1}b\ (mod\ N^2) \equiv 69 \times 184 - 14\ (mod\ 676)$$
$$\equiv 12682\ (mod\ 676) \equiv 514\ (mod\ 676) = 514$$
$$P_{14}(HC) = 514 = 19 \times 26 + 20 \rightarrow TU$$
$$P_{15}(IY) \equiv a^{-1}c'_{15} - a^{-1}b(mod\ N^2) \equiv 69 \times 232 - 14\ (mod\ 676)$$
$$\equiv 15994\ (mod\ 676) \equiv 446\ (mod\ 676) = 446$$
$$P_{15}(IY) = 446 = 17 \times 26 + 4 \rightarrow RE$$
$$P_{16}(BM) \equiv a^{-1}c'_{16} - a^{-1}b\ (mod\ N^2) \equiv 69 \times 38 - 14\ (mod\ 676)$$
$$\equiv 2608(mod\ 676) \equiv 580\ (mod\ 676) = 580$$
$$P_{16}(BM) = 580 = 22 \times 26 + 8 \rightarrow WI$$
$$P_{17}(OD) \equiv a^{-1}c'_{17} - a^{-1}b\ (mod\ N^2) \equiv 69 \times 367 - 14(mod\ 676)$$
$$\equiv 25309\ (mod\ 676) \equiv 297\ (mod\ 676) = 297$$
$$P_{17}(OD) = 297 = 11 \times 26 + 11 \rightarrow LL$$
$$P_{18}(IP) \equiv a^{-1}c'_{18} - a^{-1}b(mod\ N^2) \equiv 69 \times 223 - 14(mod\ 676)$$
$$\equiv 15373\ (mod\ 676) \equiv 501\ (mod\ 676) = 501$$
$$P_{18}(IP) = 501 = 19 \times 26 + 7 \rightarrow TH$$
$$P_{19}(YX) \equiv a^{-1}c'_{19} - a^{-1}b(mod\ N^2) \equiv 69 \times 647 - 14(mod\ 676)$$
$$\equiv 44629\ (mod\ 676) \equiv 13\ (mod\ 676) = 13$$
$$P_{19}(YX) = 13 = 0 \times 26 + 13 \rightarrow AN$$
$$P_{20}(PQ) \equiv a^{-1}c'_{20} - a^{-1}b(mod\ N^2) \equiv 69 \times 406 - 14(mod\ 676)$$
$$\equiv 28000\ (mod\ 676) \equiv 284\ (mod\ 676) = 284$$

$$P_{20}(PQ) = 284 = 10 \times 26 + 24 \rightarrow KY$$

$$P_{21}(WC) \equiv a^{-1}c'_{21} - a^{-1}b(mod\ N^2) \equiv 69 \times 574 - 14(mod\ 676)$$

$$\equiv 39592\ (mod\ 676) \equiv 384\ (mod\ 676) = 384$$

$$P_{21}(WC) = 384 = 14 \times 26 + 20 \rightarrow OU$$

$$P_{22}(LU) \equiv a^{-1}c'_{22} - a^{-1}b(mod\ N^2) \equiv 69 \times 306 - 14(mod\ 676)$$

$$\equiv 21100(mod\ 676) \equiv 144\ (mod\ 676) = 144$$

$$P_{22}(LU) = 144 = 5 \times 26 + 14 \rightarrow FO$$

$$P_{23}(QM) \equiv a^{-1}c'_{23} - a^{-1}b(mod\ N^2) \equiv 69 \times 428 - 14(mod\ 676)$$

$$\equiv 29518\ (mod\ 676) \equiv 450\ (mod\ 676) = 450$$

$$P_{23}(QM) = 450 = 17 \times 26 + 8 \rightarrow RI$$

$$P_{24}(XH) \equiv a^{-1}c'_{24} - a^{-1}b(mod\ N^2) \equiv 69 \times 605 - 14(mod\ 676)$$

$$\equiv 41731\ (mod\ 676) \equiv 495\ (mod\ 676) = 495$$

$$P_{24}(XH) = 495 = 19 \times 26 + 1 \rightarrow TB$$

$$P_{25}(SE) \equiv a^{-1}c'_{25} - a^{-1}b(mod\ N^2) \equiv 69 \times 472 - 14(mod\ 676)$$

$$\equiv 32554\ (mod\ 676) \equiv 106\ (mod\ 676) = 106$$

$$P_{25}(SE) = 106 = 4 \times 26 + 2 \rightarrow EC$$

$$P_{26}(MC) \equiv a^{-1}c'_{26} - a^{-1}b(mod\ N^2) \equiv 69 \times 314 - 14(mod\ 676)$$

$$\equiv 21652(mod\ 676) \equiv 20\ (mod\ 676) = 20$$

$$P_{26}(MC) = 20 = 0 \times 26 + 20 \rightarrow AU$$

$$P_{27}(FY) \equiv (a^{-1}c'_{27} - a^{-1}b)mod\ N^2 \equiv (69 \times 154 - 14)mod\ 676$$

$$\equiv 10612\ (mod\ 676) \equiv 472\ (mod\ 676) = 472$$

$$P_{27}(FY) = 472 = 18 \times 26 + 4 \rightarrow SE$$

$$P_{28}(KC) \equiv a^{-1}c'_{28} - a^{-1}b(mod\ N^2) \equiv 69 \times 262 - 14(mod\ 676)$$

$$\equiv 18064\ (mod\ 676) \qquad \equiv 488\ (mod\ 676) = 488$$

$$P_{28}(KC) = 488 = 18 \times 26 + 20 \qquad \rightarrow SU$$

$$P_{29}(YE) \equiv a^{-1}c'_{29} - a^{-1}b(mod\ N^2) \qquad \equiv 69 \times 628 - 14(mod\ 676)$$

$$\equiv 43318\ (mod\ 676) \qquad \equiv 54\ (mod\ 676) = 54$$

$$P_{29}(YE) = 54 = 2 \times 26 + 2 \qquad \rightarrow CC$$

$$P_{30}(WI) \equiv a^{-1}c'_{30} - a^{-1}b(mod\ N^2) \qquad \equiv 69 \times 580 - 14(mod\ 676)$$

