Jurnal Riset Mahasiswa Matematika
Volume 4(3) (2025), Pages 133-137
p-ISSN: 2808-1552; e-ISSN: 2808-4926

Penerapan Kriptosistem Niederreiter Menggunakan Kode Goppa Biner untuk Mendukung Keamanan Data dalam Sistem Kriptografi Modern

Aldina Laili Chusnia, Muhammad Khudzaifah*, Erna Herawati

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

Email: khudzaifah@uin-malang.ac.id

Abstrak

Perkembangan kriptografi modern menghadirkan tantangan baru berupa ancaman dari komputer kuantum, yang mendorong kebutuhan akan proses enkripsi yang lebih kuat. Salah satu metode kriptografi pasca-kuantum yang mampu memberikan perlindungan terhadap ancaman tersebut adalah kriptosistem Niederreiter berbasis kode Goppa biner. Dalam penelitian ini, kode Goppa biner digunakan dalam pembentukan kunci publik dan kunci privat, serta dalam proses decoding. Implementasi dilakukan dengan memanfaatkan polinomial tertentu pada medan hingga berorde enam belas, yang menghasilkan parameter kode dengan panjang 12, dimensi 4, dan kapasitas koreksi hingga dua kesalahan. Kode Goppa diterapkan dalam proses koreksi kesalahan melalui perhitungan sindrom, yang memungkinkan deteksi dan perbaikan bit-bit yang salah sehingga pesan asli dapat dipulihkan dengan akurat. Hasil penelitian menunjukkan bahwa kode Goppa biner efektif dalam mendeteksi dan memperbaiki kesalahan, sehingga memastikan integritas pesan. Penelitian ini diharapkan dapat berkontribusi terhadap pengembangan kriptosistem yang lebih tangguh dalam menjaga kerahasiaan informasi di era digital yang terus berkembang.

Kata kunci: Kode Goppa; Kriptosistem *Niederreiter*; Kriptografi

Abstract

The advancement of modern cryptography presents new challenges posed by quantum computers, necessitating the development of stronger encryption processes. One of the post-quantum cryptographic methods capable of providing protection against such threats is the Niederreiter cryptosystem based on binary Goppa codes. In this study, binary Goppa codes are utilized in the formation of public and private keys, as well as in the decoding process. The implementation employs a specific polynomial over a finite field of order sixteen, resulting in code parameters with a length of 12, a dimension of 4, and the capability to correct up to two errors. Goppa codes are applied in the error correction process through syndrome calculation, enabling the detection and correction of erroneous bits and accurate recovery of the original message. The results demonstrate that binary Goppa codes are effective in detecting and correcting errors, thereby ensuring message integrity. This research is expected to contribute to the development of more robust cryptosystems for maintaining information confidentiality in the rapidly evolving digital era.

Keywords: Goppa Code; *Niederreiter* Cryptosystem; Cryptography

PENDAHULUAN

Pada era digital yang semakin maju, komunikasi telah menjadi aspek penting dalam berbagai bidang kehidupan. Seiring dengan peningkatan konektivitas dan pertukaran informasi secara daring, perlindungan terhadap data dan pesan yang ditransmisikan melalui jaringan komunikasi menjadi semakin krusial [1]. Informasi disampaikan melalui berbagai bentuk pesan seperti tulisan, gambar,

Submitted: 28 Desember 2024 Reviewed: 7 Februari 2025 Accepted: 24 Februari 2025
Doi: http://dx.doi.org/10.18860/jrmm.v4i3.31216

atau simbol, yang dapat dibagi menjadi beberapa kategori, termasuk pesan grup dan pesan rahasia. Pesan rahasia merupakan pesan yang hanya diketahui oleh individu tertentu dan tidak boleh diakses oleh pihak lain [2]. Pentingnya menjaga kerahasiaan pesan tercermin dari banyaknya kasus perubahan atau manipulasi dokumen oleh pihak yang tidak berwenang, sehingga diperlukan prosedur untuk menjaga kerahasiaan dan integritas pesan [3].

Salah satu metode utama untuk menjaga kerahasiaan pesan adalah dengan menggunakan kriptografi. Kriptografi merupakan ilmu yang berkaitan dengan metode untuk mengamankan pesan atau informasi penting, menjaga integritas, serta memastikan autentikasi informasi agar hanya dapat diakses oleh pihak yang berwenang melalui penggunaan kunci rahasia [4]. Meskipun kriptografi telah digunakan sejak zaman kuno, tantangan keamanan yang terus berkembang di dunia digital mendorong perlunya inovasi dalam teknik kriptografi. Proses utama dalam kriptografi mencakup enkripsi dan dekripsi, yaitu proses pengubahan plainteks menjadi cipherteks agar tidak dapat dibaca oleh pihak yang tidak berwenang [5], serta proses mengembalikan cipherteks menjadi plainteks untuk dibaca oleh penerima [6].

