ISSN : 2460 – 7797
e-ISSN : 2614-8234
Website : jurnal.umj.ac.id/index.php/fbc
Email : fibonacci@umj.ac.id

FIBONACCI
Jurnal Pendidikan Matematika dan Matematika

PENERAPAN KODE REED SOLOMON PADA KRIPTOSISTEM MCELIECE

Rizki Eka Oktavia [1)*], Putranto Hadi Utomo [2)], Titin Sri Martini [3)]
[1,2,3)] Program Studi Matematika, Fakultas Matematika dan Ilmu Pengetahuan Alam, Universitas Sebelas Maret, Jl. Ir. Sutami No.36, Kentingan, Jebres, Kota Surakarta, 57126

[*] *rizkiekaoktavia@student.uns.ac.id*

ABSTRACT

In this modern era, the security of message transmission is weak. Various cryptosystem algorithms are vulnerable being solved by quantum computer that are able to complete calculations faster than conventional computer. The McEliece cryptosystem is relatively safe to use after quantum computer because it utilizes error correcting code. The algorithm is based on adding errors to message so the message is encrypted and cannot be attacked by others. Reed Solomon code is error correction-based codes with certain parameters. In this article, we will explain the application of Reed Solomon code with a length of 15 bits that can correct up to 3 errors in the McEliece cryptosystem.

Keywords*: Quantum Computer, Cryptography, McEliece Cryptosystem, Error-Correcting Codes, Reed Solomon Code*

Abstrak

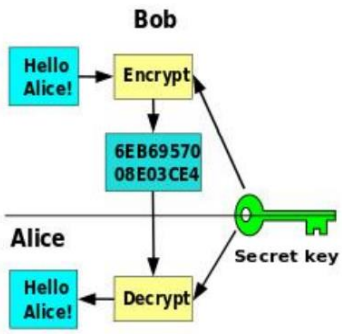
Era modern ini, keamanan pesan dalam suatu transmisi tergolong lemah. Berbagai algoritme kriptosistem rentan dipecahkan oleh komputer kuantum yang mampu menyelesaikan perhitungan lebih cepat dibanding komputer konvensional. Kriptosistem McEliece tergolong aman digunakan pasca komputer kuantum karena memanfaatkan kode pengoreksi eror. Algoritmenya didasarkan pada penambahan eror pada pesan sehingga pesan tersandi dan tidak dapat diserang oleh pihak lain. Kode Reed Solomon merupakan kode berbasis koreksi eror dengan parameter tertentu. Pada artikel ini akan dijelaskan penerapan kode Reed Solomon dengan panjang 15 bit yang dapat mengoreksi hingga 3 eror pada kriptosistem McEliece.

Kata Kunci: *Komputer Kuantum, Kriptografi, Kriptosistem McEliece, Kode Koreksi Eror, Kode Reed Solomon.*

DOI: https://dx.doi.org/10.24853/fbc.9.1.79-88

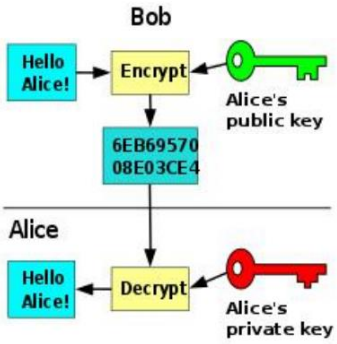
PENDAHULUAN

Internet dikenal sebagai sarana komunikasi yang tergolong mudah. Kemudahannya tidak menutup kemungkinan buruk terkait keamanan pesan. Suatu data menurut Suryono (2022) sangat rawan mengalami suatu corrupt meski dalam jumlah kecil yang dapat menyebabkan kesalahan dalam informasinya. Kriptografi menjadi solusi pengamanan pesan. Kriptografi menurut Menezes et al. (1997) adalah studi tentang teknik matematika yang terkait dengan aspek keamanan informasi meliputi kerahasiaan, integritas data, autentikasi, dan anti-penyangkalan. Menurut Sinaga (2017), kriptografi dibedakan menjadi 2 jenis, yaitu kriptografi kunci simetris dan kriptografi kunsi asimetris. Kriptografi kunci simetris menggunakan kunci privat dalam mekanisme enkripsi dan dekripsi, sedangkan kriptografi kunci asimetris menggunakan kunci publik pada enkripsi dan kunci privat pada dekripsi. Kunci publik merupakan kunci yang bersifat terbuka, artinya dapat diketahui oleh banyak pihak, sedangkan kunci privat bersifat rahasia. Skema kriptografi kunci simetris diberikan pada Gambar 1 dan kriptografi kunci asimetris diberikan pada Gambar 2.