$$\equiv 40006\ (mod\ 676) \qquad \equiv 122\ (mod\ 676) = 122$$

$$P_{30}(WI) = 122 = 4 \times 26 + 18 \qquad \rightarrow ES$$

$$P_{31}(CE) \equiv a^{-1}c'_{31} - a^{-1}b(mod\ N^2) \qquad \equiv 69 \times 56 - 14(mod\ 676)$$

$$\equiv 3850\ (mod\ 676) \qquad \equiv 470\ (mod\ 676) = 470$$

$$P_{31}(CE) = 470 = 18 \times 26 + 2 \qquad \rightarrow SC$$

$$P_{32}(HA) \equiv a^{-1}c'_{32} - a^{-1}b(mod\ N^2) \qquad \equiv 69 \times 182 - 14(mod\ 676)$$

$$\equiv 12544(mod\ 676) \qquad \equiv 376\ (mod\ 676) = 376$$

$$P_{32}(HA) = 376 = 14 \times 26 + 12 \qquad \rightarrow OM$$

$$P_{33}(WI) \equiv a^{-1}c'_{33} - a^{-1}b(mod\ N^2) \qquad \equiv 69 \times 580 - 14(mod\ 676)$$

$$\equiv 40006\ (mod\ 676) \qquad \equiv 122\ (mod\ 676) = 122$$

$$P_{33}(WI) = 122 = 4 \times 26 + 18 \qquad \rightarrow ES$$

$$P_{34}(RL) \equiv a^{-1}c'_{34} - a^{-1}b(mod\ N^2) \qquad \equiv 69 \times 453 - 14(mod\ 676)$$

$$\equiv 31243\ (mod\ 676) \qquad \equiv 147\ (mod\ 676) = 147$$

$$P_{34}(RL) = 147 = 5 \times 26 + 17 \qquad \rightarrow FR$$

$$P_{35}(HA) \equiv a^{-1}c'_{35} - a^{-1}b(mod\ N^2) \qquad \equiv 69 \times 182 - 14(mod\ 676)$$

$$\equiv 12544\ (mod\ 676) \qquad \equiv 376\ (mod\ 676) = 376$$

$$P_{35}(HA) = 376 = 14 \times 26 + 12 \qquad \rightarrow OM$$

$$P_{36}(ZP) \equiv a^{-1}c'_{36} - a^{-1}b(mod\ N^2) \equiv 69 \times 665 - 14(mod\ 676)$$
$$\equiv 45871(mod\ 676) \equiv 579\ (mod\ 676) = 579$$
$$P_{36}(ZP) = 579 = 22 \times 26 + 7 \rightarrow WH$$
$$P_{37}(KF) \equiv a^{-1}c'_{37} - a^{-1}b(mod\ N^2) \equiv 69 \times 265 - 14(mod\ 676)$$
$$\equiv 18271\ (mod\ 676) \equiv 19\ (mod\ 676) = 19$$
$$P_{37}(KF) = 19 = 0 \times 26 + 19 \rightarrow AT$$
$$P_{38}(GU) \equiv a^{-1}c'_{38} - a^{-1}b(mod\ N^2) \equiv 69 \times 176 - 14(mod\ 676)$$
$$\equiv 12130\ (mod\ 676) \equiv 638\ (mod\ 676) = 638$$
$$P_{38}(GU) = 638 = 24 \times 26 + 14 \rightarrow YO$$
$$P_{39}(YB) \equiv a^{-1}c'_{39} - a^{-1}b(mod\ N^2) \equiv 69 \times 625 - 14(mod\ 676)$$
$$\equiv 43111\ (mod\ 676) \equiv 523\ (mod\ 676) = 523$$
$$P_{39}(YB) = 523 = 20 \times 26 + 3 \rightarrow UD$$
$$P_{40}(OE) \equiv a^{-1}c'_{40} - a^{-1}b(mod\ N^2) \equiv 69 \times 368 - 14(mod\ 676)$$
$$\equiv 25378\ (mod\ 676) \equiv 366\ (mod\ 676) = 366$$
$$P_{40}(OE) = 366 = 14 \times 26 + 2 \rightarrow OC$$
$$P_{41}(IX) \equiv a^{-1}c'_{41} - a^{-1}b(mod\ N^2) \equiv 69 \times 231 - 14(mod\ 676)$$
$$\equiv 15925\ (mod\ 676) \equiv 377\ (mod\ 676) = 377$$
$$P_{41}(IX) = 377 = 14 \times 26 + 13 \rightarrow ON$$
$$P_{42}(NM) \equiv a^{-1}c'_{42} - a^{-1}b(mod\ N^2) \equiv 69 \times 350 - 14(mod\ 676)$$
$$\equiv 24136\ (mod\ 676) \equiv 476\ (mod\ 676) = 476$$
$$P_{42}(NM) = 476 = 18 \times 26 + 8 \rightarrow SI$$
$$P_{43}(IF) \equiv a^{-1}c'_{43} - a^{-1}b(mod\ N^2) \equiv 69 \times 213 - 14(mod\ 676)$$
$$\equiv 14683\ (mod\ 676) \equiv 487\ (mod\ 676) = 487$$

$$P_{43}(IF) = 487 = 18 \times 26 + 19 \rightarrow ST$$

$$P_{44}(MX) \equiv a^{-1}c'_{44} - a^{-1}b(mod\ N^2) \equiv 69 \times 335 - 14(mod\ 676)$$

$$\equiv 23101\ (mod\ 676) \equiv 117\ (mod\ 676) = 117$$

$$P_{44}(MX) = 117 = 4 \times 26 + 13 \rightarrow EN$$

$$P_{45}(MQ) \equiv a^{-1}c'_{45} - a^{-1}b(mod\ N^2) \equiv 69 \times 328 - 14(mod\ 676)$$

$$\equiv 22618\ (mod\ 676) \equiv 310\ (mod\ 676) = 310$$

$$P_{45}(MQ) = 310 = 11 \times 26 + 24 \rightarrow LY$$

Dengan demikian, *ciphertext* :

IUSUCSRAPCYLQHEQRAZL\USFCXBXRSHV^DRASCAQ]XFUQVCBYTV XLSZXST]RXTBP]RIFBPKAZL\VSH^TRCNVRLVCVQ. Setelah didekripsi, kembali menjadi bentuk *plaintext* : DO SOMETHING TODAY THAT YOUR FUTURE WILL THANK YOU FOR IT BECAUSE SUCCESS COMES FROM WHAT YOU DO CONSISTENLY.