Kriptografi terbagi menjadi dua jenis, yaitu kriptografi simetris dan asimetris. Kriptografi simetris menggunakan satu kunci yang sama untuk enkripsi dan dekripsi, sedangkan kriptografi asimetris menggunakan sepasang kunci, yaitu kunci publik dan kunci privat, dalam proses enkripsi dan dekripsi pesan [7].

Munculnya teknologi komputer kuantum menjadi ancaman serius bagi sistem kriptografi klasik. Algoritma kunci publik seperti ElGamal dan RSA berpotensi menjadi tidak aman karena komputer kuantum mampu memecahkan kode-kode tersebut dalam waktu yang relatif singkat [8]. Pada tahun 1990-an, Shor mengusulkan algoritma yang dapat menyelesaikan masalah faktorisasi bilangan bulat dan logaritma diskrit dalam waktu polinomial menggunakan komputer kuantum [2]. Ancaman ini memicu lahirnya bidang baru yang disebut kriptografi pasca-kuantum, yaitu pengembangan sistem kriptografi yang tetap aman meskipun serangan dilakukan dengan komputer kuantum.

Salah satu contoh kriptografi pasca-kuantum adalah kriptosistem Niederreiter, yang merupakan varian dari kriptosistem McEliece. Kriptosistem ini menawarkan beberapa perbaikan, seperti penggunaan ukuran kunci publik yang lebih kecil serta proses enkripsi dan dekripsi yang lebih efisien dibandingkan McEliece [2]. Kriptosistem Niederreiter, yang dikembangkan oleh Harald Niederreiter pada tahun 1986, memanfaatkan prinsip aljabar linier dan teori kode untuk mengamankan pertukaran informasi [9]. Sistem ini menggunakan matriks pemeriksaan paritas dari kode linier sebagai dasar kriptografi, dengan sindrom sebagai bentuk cipherteks, sehingga menghasilkan enkripsi yang lebih cepat.

Kelebihan kriptosistem ini mencakup tingkat keamanan tinggi terhadap serangan komputer kuantum serta efisiensi enkripsi dan dekripsi. Sebagai ilustrasi, kriptosistem ini dapat menggunakan kunci publik hingga ukuran 1MB untuk memberikan keamanan setara 256-bit klasik, yang sesuai dengan standar keamanan pasca-kuantum 128-bit [10].

Dalam implementasi kriptosistem Niederreiter, diperlukan kode koreksi kesalahan yang andal, salah satunya adalah kode Goppa biner. Kode ini merupakan bagian dari keluarga kode Goppa umum yang diperkenalkan oleh Valerii Denisovich Goppa pada 1970-an, dengan struktur binernya yang memberikan keunggulan tertentu dibandingkan kode nonbiner [11]. Dalam konteks kriptografi, kode Goppa biner digunakan untuk mendukung pembentukan kunci publik dan privat melalui pencarian support dan polinomial Goppa yang besar. Polinomial Goppa dengan koefisien biner memungkinkan deteksi dan koreksi kesalahan secara efisien [12]. Keunggulan utama kode Goppa biner adalah kemampuannya dalam mendeteksi dan memperbaiki kesalahan transmisi data dengan tingkat keandalan tinggi [13], sehingga menjadikannya pilihan utama dalam sistem kriptografi pasca-kuantum [14].

Beberapa penelitian terdahulu telah menerapkan kriptosistem Niederreiter berbasis kode Goppa biner pada implementasi perangkat keras, seperti FPGA (Field-Programmable Gate Array). Penelitian tersebut bertujuan mengembangkan implementasi FPGA untuk kriptosistem Niederreiter, di mana plainteks dienkripsi dengan kriptosistem Niederreiter dan pembentukan kunci menggunakan parameter dari kode Goppa biner [2]. FPGA sebagai perangkat IC yang dapat

diprogram secara fleksibel, memungkinkan optimasi performa dan efisiensi sumber daya untuk berbagai kebutuhan, baik dalam sistem tertanam maupun akselerator server.

Dalam penelitian ini, dilakukan implementasi kode Goppa biner dalam kriptosistem Niederreiter. Kode Goppa biner digunakan dalam pembentukan kunci publik dan kunci privat, serta dalam proses enkripsi dan dekripsi, dengan tujuan utama untuk melindungi kerahasiaan dan integritas data.