Sumber : Matius (2017)

Gambar 1. Skema kriptografi kunci simetris



Sumber : Matius (2017)

Gambar 2. Skema kriptografi kunci asimetris

Seiring perkembangan teknologi, berbagai algoritme kriptografi yang diciptakan sebelumnya seperti Diffie-Helman key exchange, enkripsi kunci publik Rivest-Shamir-Adleman (RSA), Algebraic Homomorphic, Buchmann-Williams key exchange, dan kurva eliptik telah digagalkan oleh komputasi komputer kuantum. Komputer kuantum menurut Bernstein et al. (2009) adalah komputer yang dijalankan berdasarkan hukum mekanika kuantum dan dapat menyelesaikan perhitungan data yang besar dengan jauh lebih cepat dibanding komputer konvensional. Kriptosistem yang masih tergolong aman diantaranya adalah enkripsi kunci publik NTRU, kriptosistem McEliece, dan enkripsi kunci publik Lattice-based. Chen (2016) mengatakan bahwa algoritme kriptosistem yang banyak digunakan saat ini, yaitu RSA dan kurva eliptik telah digagalkan algoritme Shor yang dapat menyelesaikan masalah faktorisasi prima dengan mudah. Pada tahun 1978, McEliece merumuskan suatu algoritme kunci asimetris dan memanfaatkan kode pengoreksi eror yaitu kode Goppa dalam mekanismenya yang kemudian dikenal sebagai kriptosistem McEliece. Roering (2013) mendesain kriptosistem McEliece berukuran 460 Kb dengan kode Goppa. Gagasannya yaitu dengan menambahkan

eror pada codeword sehingga pesan menjadi tersandi dan eror akan dikoreksi ketika penerima mendekripsi pesan. Enkripsi dan dekripsi kriptosistem McEliece memanfaatkan matriks generator kode. Seiring waktu, muncul berbagai kode yang dapat dimanfaatkan dalam suatu kriptosistem, diantaranya kode Bose-Chaudhuri-Hocquenghem (BCH), kode Reed Solomon, kode Reed Muller, kode Goppa, kode Golay, kode Hamming, dan kode Hadamard.

Reed dan Solomon (1960) merumuskan kode yang dirancang dari suatu lapangan hingga dan dapat mengoreksi eror. Kode tersebut kemudian dikenal sebagai kode Reed Solomon. Dalam komunikasi digital, metode yang paling umum digunakan menurut Kartika et al. (2015) adalah Forward Error Correction (FEC) sehingga dapat memanfaatkan kode Reed Solomon untuk mengatasi eror pada transmisi. Koreksi eror menurut Hakim et al. (2014) merupakan teknik untuk menjaga keaslian data selama proses pengiriman dan penyimpanan. Menurut Jariyah et al. (2013) kode Reed Solomon direpresentasikan dengan format RS(n,k) dengan n merupakan panjang keseluruhan informasi sedangkan k adalah Panjang informasi awal. Jamal et al. (2014) menyatakan bahwa kode Reed Solomon pertama kali diaplikasikan pada tahun 1970 dalam pengkodean transmisi pesawat ruang angkasa Voyager. Kode RS(255, 223, 33) dimanfaatkan pada pengiriman dokumentasi eksplorasi planet oleh NASA dan ESA. Akhir tahun 1980, kode Reed Solomon juga diterapkan dalam pengkodean informasi digital seperti CD, dan DVD. Kode Reed Solomon menurut Widiastuti et al. (2016) juga diterapkan dalam aplikasi pada sistem komunikasi maupun informasi. Wu (2017) juga mengatakan bahwa kode Reed Solomon secara luas digunakan dalam komunikasi dan penyimpanan besar untuk mengoreksi eror yang besar. Apriansyah et al. (2019) memberikan metode kode Reed Solomon pada encoding QR-code sebagai koreksi eror. Pada penelitian ini akan diterapkan kode Reed Solomon pada kriptosistem McEliece.