BAB IV
PENUTUP

4.1 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. Kemudian proses dekripsi pesan yang dilakukan, mampu mengembalikan pesan yang terenkripsi. Sehingga, penggabungan dua algoritma yaitu transformasi digraf dan kriptografi DNA menghasilkan teks sandi yang acak dan baik digunakan untuk melakukan enkripsi pesan rahasia.

4.2 Saran

Berdasarkan hasil analisis yang telah dilakukan pada penelitian ini, peneliti selanjutnya 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.

DAFTAR PUSTAKA

Al-Quran dan Terjemahnya. 1998. Al Basyir. Semarang: ASY-SYIFA'

Abidin, Z. (2017). Penafsiran Ayat-ayat Amanah Dalam Al-Qur'an. *Jurnal Syahadah vol. V, No. 2*, 122-140.

Andriana, E. (2016). Algoritma Enkripsi Playfair Cipher. *www.researchgate.net*, 2.

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

Az-Zuhaili, P. D. (2013). *Tafsir Al Wasith.* Depok: GEMA INSANI.

Elfadel, A. (2014). Cryptography by Means of Linear Algebra and Number Theory. 41-43.

Gallian, J. A. (2012). *Contemporary Abstract Algebra, 8th Edition.* USA: Brooks/Cole Cengage Learning.

Ginting, D. B. (2010). Peranan Aritmetika Modulo dan Bilangan Prima Pada Algoritma Kriptografi RSA. *Media Informasi Vol. 9 No. 2*, 48.

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

Imam, S. (2008). *Tafsir Al Qurthubi.* Jakarta: PUSTAKA AZZAM.

Irawan, W. H., Hijriyah, N., & Habibi, A. R. (2014). *Pengantar Teori Bilangan.* Malang: UIN-MALIKI PRESS.

Kromodimoeljo, S. (2009). *Teori Aplikasi dan Kriptografi.* SPK IT Consulting.

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

Munir, R. (2004). Teori Bilangan (Number Theory). *Bahan Kuliah Ke-3. IF5054 Kriptografi*, 2-3.

Munir, R. (2004). Teori Bilangan (Number Theory) . *Bahan Kuliah. IF5054 Kriptografi*, 8-9.

Munir, R. (2006). *Kriptografi.* Bandung: Inform.

Munir, R. (2019). *Kriptografi Edisi Kedua.* Bandung: INFORMATIKA.

Munir, R. (n.d.). *informatika.stei.itb.ac.id.* Retrieved November 21, 2020, from informatika.stei.itb.ac.id: https://informatika.stei.itb.ac.id/~rinaldi.munir/Buku/Kriptografi/Bab-1_Pengantar%20Kriptografi.pdf

Nadeak, T. A. (2019). Perancangan Aplikasi Pembelajaran Kriptografi Algoritma GOST dengan Menggunakan Metode Computer Based Instruction. *KAKIFIKOM (Kumpulan Artikel Karya Ilm, Fak. Ilmu Komputer), vol. 1, no. 1*, 40-46.

Parama, R. I. (2016/2017). Aplikasi Teori Bilangan Dalam Kriptografi Untuk Keamanan Teknologi Informasi Dalam Bentuk Algoritma RSA. *Makalah IF2120 Matematika Diskrit*, 2.

Qiao, C. S. (2015). A Novel Image Encryption Algorithm Based on DNA Encoding and Spatiotemporal Chaos. *Entropy*, 6956.

Raj, B. B., J. Frank Vijay, P., & T. Mahalakshmi, P. (2016). Secure Data Transfer through DNA Cryptography using Symmetric Algorithm. *International Journal of Computer Applications Volume 133- No. 2*, 22.

RI, K. A. (2011). *Al-Qur'an Dan Tafsirnya Edisi yang Disempurnakan.* Jakarta: Widya Cahaya.

Riskiyah, W. (2016). Enkripsi dan Dekripsi Pesan Menggunakan Grup Simetri untuk Mengamankan Informasi. *SKRIPSI*, 2-3.

Sansani, S. (2008). Penggunaan Aritmetika Modulo dan Balikan Modulo pada Modifikasi Algoritma Knapsack. 3-4.

Sasmita, A. (2014). Makalah Aritmetika Modulo.

Sholehah, D. P. (2017). Penerapan Algoritma DNA-Vigenere Cipher dengan Kunci Citra Grayscale pada Data Teks. *Digital Repository Universitas Jember*, 11.

Siambaton, M. Z., & Muhazir, A. (2018). Modifikasi Algoritma Playfair Cipher dengan Pengurutan Array pada Matriks. *ALGORITMA : Jural Ilmu Komputer dan Informatika*, 66-67.

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

Surbakti, S. D. (2019). Imlementasi Algoritma Plafair Cipher pada Penyandian Data. *Jurnal Teknik Informatika Unika St. Thomas (JYIUST), Bolume 04 Nomor 02*, 125.

Toisutta, E. Y. (n.d.). Penerapan Kombinasi Playfair Cipher dan Digraph Cipher. 2.

Tung, K. Y. (2008). *Memahami Teori Bilangan Dengan Mudah dan Menarik.* Jakarta: PT. Gramedia Widiasarana Indonesia.

Vidhya, E., & Rathipriya, R. (2018). Two Level Text Data Encryption using DNA. *International Journal of Computational Intelligence and Informatics*, 107.

Wassil, I. K. (2009). *Tafsir Quran Ulul Albab.* Bandung: PT Karya Kita.