METODE

Penelitian ini memiliki tiga tahapan, yaitu:

1. Proses Pembentukan Kunci
   Pembentukan kunci meliputi tahapan sebagai berikut:
   a. Menentukan *Galois Field* (GF) dari polinomial Goppa $g(x)$ untuk mendapatkan parameter kode Goppa biner;
   b. Menghitung matriks *parity check* H dengan ukuran 8×12 untuk sebuah kode Goppa $\Gamma(L, g)$ berdimensi $k = 4$;
   c. Memilih matriks permutasi P dengan ukuran 12×12;
   d. Menentukan matriks *non-singular* S dengan ukuran 8×8;
   e. Menghitung nilai pembentukan kunci H' sebagai kunci publik berukuran 8×12;

$$H' = S \cdot H \cdot P$$

2. Proses Enkripsi
   Proses enkripsi meliputi tahapan sebagai berikut:
   a. Membuat suatu pesan m dengan panjang n-bit dan bobot *hamming* t sebagai *plaintext*;
   b. Mengubah m *plaintext* ke bentuk biner dengan menggunakan kode ASCII;
   c. Mengurangkan m *plaintext* menggunakan vektor e *error* dengan bobot hamming t;

$$m' = m - e$$

   d. Menghitung *codeword* $C = S \cdot H \cdot P \cdot (m')^T$.
3. Proses Dekripsi
   Proses dekripsi meliputi tahapan sebagai berikut:
   a. Menghitung invers dari matriks *non-singular S;*
   b. Mengalikan *ciphertext* C_i dengan invers dari matriks *non-singular* S untuk menghasilkan matriks Y_i;

$$Y_i = S^{-1} \times C_i$$

   c. Menghitung vektor z sedemikian hingga $H \times z^T = Y_i$;
   d. Menghitung matriks *parity check* H untuk $\Gamma(L, g^2(x))$;
   e. Mencari sindrom $s(x)$;
   f. Mencari himpunan lokasi *error* sehingga mendapatkan $\hat{m}$*;*
   g. Mengalikan matriks $\hat{m}$ dengan matriks permutasi P untuk mengembalikan *ciphertext* ke bentuk aslinya;
   h. Kode biner m_i yang diperoleh dikembalikan kedalam bentuk teks berdasarkan tabel ASCII.

HASIL DAN PEMBAHASAN

Proses Pembentukan Kunci

Kriptosistem *Niederreiter* merupakan salah satu kriptosistem kunci publik yang berbasis teori kode dan dikategorikan sebagai tingkat keamanan yang paling kuat untuk kriptografi *post-quantum*. Proses pembentukan kunci pada kriptosistem *Niederreiter* menggunakan kode Goppa biner sangat penting untuk menjamin keamanan dan keefektifan sistem kriptografi. Terdapat dua jenis kunci yang akan dibangkitkan yaitu kunci publik dan kunci privat Proses pembentukan kunci diawali dengan mencari parameter dari kode Goppa biner yaitu $[n, k, d]$ [15].

Selanjutnya yaitu membuat kunci privat berupa matriks *parity-check* H berukuran $(n-k) \times n$ berdasarkan parameter kode Goppa biner. kemudian matriks *non-singular* S berukuran $(n-k) \times (n-k)$ yang dipilih secara acak. Kemudian untuk kunci privat matriks permutasi P diperoleh dengan memilih sembarang matriks berukuran $n \times n$. Terakhir yaitu membangkitkan kunci publik dengan menghitung $H' = SHP$ yang akan menghasilkan matriks berukuran $(n-k) \times n$.

Proses Enkripsi

Proses enkripsi menggunakan kriptosistem *Niederreiter* melibatkan tahapan-tahapan yang berbasis pada teori kode linear. Dalam kriptosistem ini, pesan yang akan dienkripsi akan direpresentasikan sebagai vektor biner. Proses ini diawali dengan pemilihan pesan *m plaintext* yang akan dienkripsi, kemudian dikonversi menjadi vektor biner menggunakan kode ASCII dengan panjang n-bit dan bobot *hamming* t. Kemudian vektor ini dikurangkan dengan vektor *e error* agar pesan dapat menghasilkan bobot *hamming* t. Selanjutnya, hasil tersebut ditransposekan dan dikalikan dengan kunci publik H'. Hasil dari perkalian ini menghasilkan vektor *ciphertext* $C = H' \times (m')^T$. *Ciphertext* yang telah dihasilkan berukuran menjadikan pesan tersebut sulit dibaca oleh pihak yang tidak berwenang.