METODE PENELITIAN

Metode yang digunakan pada penelitian ini adalah studi literatur dan terapan. Literatur yang digunakan meliputi buku, artikel dalam jurnal, tesis, dan tulisan yang bersumber dari internet terkait kode Reed Solomon dan kriptosistem McEliece. Selanjutnya dilakukan penerapan algoritme dalam bahasa pemrograman Python berdasarkan parameter kode Reed Solomon.

Penentuan Parameter Kode

Kode Reed Solomon RS(n,k) merupakan kode linear berbasis blok atas $GF(q^m)$ untuk setiap bilangan bulat positif $z \leq q^m - 1$. *Galois Field* (GF) merupakan lapangan dengan banyak elemennya berhingga. Elemen di dalamnya dapat direpresentasikan oleh $\{0,1,2,\cdots,q^m-1\}$ dengan q merupakan bilangan prima sehingga tiap elemennya dapat direpresentasikan dalam bentuk *m-tuple* maupun integer. Umumnya, nilai q yang digunakan adalah 2. Pada penerapan kali ini akan digunakan contoh kode RS(15,9) atas lapangan hingga $GF(2^4)$ dengan total simbol (n) adalah $q^m - 1$, jumlah simbol data (k) adalah $n - 2t$, dan jumlah simbol koreksi $(t) = \frac{n-k}{2}$ maka diperoleh parameter untuk kode Reed Solomon sebagai berikut

1. Jumlah total simbol $(n) = 15$
2. Jumlah simbol data $(k) = 9$

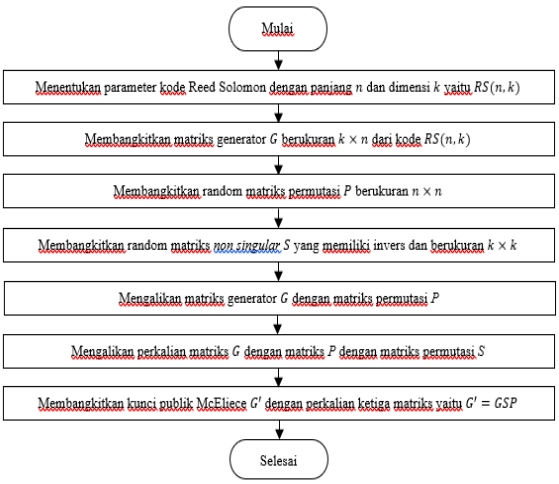
3. Jumlah simbol koreksi $(t) = 3$

Berdasarkan parameter kode Reed Solomon tersebut, maka elemen dalam *Galois Field* dapat direpresentasikan oleh bilangan $\{0,1,2,\cdots,15\}$. Menurut Gauthier [4], secara umum kode ditentukan oleh suatu matriks yang disebut matriks generator atas *Galois Field* tersebut.

Pembangkitan Kunci

Penerapan Kode Reed Solomon dalam suatu kriptosistem memerlukan adanya proses pembangkitan kunci. Proses ini merupakan proses penting dalam proses *encoding* dan *decoding* pada kriptosistem McEliece. Kriptosistem McEliece merupakan kriptosistem asimetris sehingga kunci yang digunakan berbeda dengan kriptosistem simetris. Terdapat dua kunci yang digunakan dalam mekanismenya yaitu kunci publik dan kunci privat. Kunci publik dibangun berdasarkan perkalian matriks G , matriks P, dan matriks S, sedangkan kunci privat pada mekanismenya terdiri dari matriks S, matriks P dan *decoding* pada matriks generator yang telah dibangkitkan. Ketiga matriks tersebut memiliki peran yang berbeda dalam mekanisme kriptosistem. Matriks G merupakan matriks generator berukuran $k \times n$ yang dibangkitkan berdasarkan parameter kode yang digunakan. Konstruksi matriks generator berbeda-beda dan bergantung pada jenis kode dan parameter yang digunakan. Elemen dalam suatu matriks generator direpresentasikan dalam *Galois Field* (2^4) sehingga banyaknya elemen dalam matriksnya berhingga, yaitu $\{0,1,2,\cdots,15\}$. Matriks P merupakan random matriks permutasi berukuran $n \times n$yang dibangun secara acak dan berguna untuk mengaburkan elemen pada matriks generator kode sehingga matriks generator menjadi tidak jelas. Matriks P dapat diperoleh dengan mengubah kolom pada suatu matriks identitas. Elemen pada matriks P berisi bilangan 0 atau 1 dengan tepat satu bit bukan nol pada setiap baris dan kolom, artinya tidak ada angka 1 yang terletak dalam baris maupun kolom yang sama. Matriks S merupakan random matriks *non singular* berukuran $k \times k$ dan berguna untuk mengacak susunan elemen sehingga susunan matriks generator kode tersembunyi. Matriks ini juga disebut sebagai matriks pengacak S. Elemen dalam suatu matriks *non singular* direpresentasikan dalam *Galois Field* (2^4) sehingga elemennya yaitu berkisar pada $\{0,1,2,\cdots,15\}$. Ukuran pada masing-masing matriks merepresentasikan parameter yang digunakan dalam membangkitkan matriks, yaitu n sebagai panjang kode linear, dan k sebagai dimensi kode linear. Ketiga matriks tersebut berperan penting dalam mekanisme kriptosistem McEliece.