Wicaksono, D. R. (2014). Aplikasi Aljabar Min-Plus untuk Mengamankan Informasi Rahasia. *Skripsi*, 7.

Yuliandaru, A. R. (2015/2016). Teknik Kriptografi Hill Cipher Menggunakan Matriks. *Makalah IF2123 Aljabar Geometri-Informatika ITB*, 2.

LAMPIRAN - LAMPIRAN

Lampiran 1: Tabel *Alphabet*

A	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**
0	1	2	3	4	5	6	7	8	9	10	11	12
N	**O**	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**
13	14	15	16	17	18	19	20	21	22	23	24	25

Lampiran 2: Tabel ASCII

Kode ASCII (desimal)	**Kode ASCII (Biner)**	**Karakter**
00	00000000	NULL
01	00000001	SOH
02	00000010	STX
03	00000011	ETX
04	00000100	EOT
05	00000101	ENQ
06	00000110	ACK
07	00000111	BEL
08	00001000	BS
09	00001001	HT
10	00001010	LF
11	00001011	VT
12	00001100	FF
13	00001101	CR
14	00001110	SO
15	00001111	SI
16	00010000	DLE
17	00010001	DC1
18	00010010	DC2
19	00010011	DC3
20	00010100	DC4
21	00010101	NAK

22	00010110	SYN
23	00010111	ETB
24	00011000	CAN
25	00011001	EM
26	00011010	SUB
27	00011011	ESC
28	00011100	FS
29	00011101	GS
30	00011110	RS
31	00011111	US
32	00100000	space
33	00100001	!
34	00100010	"
35	00100011	#
36	00100100	$
37	00100101	%
38	00100110	&
39	00100111	'
40	00101000	(
41	00101001	)
42	00101010	*
43	00101011	+
44	00101100	,
45	00101101	-
46	00101110	.
47	00101111	/
48	00110000	0
49	00110001	1
50	00110010	2
51	00110011	3
52	00110100	4

53	00110101	5
54	00110110	6
55	00110111	7
56	00111000	8
57	00111001	9
58	00111010	:
59	00111011	;
60	00111100	<
61	00111101	=
62	00111110	>
63	00111111	?
64	01000000	@
65	01000001	A
66	01000010	B
67	01000011	C
68	01000100	D
69	01000101	E
70	01000110	F
71	01000111	G
72	01001000	H
73	01001001	I
74	01001010	J
75	01001011	K
76	01001100	L
77	01001101	M
78	01001110	N
79	01001111	O
80	01010000	P
81	01010001	Q
82	01010010	R
83	01010011	S

84	01010100	T
85	01010101	U
86	01010110	V
87	01010111	W
88	01011000	X
89	01011001	Y
90	01011010	Z
91	01011011	[
92	01011100	\
93	01011101	]
94	01011110	^
95	01011111	_
96	01100000	`
97	01100001	a
98	01100010	b
99	01100011	c
100	01100100	d
101	01100101	e
102	01100110	f
103	01100111	g
104	01101000	h
105	01101001	i
106	01101010	j
107	01101011	k
108	01101100	l
109	01101101	m
110	01101110	n
111	01101111	o
112	01110000	p
113	01110001	q
114	01110010	r

115	01110011	s
116	01110100	t
117	01110101	u
118	01110110	v
119	01110111	w
120	01111000	x
121	01111001	y
122	01111010	z
123	01111011	{
124	01111100	|
125	01111101	}
126	01111110	~
127	01111111	DEL
128	10000000	Ç
129	10000001	ü
130	10000010	é
131	10000011	â
132	10000100	ä
133	10000101	à
134	10000110	å
135	10000111	ç
136	10001000	ê
137	10001001	ë
138	10001010	è
139	10001011	ï
140	10001100	î
141	10001101	ì
142	10001110	Ä
143	10001111	Å
144	10010000	É
145	10010001	æ

146	10010010	Æ
147	10010011	ô
148	10010100	ö
149	10010101	ò
150	10010110	û
151	10010111	ù
152	10011000	ÿ
153	10011001	Ö
154	10011010	Ü
155	10011011	ø
156	10011100	£
157	10011101	Ø
158	10011110	×
159	10011111	*f*
160	10100000	á
161	10100001	í
162	10100010	ó
163	10100011	ú
164	10100100	ñ
165	10100101	Ñ
166	10100110	ª
167	10100111	º
168	10101000	¿
169	10101001	®
170	10101010	¬
171	10101011	½
172	10101100	¼
173	10101101	¡
174	10101110	«
175	10101111	»
176	10110000	▒

177	10110001	▒
178	10110010	▓
179	10110011	│
180	10110100	┤
181	10110101	Á
182	10110110	Â
183	10110111	À
184	10111000	©
185	10111001	╣
186	10111010	║
187	10111011	╗
188	10111100	╝
189	10111101	¢
190	10111110	¥
191	10111111	┐
192	11000000	└
193	11000001	┴
194	11000010	┬
195	11000011	├
196	11000100	─
197	11000101	┼
198	11000110	ã
199	11000111	Ã
200	11001000	╚
201	11001001	╔
202	11001010	╩
203	11001011	╦
204	11001100	╠
205	11001101	═
206	11001110	╬
207	11001111	¤

208	11010000	ð
209	11010001	Ð
210	11010010	Ê
211	11010011	Ë
212	11010100	È
213	11010101	ı
214	11010110	Í
215	11010111	Î
216	11011000	Ï
217	11011001	┘
218	11011010	┌
219	11011011	█
220	11011100	▄
221	11011101	¦
222	11011110	Ì
223	11011111	▀
224	11100000	Ó
225	11100001	ß
226	11100010	Ô
227	11100011	Ò
228	11100100	õ
229	11100101	Õ
230	11100110	µ
231	11100111	þ
232	11101000	Þ
233	11101001	Ú
234	11101010	Û
235	11101011	Ù
236	11101100	ý
237	11101101	Ý
238	11101110	¯