Proses Dekripsi

Proses dekripsi ini digunakan untuk mengembalikan pesan ke bentuk semula. Proses dekripsi menggunakan kriptosistem *Niederreiter* melibatkan penggunaan kunci privat untuk mengubah pesan tersebut dari *ciphertext* C_1 dan C_2 yang telah dienkripsi dengan menggunakan kunci publik H'. Kemudian mengalikan *invers* dari matriks *non singular* S^{-1} dengan *ciphertext* C_1 dan C_2. Kemudian hasil tersebut digunakan untuk mencari vektor *z* dengan menggunakan rumus $H \times z_i^T = S^{-1} \times C_i$. Selanjutnya, penerima menggunakan algoritma *decoding* untuk mengoreksi kesalahan yang ada pada *ciphertext.* Selanjutnya, penerima mengalikan hasil tersebut dengan matriks permutasi P untuk mendapatkan pesan asli.

$$m_i = \widehat{m}_i \times P$$

KESIMPULAN

Proses pembentukan kunci pada kriptosistem *Niederreiter* menggunakan kode Goppa biner menghasilkan kunci privat dan kunci publik. Kunci privat terdiri dari matriks *non-singular* S berukuran 8×8, matriks *parity-check* H berukuran 8×12, dan matriks permutasi P berukuran 12×12. Sedangkan pada kunci publik menghasilkan matriks H' berukuran 8×12.

Proses enkripsi dalam kriptosistem *Niederreiter* melakukan perubahan pesan menjadi vektor biner dan dikurangkan dengan *error* kemudian dikalikan dengan matriks kunci public H' menghasilkan *ciphertext* 8-bit. Proses ini menjadikan proses enkripsi sebagai langkah penting dalam menjaga kerahasiaan dan keamanan pesan.

Proses dekripsi kriptosistem *Niederreiter* melibatkan proses untuk membalikkan enkripsi. Proses ini diawali dengan mengalikan *ciphertext* dengan invers matriks *non-singular S,* kemudian *error* dikoreksi dengan memanfaat kode Goppa biner. Setelah *error* dikoreksi dan didapatkan vektor kode ($\widehat{m}$), selanjutnya dikalikan dengan matrik permutasi P untuk mendapatkan pesan semula. Sehingga, pada proses dekripsi ini pesan yang telah terenkripsi kembali ke pesan semula. Dengan mengimplementasikan kode Goppa biner pada kriptosistem *Niederreiter* menunjukkan potensi besar dalam meningkatkan keamanan informasi.

DAFTAR PUSTAKA

[1] Baldi M. QC-LDPC Code-Based Cryptography. Cham: Springer International Publishing; 2014. (SpringerBriefs in Electrical and Computer Engineering).

[2] Danner J, Kreuzer M. A Fault Attack On The Niederreiter Cryptosystem Using Binary Irreducible Goppa Codes. Complexity, Cryptology. 2020;12(1).

[3] Sari A. Karakteristik Bilangan Cokelat. Matematika. Bandar Lampung; 2018.

[4] Farooq S, Altaf A, Iqbal F, Thompson EB, Vargas DLR, Díez I de la T, et al. Resilience Optimization of Post-Quantum Cryptography Key Encapsulation Algorithms. Sensors (Basel). 2023 Jun 6;23(12):1–24.

[5] Ariska B, Suroso, Endri J. Rancangan Kriptografi Hybrid Kombinasi Metode Vigenere Cipher dan Elgamal pada Pengamanan Pesan Rahasia. Seminar Nasional Inovasi dan Aplikasi Teknologi di Industri . 2018;328–36.

[6] Carita SS. Implementasi Kode Goppa Biner Terpisahkan dalam Kriptosistem McElice. [Bandung]; 2017.

[7] Fadilatul Ilmiyah N. Kajian tentang Kriptosistem McEliece dalam Menghadapi Tantangan Komputer Kuantum di Era Revolusi Industri 4.0. Prosiding Seminar Nasional MIPA. 2018.

[8] Ling S, Xing C. coding theory. 2004.

[9] Rinaldi Munir. Matematika Diskrit. 2008;

[10] Wang W, Szefer J, Niederhagen R. FPGA-based Niederreiter Cryptosystem using Binary Goppa Codes. 2018;

[11] Jochemsz. Ellen. Goppa Codes & the McEliece Cryptosystem. Vrije Universiteit. 2002;

[12] B C, G Z. The number of extended irreducible binary Goppa codes.

[13] Ilmiyah NF. Kajian Tentang Kriptosistem Mceliece Dalam Menghadapi Tantangan Komputer Kuantum Di Era Revolusi Industri 4.0. Prosiding Seminar Nasional MIPA. 2018;216–26.

[14] Waliprrana, W. Studi dan implementasi algoritma kunci publik McEliece. 2011;

[15] Singh H. Code based Cryptography: Classic McEliece. 2020 Jul 30;