Setiap kode memiliki algoritme *decoding* yang berbeda. Pada penelitian ini, proses *decoding* didasarkan pada penggunaan algoritme *decoding* untuk kode Reed Solomon $RS(15,9)$ atas $GF(2^4)$. Berikut diberikan skema pembangkitan kunci yaitu



Gambar 3. Skema pembangkitan kunci

FIBONACCI : Jurnal Pendidikan Matematika dan Matematika. Vol. 9 (1), pp: 79 – 88.

Enkripsi Kunci Publik McEliece

Proses enkripsi pada kriptosistem McEliece memerlukan kunci publik yang sebelumnya telah dibangkitkan. Mekanisme enkripsi dilakukan dengan pengirim menentukan suatu pesan string m. Kemudian pesan tersebut akan diatur agar memenuhi ukuran panjang k. Jika pesan yang dikirim sudah sesuai dengan panjang simbol data k maka pesan tersebut dapat langsung diubah ke dalam UNICODE. Jika panjang pesan tersebut kurang dari panjang simbol data k maka perlu dilakukan *padding* terhadap pesan yang akan dikirim. Setelah memperoleh pesan m yang telah diubah ke dalam UNICODE maka pesan m dapat dikalikan dengan kunci publik G' sehingga pesan sepanjang k akan berubah menjadi pesan sepanjang n. Selanjutnya, untuk melakukan enkripsi pada pesan dapat dilakukan dengan menambahkan eror (e) sebanyak t pada *codeword* sehingga *codeword* tersebut menjadi suatu *ciphertext*. Algoritma *encoding* yaitu:

$$y = mG' + e \quad (1)$$

dengan y merupakan *ciphertext* yang diperoleh berdasarkan hasil keseluruhan enkripsi.

Dekripsi Kunci Publik McEliece

Setelah pesan terenkripsi $y = mG' + e$ diterima oleh penerima maka penerima melakukan dekripsi guna memeroleh pesan asli m dengan rumus yaitu:

$$D(yP^{-1}) = D([mG' + e]P^{-1} \quad (2)$$
$$= D(mSGPP^{-1} + eP^{-1}) \quad (3)$$
$$= D(mSG + e') \quad (4)$$
$$= msG \quad (5)$$

dengan $e' = eP^{-1}$ dan D merupakan fungsi *decoding*. Dalam mendekripsi pesan, penerima melakukan perkalian *codeword* c terhadap invers matriks P, kemudian melakukan proses *decoding* untuk kode Reed Solomon yaitu

a. Menghitung matriks *parity check* H berukuran $(n-k) \times n$,
b. Menghitung *syndrome* vektor dengan $s = c \times H^T \ mod\ 16$ dengan c merupakan *codeword* yang diterima dan H^T merupakan transpose matriks *parity check*,
c. Memeriksa *syndrome* vektor yaitu jika terdapat elemen bukan nol dalam vektorr tersebut maka eror terdeteksi,
d. Mencari posisi eror jika terdeteksi eror pada langkah sebelumnya $e\_p = \{i | H^T[i] = syndrome\}$ untuk $i = 0$ hingga $(n-k-1)$ dengan i merupakan elemen ke-i dalam vektor c dan $H^T[i]$ mengacu pada baris ke-i dalam matriks transpose H,
e. Memperbaiki eror dengan $c[e_p] = (c[e_p] - syndrome[e\_p])\ mod\ 16$.