239	11101111	´
240	11110000	≡
241	11110001	±
242	11110010	‗
243	11110011	¾
244	11110100	¶
245	11110101	§
246	11110110	÷
247	11110111	¸
248	11111000	°
249	11111001	¨
250	11111010	·
251	11111011	¹
252	11111100	³
253	11111101	²
254	11111110	■
255	11111111	nbsp

Lampiran 3: Tabel Proses Perhitungan Kunci Pembangun Acak Kriptografi DNA

Kode Desimal	**Kode Biner**	**Balikan Kode Biner**	**Kode Biner : Kunci (: 1000)**		**Hasil**	**Kode DNA**
			Sisa	**Hasil Bagi**		
00	00000000	00000000	0	0	00000000	AAAA
01	00000001	10000000	0	10000	00010000	ACAA
02	00000010	01000000	0	1000	00001000	AAGA
03	00000011	11000000	0	11000	00011000	ACGA
04	00000100	00100000	0	100	00000100	AACA
05	00000101	10100000	0	10100	00010100	ACCA
06	00000110	01100000	0	1100	00001100	AATA
07	00000111	11100000	0	11100	00011100	ACTA
08	00001000	00010000	0	10	00000010	AAAG

09	00001001	10010000	0	10010	00010010	ACAG
10	00001010	01010000	0	1010	00001010	AAGG
11	00001011	11010000	0	11010	00011010	ACGG
12	00001100	00110000	0	110	00000110	AACG
13	00001101	10110000	0	10110	00010110	ACCG
14	00001110	01110000	0	1110	00001110	AATG
15	00001111	11110000	0	11110	00011110	ACTG
16	00010000	00001000	0	1	00000001	AAAC
17	00010001	10001000	0	10001	00010001	ACAC
18	00010010	01001000	0	1001	00001001	AAGC
19	00010011	11001000	0	11001	00011001	ACGC
20	00010100	00101000	0	101	00000101	AACC
21	00010101	10101000	0	10101	00010101	ACCC
22	00010110	01101000	0	1101	00001101	AATC
23	00010111	11101000	0	11101	00011101	ACTC
24	00011000	00011000	0	11	00000011	AAAT
25	00011001	10011000	0	10011	00010011	ACAT
26	00011010	01011000	0	1011	00001011	AAGT
27	00011011	11011000	0	11011	00011011	ACGT
28	00011100	00111000	0	111	00000111	AACT
29	00011101	10111000	0	10111	00010111	ACCT
30	00011110	01111000	0	1111	00001111	AATT
31	00011111	11111000	0	11111	00011111	ACTT
32	00100000	00000100	100	0	10000000	GAAA
33	00100001	10000100	100	10000	10010000	GCAA
34	00100010	01000100	100	1000	10001000	GAGA
35	00100011	11000100	100	11000	10011000	GCGA
36	00100100	00100100	100	100	10000100	GACA
37	00100101	10100100	100	10100	10010100	GCCA
38	00100110	01100100	100	1100	10001100	GATA
39	00100111	11100100	100	11100	10011100	GCTA

40	00101000	00010100	100	10	10000010	GAAG
41	00101001	10010100	100	10010	10010010	GCAG
42	00101010	01010100	100	1010	10001010	GAGG
43	00101011	11010100	100	11010	10011010	GCGG
44	00101100	00110100	100	110	10000110	GACG
45	00101101	10110100	100	10110	10010110	GCCG
46	00101110	01110100	100	1110	10001110	GATG
47	00101111	11110100	100	11110	10011110	GCTG
48	00110000	00001100	100	1	10000001	GAAC
49	00110001	10001100	100	10001	10010001	GCAC
50	00110010	01001100	100	1001	10001001	GAGC
51	00110011	11001100	100	11001	10011001	GCGC
52	00110100	00101100	100	101	10000101	GACC
53	00110101	10101100	100	10101	10010101	GCCC
54	00110110	01101100	100	1101	10001101	GATC
55	00110111	11101100	100	11101	10011101	GCTC
56	00111000	00011100	100	11	10000011	GAAT
57	00111001	10011100	100	10011	10010011	GCAT
58	00111010	01011100	100	1011	10001011	GAGT
59	00111011	11011100	100	11011	10011011	GCGT
60	00111100	00111100	100	111	10000111	GACT
61	00111101	10111100	100	10111	10010111	GCCT
62	00111110	01111100	100	1111	10001111	GATT
63	00111111	11111100	100	11111	10011111	GCTT
64	01000000	00000010	10	0	01000000	CAAA
65	01000001	10000010	10	10000	01010000	CCAA
66	01000010	01000010	10	1000	01001000	CAGA
67	01000011	11000010	10	11000	01011000	CCGA
68	01000100	00100010	10	100	01000100	CACA
69	01000101	10100010	10	10100	01010100	CCCA
70	01000110	01100010	10	1100	01001100	CATA

71	01000111	11100010	10	11100	01011100	CCTA
72	01001000	00010010	10	10	01000010	CAAG
73	01001001	10010010	10	10010	01010010	CCAG
74	01001010	01010010	10	1010	01001010	CAGG
75	01001011	11010010	10	11010	01011010	CCGG
76	01001100	00110010	10	110	01000110	CACG
77	01001101	10110010	10	10110	01010110	CCCG
78	01001110	01110010	10	1110	01001110	CATG
79	01001111	11110010	10	11110	01011110	CCTG
80	01010000	00001010	10	1	01000001	CAAC
81	01010001	10001010	10	10001	01010001	CCAC
82	01010010	01001010	10	1001	01001001	CAGC
83	01010011	11001010	10	11001	01011001	CCGC
84	01010100	00101010	10	101	01000101	CACC
85	01010101	10101010	10	10101	01010101	CCCC
86	01010110	01101010	10	1101	01001101	CATC
87	01010111	11101010	10	11101	01011101	CCTC
88	01011000	00011010	10	11	01000011	CAAT
89	01011001	10011010	10	10011	01010011	CCAT
90	01011010	01011010	10	1011	01001011	CAGT
91	01011011	11011010	10	11011	01011011	CCGT
92	01011100	00111010	10	111	01000111	CACT
93	01011101	10111010	10	10111	01010111	CCCT
94	01011110	01111010	10	1111	01001111	CATT
95	01011111	11111010	10	11111	01011111	CCTT
96	01100000	00000110	110	0	11000000	TAAA
97	01100001	10000110	110	10000	11010000	TCAA
98	01100010	01000110	110	1000	11001000	TAGA
99	01100011	11000110	110	11000	11011000	TCGA
100	01100100	00100110	110	100	11000100	TACA
101	01100101	10100110	110	10100	11010100	TCCA