Setelah eror dikoreksi maka selanjutnya yaitu mengalikan hasilnya dengan invers matriks S untuk mengembalikan pesan tersebut kembali pada bentuk originalnya. Matriks dan fungsi *decoding* merupakan kunci privat pada mekanisme kriptosistem. Pada proses ini digunakan modulo 16 sebagai representasi *Galois Field* $GF(2^4)$ sehingga nilai elemen dalam rentang *Galois Field* tersebut terjaga.

HASIL DAN PEMBAHASAN

Pada penelitian ini digunakan kode Reed Solomon $RS(15,9)$ yaitu dengan $n = 15$, dan $k = 9$ yang akan diterapkan pada kriptosistem McEliece. Akan dikirim pesan

string maka sebelum pesan tersebut dikirimkan, perlu dilakukan pembangkitan kunci sehingga diperoleh kunci publik dan kunci privat. Setelah kunci tersebut diperoleh melalui perkalian matriks-matriks, selanjutnya dilakukan enkripsi pada pesan. Dimisalkan akan dikrimkan pesan string m berupa kalimat "Halo, Bob". Pesan tersebut diubah ke dalam karakter lain dengan memanfaatkan standar UNICODE. Setiap karakter pada pesan "Halo, Bob" kemudian ditransformasikan menjadi bilangan $[72, 97, 108, 111, 44, 32, 66, 111, 98]$.

Pesan tersebut memiliki panjang 9 (sesuai dengan ukuran k) sehingga tidak perlu dilakukan *padding* pesan. Hasil tersebut kemudian diubah menjadi vektor pesan dengan cara mengubah karakter ke dalam ASCII sehingga diperoleh [72 97 108 111 44 32 66 111 98]. Oleh karena algoritme beroperasi pada $GF(2^4)$ maka karakter tersebut disesuaikan pada lapangan tersebut sehingga diperoleh vektor pesan [8 1 12 15 12 0 2 15 2]. Berikutnya melakukan proses enkripsi dengan mengalikan vektor pesan dengan kunci publik yang telah dibangkitkan dan menambahkan eror acak diperoleh [30 0 0 0 0 9 11 5 0 2 1 0 0 13 7 1 2].Berikutnya mendeteksi dan mengoreksi pesan sehingga diperoleh vektor pesan [14 0 1 0 11 0 13 0 7 2 9 0 12 0 5].

Vektor pesan kemudian dikalikan dengan invers matriks permutasi P. Setelah diperoleh *codeword* dilakukan proses *decoding* berdasarkan algoritme kode Reed Solomon sesuai parameter yang ditentukan. Setelah proses selesai maka dilakukan proses dekripsi untuk mengembalikan pesan ke bentuk awal. Pesan terdekripsi merupakan karakter dalam UNICODE $[72, 97, 108, 111, 44, 32, 66, 111, 98]$, lalu diubah ke dalam string sehingga diperoleh [H, a, l, o, , , B, o, b]. Output dari proses dekripsi yaitu kalimat "Halo, Bob". Kalimat tersebut merupakan kalimat awal yang diinputkan. Oleh karena itu, proses dekripsi berjalan lancar.

Penelitian ini berfokus pada penerapan kode Reed Solomon $RS(15,9)$ pada kriptosistem McEliece menggunakan bahasa pemrograman Python. Mekanisme dalam penerapan kode Reed Solomon pada kriptosistem McEliece merupakan bentuk terapan dari ilmu aljabar abstrak yang dituangkan ke dalam ilmu kriptografi.