102	01100110	01100110	110	1100	11001100	TATA
103	01100111	11100110	110	11100	11011100	TCTA
104	01101000	00010110	110	10	11000010	TAAG
105	01101001	10010110	110	10010	11010010	TCAG
106	01101010	01010110	110	1010	11001010	TAGG
107	01101011	11010110	110	11010	11011010	TCGG
108	01101100	00110110	110	110	11000110	TACG
109	01101101	10110110	110	10110	11010110	TCCG
110	01101110	01110110	110	1110	11001110	TATG
111	01101111	11110110	110	11110	11011110	TCTG
112	01110000	00001110	110	1	11000001	TAAC
113	01110001	10001110	110	10001	11010001	TCAC
114	01110010	01001110	110	1001	11001001	TAGC
115	01110011	11001110	110	11001	11011001	TCGC
116	01110100	00101110	110	101	11000101	TACC
117	01110101	10101110	110	10101	11010101	TCCC
118	01110110	01101110	110	1101	11001101	TATC
119	01110111	11101110	110	11101	11011101	TCTC
120	01111000	00011110	110	11	11000011	TAAT
121	01111001	10011110	110	10011	11010011	TCAT
122	01111010	01011110	110	1011	11001011	TAGT
123	01111011	11011110	110	11011	11011011	TCGT
124	01111100	00111110	110	111	11000111	TACT
125	01111101	10111110	110	10111	11010111	TCCT
126	01111110	01111110	110	1111	11001111	TATT
127	01111111	11111110	110	11111	11011111	TCTT
128	10000000	00000001	1	0	00100000	AGAA
129	10000001	10000001	1	10000	00110000	ATAA
130	10000010	01000001	1	1000	00101000	AGGA
131	10000011	11000001	1	11000	00111000	ATGA
132	10000100	00100001	1	100	00100100	AGCA

133	10000101	10100001	1	10100	00110100	ATCA
134	10000110	01100001	1	1100	00101100	AGTA
135	10000111	11100001	1	11100	00111100	ATTA
136	10001000	00010001	1	10	00100010	AGAG
137	10001001	10010001	1	10010	00110010	ATAG
138	10001010	01010001	1	1010	00101010	AGGG
139	10001011	11010001	1	11010	00111010	ATGG
140	10001100	00110001	1	110	00100110	AGCG
141	10001101	10110001	1	10110	00110110	ATCG
142	10001110	01110001	1	1110	00101110	AGTG
143	10001111	11110001	1	11110	00111110	ATTG
144	10010000	00001001	1	1	00100001	AGAC
145	10010001	10001001	1	10001	00110001	ATAC
146	10010010	01001001	1	1001	00101001	AGGC
147	10010011	11001001	1	11001	00111001	ATGC
148	10010100	00101001	1	101	00100101	AGCC
149	10010101	10101001	1	10101	00110101	ATCC
150	10010110	01101001	1	1101	00101101	AGTC
151	10010111	11101001	1	11101	00111101	ATTC
152	10011000	00011001	1	11	00100011	AGAT
153	10011001	10011001	1	10011	00110011	ATAT
154	10011010	01011001	1	1011	00101011	AGGT
155	10011011	11011001	1	11011	00111011	ATGT
156	10011100	00111001	1	111	00100111	AGCT
157	10011101	10111001	1	10111	00110111	ATCT
158	10011110	01111001	1	1111	00101111	AGTT
159	10011111	11111001	1	11111	00111111	ATTT
160	10100000	00000101	101	0	101000	GGAA
161	10100001	10000101	101	10000	101100	GTAA
162	10100010	01000101	101	1000	10101000	GGGA
163	10100011	11000101	101	11000	10111000	GTGA

164	10100100	00100101	101	100	10100100	GGCA
165	10100101	10100101	101	10100	10110100	GTCA
166	10100110	01100101	101	1100	10101100	GGTA
167	10100111	11100101	101	11100	10111100	GTTA
168	10101000	00010101	101	10	10100010	GGAG
169	10101001	10010101	101	10010	10110010	GTAG
170	10101010	01010101	101	1010	10101010	GGGG
171	10101011	11010101	101	11010	10111010	GTGG
172	10101100	00110101	101	110	10100110	GGCG
173	10101101	10110101	101	10110	10110110	GTCG
174	10101110	01110101	101	1110	10101110	GGTG
175	10101111	11110101	101	11110	10111110	GTTG
176	10110000	00001101	101	1	10100001	GGAC
177	10110001	10001101	101	10001	10110001	GTAC
178	10110010	01001101	101	1001	10101001	GGGC
179	10110011	11001101	101	11001	10111001	GTGC
180	10110100	00101101	101	101	10100101	GGCC
181	10110101	10101101	101	10101	10110101	GTCC
182	10110110	01101101	101	1101	10101101	GGTC
183	10110111	11101101	101	11101	10111101	GTTC
184	10111000	00011101	101	11	10100011	GGAT
185	10111001	10011101	101	10011	10110011	GTAT
186	10111010	01011101	101	1011	10101011	GGGT
187	10111011	11011101	101	11011	10111011	GTGT
188	10111100	00111101	101	111	10100111	GGCT
189	10111101	10111101	101	10111	10110111	GTCT
190	10111110	01111101	101	1111	10101111	GGTT
191	10111111	11111101	101	11111	10111111	GTTT
192	11000000	00000011	11	0	01100000	CGAA
193	11000001	10000011	11	10000	01110000	CTAA
194	11000010	01000011	11	1000	01101000	CGGA

195	11000011	11000011	11	11000	01111000	CTGA
196	11000100	00100011	11	100	01100100	CGCA
197	11000101	10100011	11	10100	01110100	CTCA
198	11000110	01100011	11	1100	01101100	CGTA
199	11000111	11100011	11	11100	01111100	CTTA
200	11001000	00010011	11	10	01100010	CGAG
201	11001001	10010011	11	10010	01110010	CTAG
202	11001010	01010011	11	1010	01101010	CGGG
203	11001011	11010011	11	11010	01111010	CTGG
204	11001100	00110011	11	110	01100110	CGCG
205	11001101	10110011	11	10110	01110110	CTCG
206	11001110	01110011	11	1110	01101110	CGTG
207	11001111	11110011	11	11110	01111110	CTTG
208	11010000	00001011	11	1	01100001	CGAC
209	11010001	10001011	11	10001	01110001	CTAC
210	11010010	01001011	11	1001	01101001	CGGC
211	11010011	11001011	11	11001	01111001	CTGC
212	11010100	00101011	11	101	01100101	CGCC
213	11010101	10101011	11	10101	01110101	CTCC
214	11010110	01101011	11	1101	01101101	CGTC
215	11010111	11101011	11	11101	01111101	CTTC
216	11011000	00011011	11	11	01100011	CGAT
217	11011001	10011011	11	10011	01110011	CTAT
218	11011010	01011011	11	1011	01101011	CGGT
219	11011011	11011011	11	11011	01111011	CTGT
220	11011100	00111011	11	111	01100111	CGCT
221	11011101	10111011	11	10111	01110111	CTCT
222	11011110	01111011	11	1111	01101111	CGTT
223	11011111	11111011	11	11111	01111111	CTTT
224	11100000	00000111	111	0	11100000	TGAA
225	11100001	10000111	111	10000	11110000	TTAA

226	11100010	01000111	111	1000	11101000	TGGA
227	11100011	11000111	111	11000	11111000	TTGA
228	11100100	00100111	111	100	11100100	TGCA
229	11100101	10100111	111	10100	11110100	TTCA
230	11100110	01100111	111	1100	11101100	TGTA
231	11100111	11100111	111	11100	11111100	TTTA
232	11101000	00010111	111	10	11100010	TGAG
233	11101001	10010111	111	10010	11110010	TTAG
234	11101010	01010111	111	1010	11101010	TGGG
235	11101011	11010111	111	11010	11111010	TTGG
236	11101100	00110111	111	110	11100110	TGCG
237	11101101	10110111	111	10110	11110110	TTCG
238	11101110	01110111	111	1110	11101110	TGTG
239	11101111	11110111	111	11110	11111110	TTTG
240	11110000	00001111	111	1	11100001	TGAC
241	11110001	10001111	111	10001	11110001	TTAC
242	11110010	01001111	111	1001	11101001	TGGC
243	11110011	11001111	111	11001	11111001	TTGC
244	11110100	00101111	111	101	11100101	TGCC
245	11110101	10101111	111	10101	11110101	TTCC
246	11110110	01101111	111	1101	11101101	TGTC
247	11110111	11101111	111	11101	11111101	TTTC
248	11111000	00011111	111	11	11100011	TGAT
249	11111001	10011111	111	10011	11110011	TTAT
250	11111010	01011111	111	1011	11101011	TGGT
251	11111011	11011111	111	11011	11111011	TTGT
252	11111100	00111111	111	111	11100111	TGCT
253	11111101	10111111	111	10111	11110111	TTCT
254	11111110	01111111	111	1111	11101111	TGTT
255	11111111	11111111	111	11111	11111111	TTTT

Lampiran 4: Tabel Kunci Pembangun Acak Kriptografi DNA

0	AAAA	43	GCGG	86	CATC	129	ATAA	172	GGCG	215	CTTC
1	ACAA	44	GACG	87	CCTC	130	AGGA	173	GTCG	216	CGAT
2	AAGA	45	GCCG	88	CAAT	131	ATGA	174	GGTG	217	CTAT
3	ACGA	46	GATG	89	CCAT	132	AGCA	175	GTTG	218	CGGT
4	AACA	47	GCTG	90	CAGT	133	ATCA	176	GGAC	219	CTGT
5	ACCA	48	GAAC	91	CCGT	134	AGTA	177	GTAC	220	CGCT
6	AATA	49	GCAC	92	CACT	135	ATTA	178	GGGC	221	CTCT
7	ACTA	50	GAGC	93	CCCT	136	AGAG	179	GTGC	222	CGTT
8	AAAG	51	GCGC	94	CATT	137	ATAG	180	GGCC	223	CTTT
9	ACAG	52	GACC	95	CCTT	138	AGGG	181	GTCC	224	TGAA
10	AAGG	53	GCCC	96	TAAA	139	ATGG	182	GGTC	225	TTAA
11	ACGG	54	GATC	97	TCAA	140	AGCG	183	GTTC	226	TGGA
12	AACG	55	GCTC	98	TAGA	141	ATCG	184	GGAT	227	TTGA
13	ACCG	56	GAAT	99	TCGA	142	AGTG	185	GTAT	228	TGCA
14	AATG	57	GCAT	100	TACA	143	ATTG	186	GGGT	229	TTCA
15	ACTG	58	GAGT	101	TCCA	144	AGAC	187	GTGT	230	TGTA
16	AAAC	59	GCGT	102	TATA	145	ATAC	188	GGCT	231	TTTA
17	ACAC	60	GACT	103	TCTA	146	AGGC	189	GTCT	232	TGAG
18	AAGC	61	GCCT	104	TAAG	147	ATGC	190	GGTT	233	TTAG
19	ACGC	62	GATT	105	TCAG	148	AGCC	191	GTTT	234	TGGG
20	AACC	63	GCTT	106	TAGG	149	ATCC	192	CGAA	235	TTGG
21	ACCC	64	CAAA	107	TCGG	150	AGTC	193	CTAA	236	TGCG
22	AATC	65	CCAA	108	TACG	151	ATTC	194	CGGA	237	TTCG
23	ACTC	66	CAGA	109	TCCG	152	AGAT	195	CTGA	238	TGTG
24	AAAT	67	CCGA	110	TATG	153	ATAT	196	CGCA	239	TTTG
25	ACAT	68	CACA	111	TCTG	154	AGGT	197	CTCA	240	TGAC
26	AAGT	69	CCCA	112	TAAC	155	ATGT	198	CGTA	241	TTAC
27	ACGT	70	CATA	113	TCAC	156	AGCT	199	CTTA	242	TGGC
28	AACT	71	CCTA	114	TAGC	157	ATCT	200	CGAG	243	TTGC
29	ACCT	72	CAAG	115	TCGC	158	AGTT	201	CTAG	244	TGCC
30	AATT	73	CCAG	116	TACC	159	ATTT	202	CGGG	245	TTCC
31	ACTT	74	CAGG	117	TCCC	160	GGAA	203	CTGG	246	TGTC
32	GAAA	75	CCGG	118	TATC	161	GTAA	204	CGCG	247	TTTC
33	GCAA	76	CACG	119	TCTC	162	GGGA	205	CTCG	248	TGAT
34	GAGA	77	CCCG	120	TAAT	163	GTGA	206	CGTG	249	TTAT
35	GCGA	78	CATG	121	TCAT	164	GGCA	207	CTTG	250	TGGT
36	GACA	79	CCTG	122	TAGT	165	GTCA	208	CGAC	251	TTGT
37	GCCA	80	CAAC	123	TCGT	166	GGTA	209	CTAC	252	TGCT
38	GATA	81	CCAC	124	TACT	167	GTTA	210	CGGC	253	TTCT
39	GCTA	82	CAGC	125	TCCT	168	GGAG	211	CTGC	254	TGTT
40	GAAG	83	CCGC	126	TATT	169	GTAG	212	CGCC	255	TTTT
41	GCAG	84	CACC	127	TCTT	170	GGGG	213	CTCC		
42	GAGG	85	CCCC	128	AGAA	171	GTGG	214	CGTC		