Secara matematis, kode ini dibentuk pada suatu lapangan berhingga yang dikenal sebagai *Galois Field*. Pembentukan elemen dalam suatu *Galois Field* bergantung pada operasi penambahan dan perkalian dalam suatu lapangan. Dalam penerapan ini, digunakan kode $RS(15,9)$ atas $GF(2^4)$ sehingga diperlukan polinomial *irreducible* berderajat 4 yaitu $P(x) = x^4 + x + 1$. Dalam memudahkan prosesnya, pada penelitian ini digunakan bahasa pemrograman Python untuk memudahkan perhitungan. Python merupakan bahasa pemrograman yang banyak digunakan secara luas karena kemudahan dan efisiensi yang ditawarkannya. Python sendiri dimanfaatkan pada pengembangan berbagai hal, seperti aplikasi, web, perangkat lunak, *machine learning*, hingga kriptografi. Berikut merupakan *syntax* yang dikonstruksi pada bahasa Pemrograman Python terkait penerapan pada penelitian dengan *import library* yang telah tersedia pada Python.

```
import numpy as np
from sympy import symbols
from sympy.polys.polytools import lcm
def reed_solomon_parameters(n, k):
    t = (n - k) // 2
    field_size = 2**4
```

```
# Definisikan Galois Field GF(2^4)
GF = np.zeros((field_size,), dtype=int)
GF[1] = 1
for i in range(2, field_size):
        GF[i] = GF[i-1] << 1
        if GF[i] >= field_size:
           GF[i] ^= 0b10011

# Definisikan generator polynomial
x = symbols('x')
g = 1
for i in range(1, 2*t + 1):
        g = lcm(g, x - GF[i])
    return n, k, t, g

def con_generator_matrix(n,k,field_size):
    gen_matrix = np.zeros((k, n), dtype=int)
    alpha_list = list(range(field_size))
    for i in range(k):
        for j in range(n):
            gen_matrix[i, j] = pow(alpha_list[j], i,
            field_size)
    return generator_matrix

H = np.concatenate((G[:, k:].T, np.eye(n - k,
dtype=int)), axis=1)

def generate_permutation_matrix(n):
    permutation_indices =
    np.random.permutation(range(n))
    permutation_matrix = np.zeros((n, n),
    dtype=int)
    permutation_matrix[np.arange(n),
    permutation_indices] = 1
    return permutation_matrix

def generate_non_singular_matrix(k):
    field_size = 2 ** 4
    non_matrix = np.zeros((k, k), dtype=int)
    while np.linalg.matrix_rank(matrix) != k:
    non_matrix = np.random.randint(0,
    field_size, size=(k, k))
    return matrix

G_publik = S.dot(G.dot(P))
    message = "Halo, Bob"
    codeword = np.dot(m.T, G_publik) %
    field_size
    eror_weight = 3
    ciphertext_y = codeword + eror_vector %
    field_size

syndrome = np.dot(y, H.T) % 16
c= np.dot(y, P_inverse)
decoded_m = transform_to_unicode(cipher)
w = transform_to_ciphertext(decoded_m)
string = arr.tobytes().decode('utf-8')
print("String:")
print(string)
```

Syntax Pyhton tersebut memproses pengiriman *input* pesan awal m yaitu “Halo, Bob”. Melalui pembangkitan berbagai matriks yang telah dibahas sebelumnya dan algoritme *encoding* dan *decoding* pada kode Reed Solomon maka diperoleh pesan yang telah didekripsi adalah sebagai berikut $[72, 97, 108, 111, 44, 32, 66, 111, 98]$ dan *output* berupa string yang sama seperti pesan awal yaitu “Halo, Bob”. Pada penelitian ini, telah dilakukan penerapan kode Reed Solomon atas *Galois Field* (2^4) pada kriptosistem McEliece secara sederhana dengan jumlah simbol data awal berjumlah 9, dan setelah melalui proses enkripsi jumlah kodenya menjadi 15 dengan kemampuan koreksi erornya adalah 3. Penerapan ini masih dapat dilanjutkan secara lebih luas dan rinci dengan menggunakan berbagai parameter yang lebih besar sehingga menguatkan argumen penelitian sebelumnya bahwa kode Reed Solomon dapat dimanfaatkan dalam salah satu kriptosistem yang saat ini masih aman digunakan yaitu kriptosistem McEliece.

SIMPULAN

Berdasarkan hasil dan pembahasan diperoleh kesimpulan bahwa kode Reed Solomon yang berbasis pada koreksi eror dapat diterapkan pada mekanisme kriptosistem McEliece dengan penambahan

eror sebesar 3 bit. Eror tersebut akan dideteksi dan dikoreksi berdasarkan algoritme *decoding* kode Reed Solomon pada proses dekripsi. Pada penelitian sebelumnya, kriptosistem McEliece menggunakan kode Goppa yang dapat mengoreksi eror sebesar 2 bit dengan jumlah simbol data awal hanya 7 bit, sedangkan pada penerapan kode Reed Solomon $RS(15,9)$ dapat mengoreksi 3 bit eror dengan jumlah simbol data awal 9 bit. Konsep penerapan kode Reed Solomon dapat dilakukan dengan bahasa pemrograman Python yang mengimplementasi setiap langkah algoritme kriptosistem McEliece mulai dari pembangkitan kunci, proses enkripsi hingga dekripsi dengan bantuan *library* yang telah tersedia pada bahasa pemrograman Python. Penelitian ini perlu dilakukan guna mengamankan pesan dalam suatu transmisi agar pesan tidak dapat dirusak oleh pihak lain. Kriptosistem McEliece masih tergolong aman sehingga menjadi pilihan yang tepat untuk dimanfaatkan secara luas meskipun membutuhkan penyimpanan yang besar.