RIWAYAT HIDUP

Widya Nur Faizah, lahir di Kabupaten Malang pada tanggal 25 Februari 2000. Ia sering disapa Widya atau Faiz. Widya merupakan putri pertama dari Bapak Bibit Asrori dan Ibu Nani Triana. Widya memiliki seorang adik bernama Humam Hisyam. Widya beralamat di Jalan Sultan Agung Sempol RT. 04 RW.05 Dusun Sempol, Ardimulyo, Kecamatan Singosari, Malang.

Penulis skripsi berjudul "*Analisis Frekuensi Hasil Enkripsi Pesan Teks dengan Algortima Kriptografi DNA dan Transformasi Digraf*" ini memulai menempuh pendidikan formal di TK Al-Akbar 02 (lulus tahun 2006), kemudian SD Islam Al-Ma'arif 02 Singosari (lulus tahun 2012). Kemudian, Widya terpilih sebagai siswi program akselerasi di MTs Negeri Lawang (lulus tahun 2014), dan melanjutkan pendidikan di SMA Negeri 1 Singosari. Selama di SMA, Widya aktif mengikuti organisasi Badan Dakwah Islam Al-Insyiroch dan diberi kesempatan menjabat sebagai Wakil Ketua (Masa Khidmat 2015-2016). Selain itu, Widya juga tergabung dalam ekstrakurikuler Jurnalistik, dan mengemban amanah sebagai sekretaris pimpinan redaksi Majalah Galaxy SMAN 1 Singosari.

Setelah lulus SMA pada tahun 2017, Widya melanjutkan studi di UIN Maulana Malik Ibrahim Malang dengan memilih program studi Matematika. Ketika masih menjadi mahasiswa baru, Widya diberi amanah untuk menjadi koordinator Divisi Ubudiyah Muharrikah Syabab Mabna Asma' Binti Abi Bakar. Selain itu, Widya juga mengikuti Komunitas Al-Farazi dan diberi amanah sebagai ketua CEO Al Farazi Community.

KEMENTERIAN AGAMA RI
UNIVERSITAS ISLAM NEGERI
MAULANA MALIK IBRAHIM MALANG
FAKULTAS SAINS DAN TEKNOLOGI
Jl. Gajayana No. 50 Dinoyo Malang Telp./Fax.(0341) 558933

BUKTI KONSULTASI SKRIPSI

Nama : Widya Nur Faizah
NIM : 17610029
Fakultas/ Program Studi : Sains dan Teknologi/ Matematika
Judul Skripsi : Analisis Frekuensi Hasil Enkripsi Pesan Teks dengan Algoritma Kriptografi DNA dan Transformasi Digraf
Pembimbing I : Muhammad Khudzaifah, M.Si
Pembimbing II : Dewi Ismiarti, M.Si

No.	Tanggal	Hal	Tanda Tangan
1.	19 April 2021	Konsultasi Bab I dan Bab II	1.
2.	19 April 2021	Konsultasi Bab I dan Bab II dan Kajian Keagamaan	2.
3.	27 April 2021	Revisi Bab I dan Bab II	3.
4.	6 Mei 2021	Konsultasi Bab I, Bab II, dan Bab III	4.
5.	15 Juni 2021	Konsultasi Bab III dan Bab IV	5.
6.	30 September 2021	Konsultasi Bab II, Bab III, dan Kajian Keagamaan	6.
7.	6 Oktober 2021	Konsultasi Bab III, Bab IV, dan Abstrak	7.
8.	1 November 2021	Revisi Bab III, Bab IV dan Abstrak	8.
9.	5 November 2021	Konsultasi Keseluruhan	9.
10.	7 November 2021	ACC Keseluruhan oleh Dosen Pembimbing 1	10.
11.	9 November 2021	ACC Keseluruhan oleh Dosen Pembimbing 2	11.

Malang, 14 Desember 2021
Mengetahui,
Ketua Program Studi Matematika

Dr. Elly Susanti, S.Pd., M.Sc
NIP. 19741129 200012 2 005