DAFTAR PUSTAKA

Apriansyah, A., Fauziah, dan Hayati, N. 2019. *Implementasi Algoritma Reed Solomon Codes pada Proses Encoding QR Code pada Sistem Absensi*. Jurnal Infomedia, Vol 4 (2), pp:75-80.

Bernstein, D.J., Buchmann, J., and Dahmen,E. 2009. *Post-Quantum Cryptography*, Berlin: Springer.

Chen, L., Jordan, S., Liu, Y.K., Moody, D., Peralta, R., Perlner, R., and Smith-Tone, D. 2016. *Report on Post-Quantum Cryptography*. U.S. Department of Commerce, National Institute of Standards and Technology. [Online] Tersedia: https://csrc.nist.gov/publications/detail/nistir/8105/final. [02 Januari 2023].

Gauthier, V., Otmani, A., and Tillich, J.P. 2012. *A Distinguisher-Based Attack on a Variant of McEliece's Cryptosystem Based on Reed-Solomon Codes.* [Online] Tersedia: https://arxiv.org/abs/1204.6459 [03 Januari 2023].

Hakim, R.H., Rahman, A., Amin, D.E., Roza, W., dan Rahim, E. 2014. *Implementasi Encoder Reed-Solomon pada FGPA Berbasis CCSDS*. Jurnal Teknologi Dirgantara. Vol 12 (2), pp:116-127.

Jamal, R.P., Haryanto, L., dan Amir, A.K. (2014). *Konstruksi Kode Reed-Solomon sebagai Kode Siklik dengan Polinomial Generator*. Paper of Semantic Scholar. Makassar. [Online] Tersedia: https://www.semanticscholar.org/paper/Konstruksi-Kode-Reed-Solomon-sebagai-Kode-Siklik-Jamal-Haryanto/22344adaeb16fcfdb51e32f451e510e8d87ea. [05 Januari 2023].

Jariyah, A., Suwadi, dan Hendrantoro, G. 2013. *Pengkodean Kanal Reed Solomon Berbasis FGPA untuk Transmisi Citra pada Satelit Nano.* Jurnal Teknik Pomits. Vol 2 (1), pp:51-56.

Kartika, W., Mustika I.W., dan Bejo, A. 2015. *Implementasi Data Kirim dan Terima dari Reed Solomon Code pada Controller Area Network*. Proceeding Departemen Teknik Elektro dan Teknologi Informasi. UGM Yogyakarta.

McEliece, R.J. 1978. *A Public-Key Cryptosystem Based On Algebraic Coding Theory*. DSN Progress Report.

Menezes, A., Oorschot, P., and Vanstone, S. 1997. *Handbook of Applied Cryptography*. CRC Press.

Reed, I.S., and Solomon, G. 1960. *Polynomial Codes over Certain Finite Fields*. Journal of the Society for Industrial and Applied Mathematics. Vol 8 (2), pp:300-304.

Roering, C. 2013. *Coding Theory-Based Cryptography: McEliece Cryptosystem in Sage*. Disertasi Honors Theses.

Sinaga, M.C. 2017. *Kriptografi Python*. Medan: INA-Rxiv.

Suryono, F.N. 2022. *Penerapan Reed-Solomon Code dalam Pembuatan Self-Correcting Data*. Makalah IF2120 Matematika Diskrit Program Studi Teknik Informatika, STEI Bandung.

Widiastuti, N., Lestari, D., dan Dhoruri, A. 2016. *Sifat dan Karakteristik Kode Reed Solomon Beserta Aplikasinya pada Steganography*. Seminar Nasional Matematika dan Pendidikan Matematika UNY 2016.

Wu, T., dan Wang, R. 2017. *Stream Cipher by Reed-Solomon Code.* Disertasi Conference Paper.